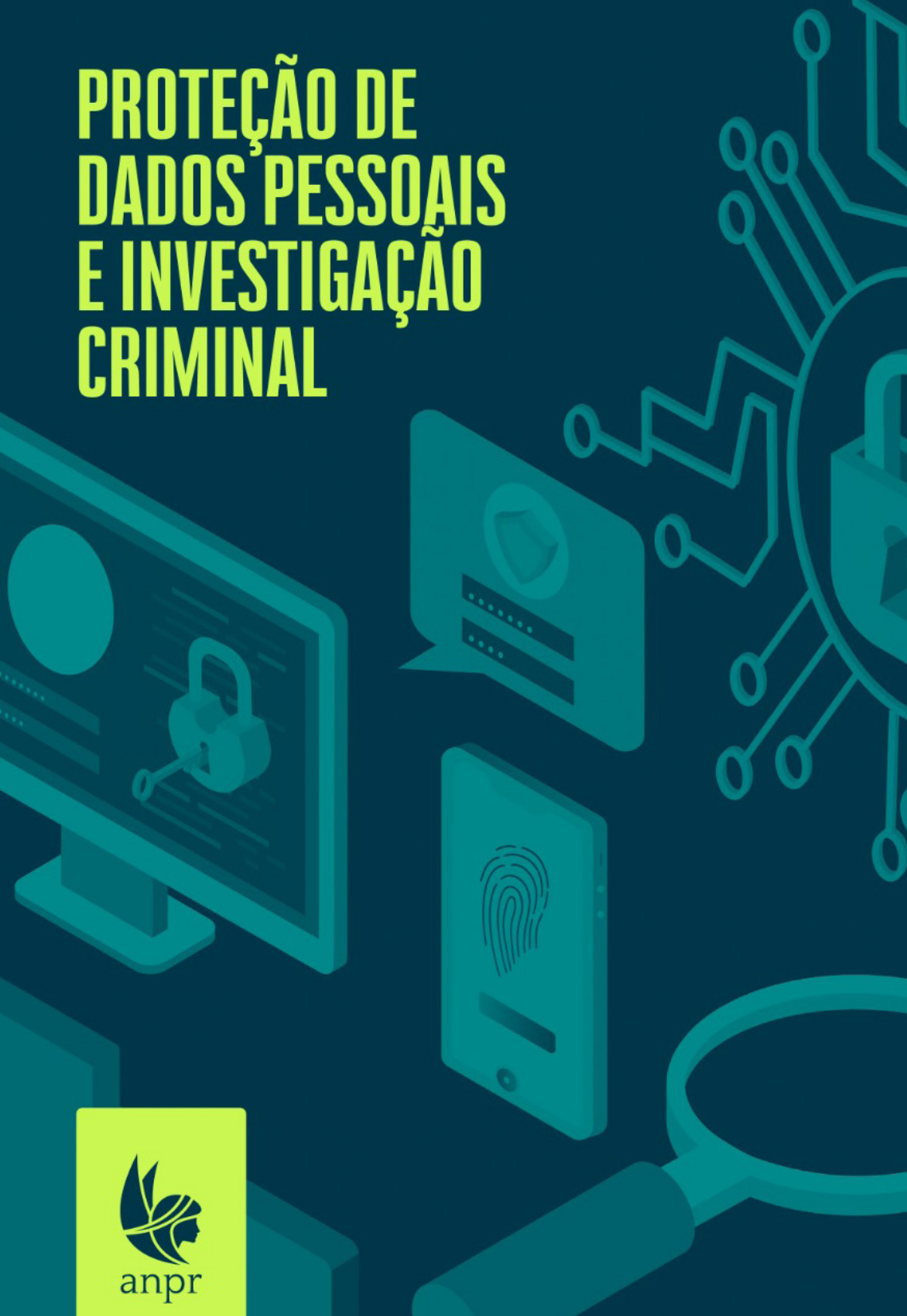
PROTEÇÃO DE DADOS PESSOAIS E INVESTIGAÇÃO CRIMINAL



anpr

Ministério Público Federal
3ª Câmara de Coordenação e Revisão

PROTEÇÃO DE DADOS PESSOAIS E INVESTIGAÇÃO CRIMINAL

Organizadores:
Vladimir Barros Aras
Andrey Borges de Mendonça
Walter Aranha Capanema
Carlos Bruno Ferreira da Silva
Marcos Antônio da Silva Costa

Brasília, 2020

Impresso no Brasil | *Printed in Brazil*

Editor: Pedro Antonio de Oliveira Machado
Editora Assistente: Alana Miranda de Gois
Organizadores: Vladimir Barros Aras; Andrey Borges de Mendonça; Walter Aranha Capanema; Carlos Bruno Ferreira da Silva e Marcos Antônio da Silva Costa
Capa: Pedro Lino
Projeto gráfico e diagramação: Eduardo Franco Dias
Revisão: Amélia Lopes Dias de Araújo, Lilian de Lima Falcão Braga e Rochelle Quito

A849c Associação Nacional dos Procuradores da República

Proteção de dados pessoais e investigação criminal /Associação Nacional dos Procuradores da República, 3ª Câmara de Coordenação e Revisão. Ministério Público Federal e Organizadores: Vladimir Barros Aras, Andrey Borges de Mendonça, Walter Aranha Capanema, Carlos Bruno Ferreira da Silva e Marcos Antônio da Silva Costa. — Brasília: ANPR, 2020.

593 p.

ISBN: 978-65-993102-0-1

1. Proteção de dados pessoais. 2. LGPD. 3. Investigação criminal. 4. Decreto 9.662/2019. 5. Decreto 10.046/2019. 6. Lei 13.709 (LGPD). 7. MPF. I. Vladimir Barros Aras (Coord). II. Andrey Borges de Mendonça (Org.). III. Walter Aranha Capanema (Org.). IV. Carlos Bruno Ferreira da Silva (Org.). V. Marcos Antônio da Silva Costa (Org.). I Título.

CDD: 340
CDU: 343.2

EDITORA ANPR
www.anpr.org.br
Editora / DF

SAF Sul Quadra 04, Conjunto C,
Bloco B, sala 113
Brasília – DF – CEP: 70050-900

Tel: (61) 3961-9025
administrativo@anpr.org.br

DIRETORIA DA ANPR

Fábio George Cruz da Nóbrega
Presidente

Ana Carolina Alves Araújo Roman
Vice-Presidente

Francisco Guilherme Vollstedt Bastos
Diretor Financeiro

Carlos Augusto da Silva Cazarré
Diretor de Assuntos Corporativos

Lea Batista de Oliveira Moreira Lima
Diretora de Assuntos Legislativos

Pedro Antonio de Oliveira Machado
Diretor Cultural

Patrick Salgado Martins
Diretor de Assuntos Jurídicos

Nathália Mariel Ferreira de Souza Pereira
Diretora de Eventos

Flávio Paixão de Moura Júnior
Diretor de Assuntos Institucionais

Hayssa Kyrie Medeiros Jardim
Diretora de Comunicação Social

Renan Paes Felix
Diretor-Secretário

Franklin Rodrigues da Costa
Diretor de Aposentados

MINISTÉRIO PÚBLICO FEDERAL
3ª CÂMARA DE COORDENAÇÃO E REVISÃO – CONSUMIDOR E ORDEM ECONÔMICA

Luiz Augusto Santos Lima
Subprocurador-Geral da República – PGR/Brasília
Coordenador

Alcides Martins
Subprocurador-Geral da República – PGR/Brasília
Membro titular

Brasilino Pereira dos Santos
Subprocurador-Geral da República – PGR/Brasília
Membro titular

Valquiria Oliveira Quixadá Nunes
Procuradora Regional da República – PRR-1ª Região/Distrito Federal
Membro suplente

Waldir Alves
Procurador Regional da República – PRR-4ª Região/Porto Alegre
Membro suplente

Lafayete Josue Petter
Procurador Regional da República – PRR-4ª Região/Porto Alegre
Membro suplente

SUMÁRIO

APRESENTAÇÃO

Em um programa televisivo de entrevistas, no final do ano de 2019, Yuval Harari, escritor e professor israelense de História da Universidade Hebraica de Jerusalém, registrava que o futuro dos dados é uma das questões políticas mais importantes da sociedade contemporânea, pois eles estão se tornando (ou já se tornaram?) o capital mais importante do mundo, equivalente à terra na antiguidade, quando a política era uma luta para controlar territórios, inclusive com a constatação de que, quando terras demais ficavam concentradas nas mãos de uma pessoa, ou de poucas pessoas, se estabelecia uma ditadura. Da mesma forma, na atualidade, uma ditadura pode se estabelecer com a concentração ou o controle de uma parte grande demais de fluxo de dados nas mãos de um governo, ou de uma ou poucas corporações.

É bem verdade que o avanço tecnológico nos legou benefícios de acesso amplo a informações e capacidade de expansão do conhecimento nunca antes imaginados, assim como nos proporcionou a possibilidade de conexão e comunicação que superaram as barreiras territoriais.

Entretanto, esse ambiente virtual, que nos possibilitou e continua a nos possibilitar essas conquistas, apresenta efeitos colaterais adversos, inclusive uma espécie de síndrome, denominada *Information Overload* (sobrecarga de informações), também conhecida como Síndrome da Fadiga por Informação (IFS). Tal síndrome atinge boa parte das pessoas, pois estamos expostos a uma quantidade de informações maior do que conseguimos assimilar, vivenciando cotidianamente um processo de escolha angustiante, face a muitas opções, desejos e estímulos a que somos submetidos nos ambientes virtuais, os quais se tornaram locais de frequência praticamente obrigatória e utilização intensa. Essa sobrecarga, com velocidade e numerosa troca de informações, pode anestesiar nossa capacidade de sentir, olhar, reparar e auscultar as pessoas; de trabalhar nossa empatia para com

os outros, de confiar em nossos sentidos e em nossas emoções.

Em uma passagem do livro *O fim do homem soviético*, Svetlana Aleksiévitch, ao entrevistar cidadãos da antiga União Soviética sobre o momento que vivenciavam com a abertura e a reestruturação econômica (*Perestroika*), em meados da década de 1980, colhe a seguinte definição: "a liberdade é a ausência de medo" e logo a seguir uma reflexão "uma pessoa que escolhe numa loja entre cem variedades de salame é mais livre do que a pessoa que escolhe entre dez variedades" (?).

De modo que vivemos em um mundo conectado, com nossas vidas sendo transformadas em dados, com intenso uso de redes sociais, transações bancárias, mensagens virtuais, aplicativos de *smartphones* para os mais variados tipos de serviços. Todas essas ações geram pegadas virtuais infinitas de navegação na internet, tudo se transformando em informações concretas de nosso cotidiano, escancarando nossos hábitos de consumo, nossas preferências de lazer, nossas posições ideológicas, o que gostamos ou não de fazer, de quem gostamos ou odiamos.

Essa farta coleta de dados (variadas informações a nosso respeito), especialmente facilitada pelo uso intensivo que fazemos das plataformas digitais e da navegação na internet, acaba gerando um mundo no qual as corporações ou os grandes detentores de dados nos conhecem melhor do que nós mesmos, com potencial para nos manipular e direcionar, ou influenciar fortemente nossos hábitos e pensamentos. Tal situação deve nos levar a pensar se hodiernamente nossas escolhas são realmente livres e autônomas como imaginamos. Ou seja, será que realmente temos liberdade de escolha?

A advertência reafirmada por Sócrates "conhece-te a ti mesmo" (para poder conhecer o mundo e a verdade), inscrita na entrada do Oráculo de Delfos, templo dedicado a Apolo, que na mitologia grega é o deus da luz, do sol, da verdade e da profecia, nunca foi tão atual. Dedicarmo-nos ao autoconhecimento e retomarmos o rumo de nossas vidas passa, portanto, a ser fundamental para a verdadeira liberdade,

para nos mantermos autênticos, pois as corporações e governos, com coletas intensas que realizam de nossos dados pessoais, sabem mais de nós do que nós mesmos, o que pode nos tornar presas fáceis de manipulações e direcionamentos.

Karl Marx, na obra *O 18 de brumário de Luís Bonaparte*, assevera que "Os homens fazem a sua própria história; contudo, não a fazem de livre e espontânea vontade, pois não são eles quem escolhem as circunstâncias sob as quais ela é feita, mas estas lhes foram transmitidas assim como se encontram".

Com esse *background*, também cabe meditar se a garantia constitucional de inviolabilidade da intimidade e da vida privada (art. 5º, X, da Constituição Federal) ainda existe, se é apenas uma questão de fé, ou nem isso.

O genial poeta brasileiro (e mineiro) Carlos Drummond de Andrade, em seu poema "Eu, Etiqueta", publicado no livro *O Corpo*, na década de 1980, no qual criticava a sociedade de consumo e massificada, legou-nos pílulas de reflexão que também servem no tema aqui tratado. Vaticinou ele:

> Com que inocência demito-me de ser
> eu que antes era e me sabia
> tão diverso de outros, tão mim-mesmo,
> ser pensante, sentinte e solidário
> com outros seres diversos e conscientes
> de sua humana, invencível condição.
> Agora sou anúncio,
> ora vulgar ora bizarro,
> em língua nacional ou em qualquer língua
> (qualquer, principalmente).
> E nisto me comprazo, tiro glória
> de minha anulação.
> (...)

Onde terei jogado fora
meu gosto e capacidade de escolher,
minhas idiossincrasias tão pessoais,
tão minhas que no rosto se espelhavam,
e cada gesto, cada olhar,
cada vinco da roupa resumia uma estética?
(...)
Já não me convém o título de homem.
Meu nome novo é coisa.
Eu sou a coisa, coisamente.

Vale lembrar que a coleta de nossos dados, assim como o uso e tratamento que se fizer deles, para além de interesses econômicos, tem real potencial de nos prejudicar, de gerar abuso do poder econômico, de violar direitos, de estabelecer discriminações vedadas no ordenamento jurídico. E mais, de colocar até mesmo em risco nossa liberdade e capacidade de escolher nossos destinos, cabendo lembrar, no ponto, do escândalo que foi protagonizado em 2016 pela *Cambridge Analytica*, empresa de análise de dados, que teria pago pelo acesso a informações e perfis de usuários do *Facebook*, usando tais dados para gerar um sistema que possibilitou predizer e influenciar as escolhas dos eleitores nas urnas, na consulta sobre o Brexit (referendo sobre a permanência do Reino Unido na União Europeia) e na eleição presidencial dos EUA, segundo investigação dos jornais *The Guardian* e *The New York Times*.

Assim, inevitavelmente, o tema ganhou a atenção global e levou governos e parlamentos a discutirem e aprovarem marcos legais a respeito, visando conferir proteção aos cidadãos e à própria democracia, disciplinando a coleta e o uso de dados, além de responsabilizando pelo uso abusivo que se fizer deles. Na Europa, formalizou-se o Regulamento Geral de Proteção de Dados Europeu – *General Data Protection Regulation* (GDPR), de 2016. Nos Estados Unidos, a matéria foi

tratada em legislações esparsas, como, por exemplo, *Health Insurance Portability and Accountability Act* (HIPAA), que trata do sigilo de dados médicos, e *Children's Online Privacy Protection Act* (COPPA), que disciplina e tutela os dados colhidos de crianças com menos de 13 anos, além de legislações estaduais. Na Austrália, a Lei de Privacidade de 1988 foi editada e baseada nos 13 Princípios Australianos de Privacidade, ou *Australian Privacy Principles* (APPs). No Brasil, mais especificamente, foram editados o Marco Civil da Internet (Lei n. 12.865/2014) e a Lei Geral de Proteção de Dados (Lei n. 13.709/2018).

Contudo, será que tais marcos legais foram construídos e estão estruturados para realmente proteger os cidadãos, para garantir que sejam preservadas as conquistas civilizatórias na área de direitos humanos? E como deve ser tratado o uso de dados pessoais para coleta de provas e informações no combate ao cibercrime, à macrocriminalidade ou mesmo de forma geral pelo sistema de justiça sancionador (penal ou administrativo), inclusive na área de cooperação jurídica internacional? Como devem ser exercidos os poderes da Autoridade Nacional de Proteção de Dados (ANPD)?

A Associação Nacional dos Procuradores da República, mantendo a sua tradição de estimular o debate e aprofundar a reflexão sobre temas atuais, candentes, complexos (e envolventes, como é o caso da proteção de dados), tem a honra de oferecer aos leitores essa coletânea de interessantes e instigantes artigos, com o objetivo principal de despertar e gerar curiosidade para novas pesquisas e aprofundamentos sobre essa seara do ordenamento jurídico, tão grave e que nos impacta a todos, em maior ou menor medida.

Boa leitura.

Brasília, dezembro de 2020.
Pedro Antonio de Oliveira Machado
Procurador da República
Diretor Cultural da ANPR

A TÍTULO DE INTRODUÇÃO: SEGURANÇA PÚBLICA E INVESTIGAÇÕES CRIMINAIS NA ERA DA PROTEÇÃO DE DADOS

Vladimir Aras[1]

1. INTRODUÇÃO

Que dados pessoais um viajante brasileiro disponibiliza a terceiros quando resolve passar férias na Europa? Após alguns minutos de reflexão, esse turista perceberá que, desde as pesquisas para sua viagem até a chegada ao seu hotel no destino, terá compartilhado com estranhos um conjunto impressionante de dados pessoais, incluindo seu *e-mail*, seu número de passaporte, os nomes de seu cônjuge ou companheiro e filhos e suas informações financeiras, além da localização, condição de saúde, imagem recolhida em postos de checagem nos aeroportos e fronteiras, nomes de acompanhantes em voos de companhias aéreas e de companheiros de hospedagem em hotéis.

Nossos dados pessoais estão no mundo e cada vez mais expostos, numa sociedade ávida por informações. Garantir a privacidade contra

---

1 Doutorando em Direito (UniCeub). Mestre em Direito Público (UPFE) com dissertação sobre a Convenção de Budapeste. Especialista MBA em Gestão Pública (FGV). Membro do Ministério Público brasileiro desde 1993, atualmente no cargo de procurador regional da República (MPF). Professor assistente de Processo Penal da UFBA. Ex-secretário de cooperação internacional da PGR (2013-2017). Membro do Grupo de Apoio em Cibercrimes do MPF. Foi membro da Comissão de Juristas (2019-2020) que preparou o anteprojeto da LGPD-Penal. Palestrante no Brasil e no exterior. Editor do *site* jurídico www.vladimiraras.blog.

ingerências ilegítimas e assegurar o livre fluxo de dados para atividades públicas e privadas legítimas foi o que motivou a União Europeia (UE) a aprovar em 2016 o Regulamento Geral sobre a Proteção de Dados, ou *General Data Protection Regulation* (GDPR), que entrou em vigor no dia 25 de maio de 2018.

Desenhado por Bruxelas para substituir a diretiva europeia sobre proteção de dados de 1995, com seus 99 artigos, o Regulamento (UE) n. 2016/679, conhecido internacionalmente por GDPR, pretende aperfeiçoar a proteção de dados pessoais na União Europeia, garantir sua livre circulação entre os Estados-membros do bloco e regular sua transferência a Estados terceiros (*non-EU*) e a organizações internacionais.

Aprovada simultaneamente, a Diretiva n. 2016/680, conhecida como Diretiva Policial, regula a proteção de dados no campo da segurança pública e da persecução criminal.

O GDPR, que foi convertido na lei uniforme europeia em matéria de proteção de dados e transposto para o ordenamento jurídico dos Estados-membros da União Europeia, implementa uma série de novos direitos para os cidadãos europeus ou ali residentes, aplicando-se a empresas sediadas no território da União Europeia e a pessoas jurídicas estabelecidas fora dele que ofereçam serviços ou façam negócios no bloco.

Esse marco normativo aprofunda dispositivos da Convenção do Conselho da Europa, de 1981, sobre o tratamento automatizado de dados pessoais, assim como da Carta de Direitos Fundamentais da União Europeia, de 2000, um dos instrumentos jurídicos vinculantes naquele bloco.

Considerando as intensas relações econômicas, culturais e jurídicas mantidas com o continente europeu, o Brasil não poderia ficar alheio a esse novo conjunto de direitos e obrigações. Em 2018, o Congresso Nacional aprovou a Lei Geral de Proteção de Dados (Lei n. 13.709/2018), fortemente inspirada no GDPR. Porém, o legislador brasileiro resolveu postergar a regulamentação da proteção de dados pessoais no âmbito da segurança pública e da persecução criminal, no que andou mal.

Deveríamos ter uma legislação apropriada desde a entrada em vigor da LGPD, mas não foi isso o que ocorreu. Construiu-se um sistema protetivo claudicante nesse aspecto e previu-se, no § 1º do art. 4º da LGPD, que em algum momento uma "legislação específica" regularia a matéria.

Creio que isso foi um erro de legística, uma vez que as sensíveis questões abordadas em segurança pública e persecução criminal mereceriam regulamentação simultânea às questões gerais, hoje abrangidas pela LGPD, num enfoque que garantisse a proteção de dados e, ao mesmo tempo, não criasse dificuldades insuperáveis para os órgãos de inteligência e de persecução criminal.

A legislação sobre proteção de dados pessoais abrange o tratamento de dados cadastrais (como a identificação do titular de um serviço), metadados (geolocalização, dias e horários de conexão, duração, provedores, equipamentos utilizados etc.) e dados de conteúdo (informações financeiras, tributárias, afiliações, diálogos em serviços de comunicação etc.), além de dados sensíveis, relativos à saúde e à orientação sexual, e dados biométricos, como imagens obtidas por câmeras de vigilância, imagens corporais colhidas por escâneres, impressões digitais, registros de íris e amostras de voz registradas por variados meios. Todas essas informações interessam ou podem interessar a investigações criminais e são cotidianamente utilizadas pela Polícia ou pelo Ministério Público nas mais variadas situações.

Na Sociedade da Informação, o mundo está cada vez mais conectado e imerso em dados. Vivemos numa *data-driven society*, isto é, numa sociedade orientada por dados de toda ordem. Um dos elementos-chave da globalização econômica é o incremento da interconexão do planeta, nos campos da comunicação, do comércio, do turismo, do entretenimento e da cultura. Nossos dados também estão espalhados pelo globo, na medida em que utilizamos serviços de empresas locais, nacionais ou transnacionais e também na medida em que nos sujeitamos a meios de controle e fiscalização pelos Estados. Para prover segurança pública e justiça criminal,

na proteção de direitos das vítimas e de toda a sociedade, a Polícia e o Ministério Público também dependem do tratamento de dados pessoais.

2. AS NOVAS LEIS DE PROTEÇÃO DE DADOS PESSOAIS

Quando uma empresa brasileira oferece bens ou serviços no mercado da União Europeia, deve submeter-se ao regulamento de proteção de dados pessoais ali vigente. Suas atividades comerciais podem ser gravemente impactadas se não se adequarem ao GDPR e às leis de transposição, ficando suscetíveis a pesadas multas. Relações no comércio exterior também estão nesse âmbito. Daí a importância da *compliance* ou conformidade digital, o que torna importantíssima a atuação dos gerentes (encarregados) de proteção de dados pessoais e dos controladores desses dados, assim como das agências nacionais de proteção.

Por outro lado, cidadãos brasileiros, especialmente os residentes na Europa, que adquiram bens ou utilizem serviços de empresas sediadas na União Europeia ou que se valham de provedores de conexão ou de aplicações de um dos 27 países da União estão protegidos pelo novo marco regulatório, que se baseia em dois princípios fundamentais: o consentimento expresso do titular e o respeito à finalidade de uso dos dados. Além disso, esses novos regimes preveem o direito de acesso aos dados, de retificação, de supressão, assim como o direito à informação em caso de vazamentos, entre outras faculdades previstas em lei.

Vários serviços globais de comunicação, inúmeras redes sociais de alcance mundial, serviços internacionais de distribuição de músicas, séries, filmes e outros conteúdos para entretenimento, plataformas de comercialização de livros e mercadorias diversas, redes de hotelaria, de aluguéis de veículos, de transporte e de vendas de passagens aéreas têm suas sedes no exterior, grande parte na Europa. Muitos dos servidores informáticos que viabilizam o funcionamento desses serviços também

são mantidos fora do Brasil, não raro nos Estados Unidos da América (EUA) ou em países europeus. Além disso, os provedores utilizam *Content Delivery Networks* (CDN), ou redes de distribuição de conteúdo que armazenam cópias de outros *sites* em memória para entrega mais rápida de informações aos visitantes da página que utilizam o serviço, de acordo com suas localizações geográficas, reduzindo-se o tempo de latência.

Em suma, nossos dados são sempre compartilhados com terceiros e estão espalhados em inúmeras jurisdições. Não sabemos exatamente onde eles estão. No máximo, saberemos onde estão as empresas que controlam a custódia desses dados.

Quando um cidadão brasileiro ou um estrangeiro residente no Brasil utiliza um desses serviços, seus dados cadastrais, seus metadados (incluindo elementos de geolocalização) e dados sensíveis são compartilhados com a pessoa jurídica no exterior e trafegam por servidores de internet noutras praças globais. A compra de livros, a assinatura de revistas, o aluguel de conteúdo audiovisual, a contratação de *streaming*, a aquisição de músicas, bilhetes aéreos, a chamada de um veículo de transporte por aplicativo e a reserva de hotéis pela internet revelam mais do que os nomes, endereços e dados de cartão de crédito dos compradores; revelam suas opções ideológicas, religiosas, culturais, afiliações a entidades políticas e sociais, os lugares para onde viajam e onde se hospedam, os nomes das pessoas com quem viajam ou com quem vivem, e os locais onde trabalham, onde moram e que frequentam.

No ciberespaço, a aceitação de termos de uso de aplicações de internet, que ninguém lê, ou a concretização de um simples negócio *on-line* leva os usuários, os quais são também consumidores, a revelar seus gostos, modo de pensar, vínculos e orientações. Isso permite que os detentores das informações reconstruam o perfil do usuário ou tracem uma sombra em grande parte coincidente com a *pessoa que se é*, com invasão de esferas de segredo que se relacionam a direitos da personalidade, muito relevantes.

3. OS NOVOS DIREITOS DIGITAIS

A proteção a dados pessoais na sociedade informatizada é uma preocupação que, no plano convencional, remonta, pelo menos, a 1981, quando foi concluída a Convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal (ETS 108). Em 1995, a União Europeia aprovou sua principal Diretiva sobre Proteção de Dados (95/46/CE). Porém, em virtude do novo mundo digital criado pela internet, em 2016, o Parlamento e o Conselho adotaram o GDPR, que, como vimos, entrou em vigor na União Europeia, mantendo-se a vigência da ETS 108 no âmbito do Conselho da Europa. Concomitantemente, outros países seguiram o mesmo caminho, o Brasil inclusive.

Quando entrou em vigor em 2014, o Marco Civil da Internet (MCI) – Lei n. 12.965/2014 – tornou mais claros os direitos dos usuários da internet no Brasil, entre eles a inviolabilidade e o sigilo de comunicações telemáticas e a confidencialidade dos registros de conexão e acesso.

O MCI também deu maior densidade ao direito à remoção de conteúdo pessoalmente ofensivo. No entanto, ali se sentiu a falta de uma abordagem criminal na utilização de aplicações de internet. Ou seja, no marco civil esteve ausente a questão penal.[2]

A União Europeia foi mais prudente. O GDPR é minucioso. Atribui novos direitos a cidadãos residentes na União Europeia ou amplia outros já existentes, aperfeiçoando as proteções que vêm sendo construídas desde, pelo menos, 1981 – quando foi concluída a Convenção 108 do Conselho da Europa – e desde 1995 – ano em que passou a valer

2 ARAS, Vladimir. A questão penal no marco civil. *Blog do Vlad*, 2011. Disponível em: https://blogdovladimir.files.wordpress.com/2010/01/artigo-marco-civil-da-internet.pdf. Acesso em: 13 dez. 2020.

a Diretiva 95/46/EC, no seio da União. Ao mesmo tempo, adotou-se um regulamento para a persecução criminal, a já mencionada Diretiva Policial, de 2016.

Como não poderia deixar de ser, o GDPR assegura aos cidadãos o direito à informação sobre o processamento de seus dados pessoais, sobre o local do processamento desses dados e sobre sua finalidade; protege o direito de acesso aos próprios dados pessoais; garante o direito de correção de dados incorretos, incompletos ou inexatos; e o direito de objeção ao processamento desses dados.

O Regulamento também prevê o direito de apagamento de dados pessoais cujo processamento não seja mais necessário para a finalidade inicialmente prevista ou cujo processamento tenha-se tornado ilegítimo. O direito de ser esquecido, que também ali está, é um dos que apresenta mais complexa proteção na sociedade digital.

Há também o direito de objeção ao uso de dados pessoais para fins de propaganda comercial e o inovador direito de portabilidade dos dados pessoais de um controlador a outro. O titular pode exigir que seus dados pessoais lhe sejam entregues em formato eletrônico processável.

O GDPR prevê que decisões sobre o processamento de dados pessoais sejam tomadas por seres humanos, não apenas por computadores, o que assegura alguma espécie de intervenção humana no tratamento de tais informações, que têm impacto no acesso a direitos perante o Estado e a iniciativa privada.

Para aumentar a proteção da privacidade, parte-se do pressuposto de que os sistemas de processamento de dados devem incorporar, desde sua programação, a garantia da privacidade como regra geral fundamental (*privacy by design*), como mecanismo nativo, e assegura o direito de imediata notificação quanto ao vazamento de dados pessoais, para impedir ou mitigar lesões à vida privada e a interesses econômicos.

Com o fim de reduzir os impactos sobre a privacidade, inclusive em caso de vazamentos, o GDPR estabelece o conceito de *data mi-*

nimisation, segundo o qual os controladores só devem usar os dados pessoais absolutamente necessários para sua atividade. Em harmonia com o princípio da necessidade, o acesso a tais dados deve ser restrito àquelas pessoas que realmente estejam envolvidas em seu tratamento.

Por fim, o GDPR exige que as pessoas jurídicas controladoras ou as empresas responsáveis pelo processamento de dados pessoais contratem funcionários encarregados da proteção de dados. Os *data protection officers* (DPO) devem ser contratados por empresas que controlem ou processem dados pessoais em larga escala ou que lidem com categorias especiais de dados pessoais. Tais encarregados, que podem ser funcionários ou um serviço terceirizado, precisam ser especialistas em proteção de dados e devem reportar suas atividades diretamente ao estamento gerencial superior da pessoa jurídica, sem se envolverem em outras atividades que possam importar conflito de interesses com suas obrigações. Para isso, devem ter acesso aos meios materiais e recursos humanos necessários ao desempenho de suas atividades.

Esses direitos e muitos desses deveres também foram estabelecidos pela LGPD, de 2018, o que exige o desenvolvimento de uma nova cultura de privacidade e proteção de dados no Brasil.

4. A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Uma pessoa jurídica constituída nas Ilhas Seicheles, no Oceano Índico, hospeda um *site* na Suécia e vende dados sigilosos de contribuintes do Brasil. Este é o cenário do processamento ilícito de dados pessoais na internet. Seu intuito é o lucro, em detrimento da privacidade.

Em 2015, entrou no ar o *site Tudo sobre Todos*, que publicava e comercializava dados de contribuintes brasileiros, sem consentimento expresso de seus titulares, um princípio importante em proteção de dados, especialmente diante da constante monetização de tais informações pessoais.

Como proteger esses dados num cenário em que estão envolvidas, às vezes, duas ou mais jurisdições estrangeiras? Como protegê-los diante da voracidade do Estado e das grandes corporações, especialmente as transnacionais?

Dados pessoais como esses podem ser úteis para vários cibercrimes, como estelionato e sequestro, que são consumados mediante o uso de técnicas de *phishing*, engenharia social e *identity theft* (falsa identidade). Podem servir para extorsão, perseguição obsessiva (*stalking*) e crimes contra a honra, mediante *doxxing*. Podem ser usados para uma infinidade de atos ilegítimos. Por outro lado, o acesso a dados pessoais pelas chamadas *law enforcement agencies* servirá para a elucidação desses mesmos crimes e a prevenção de delitos violentos, inclusive o terrorismo, ou extremamente repugnantes, como a violência sexual contra menores na internet e por meio dela.

É evidente que a proteção de dados dialoga com os direitos humanos em geral e com os da personalidade em particular, entre eles o de não ser conhecido, o de manter os segredos da vida privada e o de ser esquecido. Relaciona-se, também, com a proteção do patrimônio, pois dados são um *asset* valioso no mercado, tanto para empresas legítimas quanto para criminosos em geral. Ademais, proteger dados pessoais significa impedir ou minorar a possibilidade de perseguições do Estado a pessoas por motivos ligados à religião, política, origem nacional ou orientação sexual, por exemplo.

Com a entrada em vigor da LGPD em 2020, o Brasil adotou sua primeira lei geral de proteção de dados. No entanto, já havia um razoável nível de proteção aos direitos de privacidade em nossa jurisdição, a começar pelo art. 5º, X, da Constituição, que considera invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando-se o direito à indenização pelo dano material ou moral decorrente de sua violação. O inciso XII do mesmo artigo também garante a inviolabilidade do sigilo postal, de dados e das comunicações telefônicas,

salvo por ordem judicial para fins de investigação criminal ou instrução processual penal, na forma prevista na Lei n. 9.296/1996.

O art. 5º, LXXII, da Constituição ainda prevê o *habeas data* como mecanismo processual destinado a assegurar o conhecimento de informações e dados pessoais constantes de bases de dados públicas ou de caráter público, assim como o direito de retificação.

Por sua vez, o art. 11.2 da Convenção Americana de Direitos Humanos, que entrou em vigor no Brasil em 1992, prevê que ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência.

Nessa linha, o art. 43 do Código de Defesa do Consumidor (Lei n. 8.078/1990), a Lei do *Habeas Data* (Lei n. 9.507/1997), os arts. 20 e 21 do Código Civil (Lei n. 11.406/2002), os arts. 1º a 7º-B da Lei de Identificação Criminal (Lei n. 12.037/2009), o art. 3º, § 3º, da Lei do Cadastro Positivo (Lei n. 12.414/2011), o art. 31 da Lei de Acesso à Informação (Lei n. 12.527/2011) e os arts. 3º, 7º, 10, 11 e 16 do Marco Civil da Internet (Lei n. 12.965/2014), entre outros dispositivos – como os da Lei n. 7.210/1984, da Lei n. 9.613/1998, da Lei n. 12.850/2013 e do CPP, especialmente após a Lei n. 13.344/2016 –, conferem certo nível de proteção a dados pessoais no Brasil e alguns direitos a seus titulares, diante de órgãos públicos ou de pessoas jurídicas de direito privado que os detenham ou sejam encarregados do seu tratamento, inclusive para fins penais. Porém, o marco legal brasileiro ainda é insuficiente para regular por inteiro a realidade jurídica dessa temática em nosso país porque falta uma lei que trate da proteção de dados para fins penais em geral.

Para minorar o problema, a Câmara dos Deputados reuniu uma comissão de juristas encarregada de produzir um texto para cumprir o mandado expresso contido no § 1º do art. 4º da LGPD e para harmonizar o cenário jurídico brasileiro ao exigente quadro europeu, que reclama a existência de um nível de proteção adequado nos países com os quais a União, seus Estados-partes e suas empresas negociam e cooperam.

5. A QUESTÃO CRIMINAL NA PROTEÇÃO DE DADOS PESSOAIS

Quando pensamos na perspectiva penal relativa aos procedimentos de coleta, guarda, processamento, utilização e disseminação ou transferência de dados pessoais, temos de levar em conta o titular dos dados como autor de uma infração ou como vítima dela. Também devemos considerar que numa investigação criminal dados de testemunhas, peritos ou mesmo de terceiros, sem nenhuma relação com o fato a ser provado poderão ser submetidos a ingerência do Estado, especialmente no curso da investigação criminal.

O ordenamento jurídico brasileiro não ignora *normas* de proteção de dados no campo da persecução criminal. Basta que recordemos a existência da Lei de Interceptação Telefônica (Lei n. 9.296/1996), que regula as escutas telefônicas e telemáticas; da Lei da Identificação Criminal (Lei n. 12.037/2009), que cuida do registro de dados pessoais, inclusive perfis genéticos, para uso em investigações criminais; os arts. 17-B e 17-E da Lei de Lavagem de Dinheiro (Lei n. 9.613/1998) sobre acesso a dados cadastrais; os arts. 15 a 17 da Lei do Crime Organizado (Lei n. 12.850/2013); e os arts. 13-A e 13-B do Código de Processo Penal (CPP), que disciplinam o acesso a dados cadastrais e metadados para uso em investigações criminais sobre tráfico de pessoas.

Tampouco se pode ignorar que o Marco Civil da Internet (MCI), o qual, como escrevi alhures, tem uma claríssima questão penal nele embutida, sobretudo como ferramenta útil para a apuração de cibercrimes e como fundamento para modernas medidas de investigação, como o *geofence* (ou *geofencing*).[3]

---

3 ARAS, Vladimir. *Geofencing* como técnica de investigação criminal. *Blog do Vlad*, 2020. Disponível em: https://vladimiraras.blog/2020/08/27/geofencing-como-tecnica-de-investigacao-criminal/. Acesso em: 13 dez. 2020.

Evidentemente, a expansão da sociedade da informação também facilitou a globalização da criminalidade, notadamente no campo dos crimes digitais. O ciberespaço criado pela internet não conhece fronteiras e tornou-se um ambiente ideal para a prática de crimes informáticos a distância, como aqueles que têm como alvo dados pessoais em geral ou que se valem dessas informações para a prática de outras condutas ilícitas.

Em razão da característica transnacional da internet, a promoção da defesa dos direitos de personalidade (inclusive da privacidade) torna-se mais complexa, pois depende da interação de diferentes jurisdições soberanas, exigindo o uso de ferramentas de cooperação jurídica internacional no plano cível e no criminal.

Nesse sentido, as normas de proteção de dados pessoais devem aplicar-se também ao Estado quando coleta, manipula e difunde dados pessoais de investigados, suspeitos, réus, vítimas, testemunhas, peritos, autoridades e funcionários que atuam na persecução criminal e de terceiros eventualmente alcançados por medidas de apuração. Investigações criminais e medidas de segurança pública são atividades estatais que interferem rotineiramente na vida dos cidadãos, tornando-se relevante a perspectiva da privacidade.

Por outro lado, é preciso regular adequadamente a transferência internacional de dados para atividades empresariais e para a cooperação internacional nos campos policial e judicial, temática essencial num mundo hiperconectado.

Como em tudo na vida, a virtude está no plano médio. Tais proteções não devem inviabilizar os métodos operacionais do Estado na elucidação de crimes. Cada vez mais dependemos de meios tecnológicos de investigação para a descoberta de crimes, especialmente para a determinação de autoria. A *internet das coisas* incrementa a dependência de dados que acomete os órgãos de persecução criminal. A internet exige que a tecnologia seja empregada em larga escala na investigação penal. A sociedade de massa demanda o tratamento de grandes conjuntos de

dados por órgãos de inteligência e análise nas instâncias estatais. As finalidades desses tratamentos são legítimas e essenciais às sociedades democráticas, diante de ameaças como a criminalidade organizada e o terrorismo, mas também em face de crimes graves.

6. TRANSFERÊNCIA DE DADOS PESSOAIS E COOPERAÇÃO INTERNACIONAL

No âmbito da cooperação policial internacional, a Constituição da Interpol (1956) e as Regras sobre o Processamento de Dados para fins de Cooperação Policial Internacional (a começar dos seus arts. 2º e 3º) têm permitido a interação entre a Polícia Federal e seus congêneres nos demais Estados-membros da Interpol, para possibilitar as emissões das várias difusões (*notices* ou *alertas*) para captura de foragidos, localização de pessoas desaparecidas, identificação de cadáveres, rastreamento de indivíduos suspeitos e o enfrentamento do tráfico humano, do tráfico de drogas, do terrorismo e da cibercriminalidade.

Porém, atualmente, o Estado brasileiro enfrenta dificuldades para obter acesso a dados de cidadãos europeus ou de estrangeiros residentes na União Europeia, quando tais dados são necessários à segurança pública, ao controle migratório ou à persecução criminal no Brasil. Por exemplo, a necessária articulação da Polícia Federal com a Europol exigiu a formalização de um acordo específico – promulgado pelo Decreto n. 10.364/2020 – entre o Brasil e o Serviço Europeu de Polícia, para atividades de inteligência estratégica, mas sem a possibilidade de transferência de dados pessoais, conforme seu art. 1º.

Além disso, a maior integração entre o Ministério Público e a Eurojust, um dos órgãos supranacionais da União Europeia, depende de um marco normativo brasileiro. A Eurojust tem, desde 2005, suas Regras para o Processamento e Proteção de Dados Pessoais. Tal integração transnacional, crucial para o enfrentamento de várias formas de crimi-

nalidade, só poderá ocorrer quando houver no Brasil um nível adequado de proteção, que só virá com uma lei geral de proteção de dados em matéria penal, com os requisitos mínimos, aceitos por aquela comunidade política, o que inclui uma autoridade nacional de proteção de dados independente.

Com a entrada em vigor do Regulamento Geral da União Europeia e da Diretiva Policial de 2016, o Brasil ficou mais atrás neste campo e essa necessidade será ainda mais premente a cada dia, tornando-se imprescindível adequar nossa legislação ao marco europeu e às boas práticas globais.

Note-se que países vizinhos, como a Argentina e o Uruguai, já contam com uma legislação abrangente de proteção de dados, formada por diplomas nacionais e atos internacionais. Esses países são partes da Convenção 108, de 1981, do Conselho da Europa. É de se lembrar que Chile, México e Argentina também são Estados-partes da Convenção de Budapeste, de 2001, sobre cibercriminalidade, o que lhes confere uma posição privilegiada no relacionamento com mais de sessenta países vinculados a esses dois regimes.

De acordo com o GDPR, a transferência de dados pessoais para um país terceiro ou uma organização internacional só ocorrerá se a Comissão Europeia – o órgão executivo da UE, com sede em Bruxelas – decidir que o Estado ou a pessoa jurídica de direito internacional público destinatária assegura um nível de proteção adequado. Tal adequação é avaliada pela Comissão com base nos seguintes elementos:

a) o primado do Estado de Direito e o respeito aos direitos humanos, inclusive em matéria de segurança pública, direito penal e segurança nacional, no destinatário;
b) a existência e o efetivo funcionamento de uma ou mais autoridades de controle de dados independente, com competência para assegurar o cumprimento das regras de proteção de dados;
c) o cumprimento de compromissos internacionais assumidos pelo

Estado terceiro ou pela organização internacional, como partes de convenções ou tratados ou organismos multilaterais, em relação à proteção de dados pessoais.

O exame do marco europeu expõe a insuficiência da legislação brasileira no tocante à proteção de dados na cooperação jurídica internacional, sobretudo em matéria penal, especialmente se também considerada a Diretiva (UE) n. 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Os arts. 35 a 40 da Diretiva 680 regulam a transferência internacional de dados de países da União Europeia a Estados terceiros, como o Brasil e exigem uma série de requisitos para sua execução.

Países não europeus prepararam-se para esse novo salto na era da globalização digital, ao menos no campo do comércio exterior. Em 2016 entrou em vigor o *EU-US Privacy Shield*, acordo entre a União Europeia e os Estados Unidos, que estabelece o regime de proteção a dados transferidos daquela a estes. Tal arranjo pretendeu substituir o acordo *Safe Harbor*, declarado inválido pelo Tribunal de Justiça da União Europeia (TJUE) em 2015.[4] Em 2020, a mesma corte, com sede em Luxemburgo, invalidou o esquema euro-americano *Privacy Shield*[5], de transferência internacional de dados. Tais decisões, proferidas nos casos *Schrems I e II*, tiveram como fundamento, entre outras razões, o risco de tredestinação de dados de cidadãos europeus para fins criminais

4 TJUE. *Acórdão no Processo C-362/14, de 6 de outubro de 2015*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A62014CJ0362. Acesso em: 13 dez. 2020.

5 Escudo de Proteção da Privacidade.

na jurisdição euamericana e a deficiência do direito de acesso à Justiça no Estado de destino.[6]

7. CONCLUSÃO

Em suma, é imperioso que o Congresso Nacional busque simetria com o GDPR e a Diretiva Policial europeia, de 2016 (sem excessos exóticos), sem o que será muito difícil a realização de atividades corriqueiras de persecução criminal no Brasil e a coordenação das autoridades nacionais de persecução criminal com órgãos europeus e de outros países na luta contra a criminalidade grave, sobretudo a transnacional organizada. É também crucial que o governo brasileiro providencie a adesão às convenções 108 e 181 do Conselho da Europa, tal como já fez em relação à Convenção 185 (Budapeste). Esse é o patamar da harmonização entre a proteção de dados e o seu livre fluxo em ambientes de adequada salvaguarda, e a segurança no ciberespaço.

Sob outra óptica, no ambiente dos direitos civis, a privacidade e a intimidade serão cada vez mais expostas e ameaçadas na sociedade digital. A possibilidade de processamento e de manipulação de dados, áudios e imagens e outros dados biométricos, para o bem e para o mal, coloca em choque os direitos de personalidade e o direito à segurança, especialmente diante dos usos da inteligência artificial para produção de vídeos e imagens com registros de fatos ou eventos que jamais existiram.

Os direitos à privacidade, à liberdade, à segurança, à integridade e à vida são indivisíveis e devem ser mantidos em constante equilíbrio

---

6 TJUE. *Acórdão no Processo C-311/18, de 16 de julho de 2020*. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091pt.pdf. Acesso em: 13 dez. 2020.

em toda a parte para que a privacidade absoluta não seja escudo para crimes graves, e de modo que a necessidade de prover segurança para a sociedade não leve ao sacrifício de direitos fundamentais, entre eles a própria privacidade.

Como vimos, o tema em tela apresenta inúmeros desafios, exige a ponderação de diversos direitos em jogo e reclama prudência do legislador, a partir de um amplo debate com todos os *stakeholders*, tanto na sociedade civil quanto na academia e no Estado.

É com esse propósito que a ANPR traz uma contribuição para o estudo da proteção de dados no Brasil. Nesta coletânea, procuradores, procuradoras, advogados e advogadas, professores e outros profissionais brasileiros e uma estrangeira apresentam seus estudos sobre o marco normativo de proteção de dados, abordando questões inerentes à investigação criminal e à cooperação internacional e também ao enfrentamento à cibercriminalidade.

O leitor encontrará artigos sobre temas gerais da legislação de proteção de dados, sobre as instituições encarregadas dessa tarefa, assim como sobre os novos direitos e sobre algumas das formas de tratamentos de dados mais problemáticas, como a transferência internacional no contexto da luta contra a criminalidade. Aqui também estão textos sobre medidas específicas de investigação criminal que são *dado-dependentes*, como a elaboração de perfis genéticos, o reconhecimento facial, o acesso a provas mantidas em dispositivos móveis, o compartilhamento de informações obtidas em investigações criminais, o tratamento de dados pessoais em massa, e o instigante tema do *contact tracing* na investigação criminal. A coletânea traz ainda capítulos sobre questões mais gerais da era da informação, como a governança da internet, a criminalidade informática e o uso da tecnologia para policiamento preventivo contra a pornografia infantil.

Tive o prazer de organizar esta obra na companhia do professor Walter Capanema, um dos maiores especialistas em proteção de dados

do País, e do professor Andrey Borges de Mendonça, um dos mais jovens e brilhantes processualistas brasileiros. Agradeço ao procurador da República Pedro Antonio de Oliveira Machado, diretor cultural da ANPR, que chefiou a equipe editorial e apresenta a obra num texto vibrante e rico. Agradeço também aos procuradores da República Carlos Bruno Ferreira da Silva e Marcos Antônio da Silva Costa, que compuseram a comissão encarregada da seleção dos textos, que passaram por um rigoroso exame às cegas, para inclusão nesta coletânea. Merece também nosso agradecimento a equipe técnica da ANPR, cabendo nominar a assessora cultural Alana Miranda de Góis, muito cuidadosa na preparação do livro que o leitor tem às mãos. Por fim, agradeço ao presidente da ANPR, Fábio George Cruz da Nóbrega, pelo seu empenho em manter a entidade de representação dos procuradores da República engajada na discussão dos mais relevantes temas da atualidade. Oxalá a boa leitura que a ANPR oferece nesta obra contribua para o debate sobre a proteção de dados no Brasil.

DADOS PESSOAIS, CONSENTIMENTO E PRIVACIDADE: CONSIDERAÇÕES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS

Tarcísio Henriques[1]

RESUMO

O desenvolvimento da tecnologia tornou necessária a regulamentação precisa da utilização dos dados e isso é um grande desafio para todos os ordenamentos jurídicos, não por outro motivo, pela própria flexibilização do que deve ser compreendido como privado e assunto excluído da "arena pública", neste período de transição de conceitos nas sociedades em que vivemos. Em torno desse problema, tratamos neste artigo da previsão de consentimento do titular dos dados e dos aspectos fundamentais da disciplina da proteção de dados pessoais, ou seja, o respeito à privacidade, a inviolabilidade da intimidade, da honra e da imagem, os direitos humanos, além da dignidade e o exercício da cidadania pelas pessoas naturais.

---

1 Procurador da República em Minas Gerais. Mestre em direito ambiental pela Escola Superior Dom Helder Câmara. Doutor em direito público pela PUCMINAS. Professor da Escola Superior Dom Helder Câmara e do IBMEC-BH.

Palavras-chave: Informações pessoais e consentimento. Lei Geral de Proteção de Dados.

ABSTRACT

The development of technology has made it necessary to precisely regulate the use of data and this is a great challenge for all legal systems, not least because of the flexibility of what should be understood as private and a subject excluded from the "public arena", in this period of transition of concepts in the societies in which we live. Around this problem, this article deals with the prediction of consent of the data subject and the fundamental aspects of the discipline of personal data protection, that is, respect for privacy, the inviolability of intimacy, honor and image, human rights , in addition to dignity and the exercise of citizenship by natural persons.

Keywords: Personal information and consent. General Data Protection Law.

1. INTRODUÇÃO

Ao desenvolver os aspectos do que classifica como "aventuras da privacidade" em nosso mundo moderno, Bauman (2011, p. 35) nos apresenta as considerações do sociólogo Alain Ehrenberg sobre o evento social que pode ser considerado "a data de nascimento da revolução cultural moderna (ou pelo menos de seu ramo francês) que nos introduziu na era em que vivemos". Ainda segundo Bauman (2011, p. 35-36),

> Ehrenberg escolher uma noite de quarta-feira de outono, na década de 1980, quando certa Vivienne declarou durante um programa muito

> popular de entrevistas, pela televisão, na frente de milhões de telespectadores, que a maldita ejaculação precoce de seu marido, Michel, lhe impedira de ter um só orgasmo durante toda sua vida conjugal.
>
> O que houve de tão revolucionário (...) na declaração (...)? Dois fatos: primeiro, tornar público um tipo de informação que até então era considerado a quintessência da ordem do privado, até mesmo seu epônimo; segundo, usar a arena pública para expressar e discutir um assunto de interesse eminentemente privado.[2]

O evento televisivo colocou em xeque tanto o conceito de privacidade, de informações pessoais que compartilhamos ou queremos compartilhar, quanto o de privado. Além disso, apresentou à discussão o sentido atribuído às questões que são (ou deveriam ser, pelo menos) analisadas na "arena pública". A partir dessa pretensa "revolução", que Bauman define como sendo de natureza "cultural" e de hábitos sociais, chegamos ao ponto em que estamos.

Para compreendermos adequadamente o sentido jurídico das determinações da nova lei brasileira de proteção de dados, é necessário voltarmos às precisas considerações do aludido autor, agora no contexto

---

2 Ao discutir tais questões, Bauman (2011, p. 36) apresenta ainda o significado que a *Wikipédia* (para ele "*site* da internet que reflete de maneira meticulosa e com frequência breve, tudo que a opinião média considera verdadeiro sobre um assunto") atribuía ao termo "privacidade" em 8 de março de 2009: "capacidade de uma pessoa ou grupo de controlar a exposição e a disponibilidade de informações a seu respeito, e dessa forma revelar-se de maneira seletiva. Ela se relaciona às vezes com a capacidade de existir anonimamente na sociedade, com o desejo de não ser notado ou identificado na esfera pública. Quando algo pertence a uma pessoa de modo privado, isso em geral significa que há nela algo que se considera inerentemente especial ou pessoal (...). A privacidade pode ser entendida como um aspecto da segurança – pelo qual se torna clara, em geral, a equivalência entre os interesses de um grupo e os de outro grupo."

dos novos hábitos de liberação de informações e de dados nas "redes sociais". Em *Vida para consumo*, apresentando exemplos do que chama de "hábitos altamente mutáveis de nossa sociedade cada vez mais 'plugada'", Bauman (2008, p. 7-8) aduz:

> Em 2 de março de 2006, o *Guardian* anunciou que "nos 12 últimos meses as 'redes sociais' deixaram de ser o próximo grande sucesso para se transformarem no sucesso do momento". (...). Uma vez que finquem seus pés numa escola ou numa comunidade, seja ele física ou eletrônica, os sites de "rede social" se espalham à velocidade de uma "infecção virulenta ao extremo". Com muita rapidez, deixaram de ser apenas uma opção entre muitas para se tornarem o endereço *default* de um número crescente de jovens, homens e mulheres. Obviamente, os inventores e promotores das redes eletrônicas tocaram uma corda sensível – ou num nervo exposto e tenso que há muito esperava o tipo certo de estímulo. Eles podem ter motivos para se vangloriar de terem satisfeito uma necessidade real, generalizada e urgente. (...). "No cerne das redes sociais está o intercâmbio de informações pessoais". Os usuários ficam felizes por "revelarem detalhes íntimos de suas vidas pessoais", "fornecem informações precisas" e "compartilham fotografias".

Diante disso, podemos sustentar que o desenvolvimento da tecnologia tornou necessária a regulamentação precisa da utilização dos dados, ainda que tais disposições existam para nos proteger de nós mesmos. Contudo, esse desafio é enorme para todos os ordenamentos jurídicos, não por outro motivo, pela própria flexibilização do que deve ser compreendido como privado e assunto excluído da "arena pública", neste período de transição de conceitos em que vivemos.

2. O PÚBLICO E O PRIVADO

Como visto, o conteúdo do que se discute em espaços públicos é objeto de muita confusão, o que exige, como sugere Sampaio, "algumas atualizações de conceitos". Nas precisas considerações do autor,

> Embora estejamos em tempo de transição, confluem-se – paradoxalmente, em suas divergências – certa publicização do privado e intensa privatização do público. (...). Nenhuma abordagem sobre intimidade e vida privada pode fugir da distinção das esferas pública e privada, porém, contemporaneamente, sob um discurso muito mais complexo do que em outros tempos, dada a multiplicidade ou variedade dos eventos de nossos dias.
>
> Recolhemos da liberdade um desdobramento imediato, referível à própria existência humana, uma autodeterminação em matéria de sexualidade, de vida familiar, de tempo de vida e morte, de informações pessoais, autodefinidora do caráter identificador da "pessoa", ganhe esta o matiz que quiser e puder. A esse desdobramento, nominamos vida privada. (SAMPAIO, 1998, p. 27)

Ao lado deste "desdobramento imediato" como conteúdo específico da privacidade e do texto constante do inciso X do art. 5º da Constituição Federal de 1988[3], Sampaio sustenta ou "propõe", como diz, a seguinte distinção:

> vida privada como autodeterminação da existência própria, autodefinição pessoal, sexual e familiar, intimidade como um de seus aspectos,

3 O mencionado dispositivo tem a seguinte redação: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."

> relativo a informações pessoais: seu controle em diversos instantes: da coleta ao uso, na perspectiva tensa da interação social, comunicativa, e do recolhimento, aí sim, do recato e da solidão. (SAMPAIO, 1998, p. 28-29)

Eis, então, o que se deve buscar com uma regulamentação da atividade de manipulação de dados pessoais: "seu controle em diversos instantes: da coleta ao uso" (SAMPAIO, 1998, p. 29), mesmo nos casos em que não seja do interesse do cidadão o mencionado controle.

2.1 INFORMAÇÕES PESSOAIS E CONSENTIMENTO

Definidos os aspectos constitucionais contidos no inciso X do art. 5º da Constituição, é importante enfrentarmos a necessidade de controle e o papel da vontade, ou do consentimento, do titular dos dados.

Sobre o primeiro ponto, Sampaio aponta a condição de "senhorio" do titular sobre seus dados. Segundo ele,

> (...) o homem tem um direito a controlar informação sobre ele mesmo, decidindo quando, como, em que extensão e para que finalidade tais informações serão conhecidas pelos outros.
>
> Em conceito envolve uma "senhoria" sobre todo o processo informativo, desde a sua obtenção por outros até seu uso ulterior. Diz-se assim que o direito à intimidade concede um poder ao indivíduo para controlar a circulação de informações a seu respeito. (SAMPAIO, 1998, p. 368-369)

No que se refere ao papel da vontade do titular, o autor sustenta que

> [a] autorização ou o consentimento do interessado retira o caráter ilícito da obtenção ou divulgação de informação da vida privada. Isso

> equivale dizer que a revelação voluntária, sendo forma de exercício do controle informacional, significa a "perda da privacidade", conquanto não percuta no âmbito da antijuridicidade.
>
> Em certo grau a vontade também é definidora daquilo que deve ser considerado como pessoal e, conseguintemente, excluído do conhecimento alheio. Não em seus termos plenos, pois deverá existir um reconhecimento social em mesmo sentido; vale dizer, não ficará ao simples arbítrio individual, sob os riscos dos excessos da susceptibilidade humana, essa definição (...). (SAMPAIO, 1998, p. 369-370)

Em decorrência da fixação de critérios adequados para essa definição, lançando mão do consentimento ou do que Sampaio classifica como "reconhecimento social" capaz de atenuar a plena escolha do "arbítrio individual", busca-se desenhar o sistema de controle da coleta e do uso dos dados pessoais. No Brasil, depois de um longo tempo, foi isso o que se tentou com as disposições da Lei Geral de Proteção de Dados (LGPD) – Lei n. 13.709/2018.

3. A REGULAMENTAÇÃO BRASILEIRA DE DADOS

De certa forma, a necessidade de regulamentação ficou patente nas próprias justificativas do Projeto de Lei (PL) n. 4.060, apresentadas pelo autor, deputado federal Milton Monti, em 2012:

> (...) a necessidade de um marco regulatório para disciplinar essa atividade e que o mesmo deveria ser, geral e abrangente, face às mutações permanentes em uma área de evolução tecnológica tão rápida, bem como que as questões específicas deveriam ficar a cargo de um conselho de autorregulamentação, aos moldes do CONAR que é destaque em eficiência aqui em nosso país como também em outros países do mundo.

> Não há dúvida nenhuma de que o Estado deve cuidar das questões gerais, mas é também evidente que a sociedade é refrataria ao excesso de tutela por parte do Estado e que deseja exercer na plenitude seus direitos constitucionais inclusive o de receber se quiser comunicações pelos meios disponíveis no momento. (MONTI, 2012, p. 7)

Deixando-se de lado o argumento de que a autorregulamentação seria mais adequada, ganhou importância enorme nos últimos anos o entendimento de que a existência de algum tipo de controle e de normas específicas sobre a utilização de dados e informações decorrentes do uso de programas tecnológicos seria fundamental, em razão da velocidade com que as aplicações e os programas são desenvolvidos e utilizados pela sociedade.

Essa questão foi também levada considerada pelo deputado, o qual, ainda nas justificativas, aduziu que a internet assumia, em 2012, uma importância crescente:

> (...) que isso continuará em ritmo acelerado e de incremento, tendo em vista a velocidade em que novas tecnologias são desenvolvidas para a comunicação com as pessoas.
>
> Dentro dessa realidade se faz necessário estabelecer normas legais para disciplinar tais relações, especialmente para dar proteção à individualidade e à privacidade das pessoas, sem impedir a livre iniciativa comercial e de comunicação. (MONTI, 2012, p. 6-7)

4. A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Com a aprovação da LGPD, tinha o legislador a pretensão de regulamentar o "tratamento de dados pessoais coletados no dia a dia" (FIESP, 2020, p. 3). De acordo com documento elaborado pela Fiesp (2020, p. 6) sobre os dispositivos da norma,

> [a] LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, estabelecendo regras e limites para empresas a respeito da coleta, armazenamento, tratamento e compartilhamento de dados, o que favorece o desenvolvimento econômico.
>
> Em linhas gerais, os titulares de dados passarão a ter maior controle sobre todo o processamento dos seus dados pessoais, do que decorrem diversas obrigações para controladores (a quem competem as decisões sobre o tratamento dos dados) e operadores (aqueles que tratam os dados de acordo com o estipulado pelos controladores).

De modo sintético, e utilizando aqui as considerações apresentadas pela Fiesp, pode-se afirmar que a legislação busca estruturar procedimentos para a adequada coleta e utilização de dados e vincular todo esse processo às finalidades específicas. Como se fez constar no referido documento,

> [u]m dos princípios mais relevantes é o da finalidade, por meio do qual os dados deverão ser utilizados apenas para as finalidades específicas para as quais foram coletados e devidamente informadas aos titulares, juntamente com o princípio da minimização da coleta, isto é, somente devem ser coletados os dados mínimos necessários para que se possa atingir a finalidade, e o da retenção mínima, o qual determina a imediata exclusão dos dados, após atingida a finalidade pela qual eles foram coletados. (FIESP, 2020, p. 6)

De acordo com o disposto no inciso I do art. 6º da LGPD, os dados só podem ser tratados para "propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". De fato, a leitura desse

dispositivo autoriza a tese de que os dados pessoais (art. 5º, I e II), submetidos pelos interessados (controlador e operador) ao processo de tratamento (no conceito amplo estabelecido no inciso X do art. 5º), não podem ser usados fora dessas condições e só devem ser "coletados" nos limites e finalidades especificadamente indicados ao titular das informações. Dessa forma, o momento da obtenção do consentimento junto aos titulares torna-se extremamente importante.

4.1 O CONSENTIMENTO DO TITULAR DOS DADOS

As hipóteses legais para o tratamento dos dados estão indicadas nos incisos do art. 7º da LGPD, que apresenta a seguinte redação:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I – mediante o fornecimento de consentimento pelo titular;
>
> II – para o cumprimento de obrigação legal ou regulatória pelo controlador;
>
> III – pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
>
> IV – para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
>
> V – quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
>
> VI – para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

> VII – para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> VIII – para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)
>
> IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
>
> X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Para tais hipóteses de coleta, excluídas aquelas situações em que envolvidos interesses públicos (incisos II, III, VII e VIII), interesses do próprio titular dos dados ou informações (incisos V, VI) e nos casos de medidas necessárias para "atender interesses legítimos do controlador ou de terceiro" (inciso IX) e para "proteção do crédito" (inciso X), ganha delicada relevância a necessidade de consentimento do titular dos dados ou das informações.

Os princípios em questão devem ser observados até mesmo para as hipóteses em que os dados são tornados públicos por iniciativa do próprio titular. Nesse caso, a legislação autorizou a dispensa do consentimento preliminar, mas fixou como condição para a sua utilização o "resguard[o] [d]os direitos do titular e [d]os princípios" acima mencionados, como determina o § 4º do art. 7º: "É dispensada a exigência do consentimento previsto no *caput* deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei".

4.2 AS FORMALIDADES PARA A OBTENÇÃO DO CONSENTIMENTO

As formalidades exigidas para o consentimento do titular dos dados estão relacionadas no art. 8º da Lei:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
>
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
>
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
>
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
>
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do *caput* do art. 18 desta Lei.
>
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Apesar de essas condicionantes parecem insuficientes, elas são necessárias para a preservação dos direitos fundamentais que a lei visa proteger. De fato, sem o cumprimento delas, ficamos no pior dos mundos, sem meios adequados de controlar ou permitir um pequeno

monitoramento que seja na prática dos usuários, das próprias redes e dos sistemas de informação.

Sem tais instrumentos, ficamos na situação descrita por Gamble (*apud* BAUMAN, 2008, p. 10), diretor britânico de uma agência de monitoramento de rede: as redes "(...) representa[m] tudo aquilo que se vê no *playground* – a única diferença é que nesse *playground* não há professores, policiais ou moderadores que ficam de olho no que se passa".

5. CONCLUSÃO

Tudo isso posto, parece relevante que se medite ainda um pouco mais sobre o consentimento referido no art. 8º da LGPD. Para tanto, convém atentarmos para o fato de que são fundamentos da disciplina da proteção de dados pessoais, nos termos do art. 2º, o respeito à privacidade, a inviolabilidade da intimidade, da honra e da imagem, os direitos humanos, além da dignidade e o exercício da cidadania pelas pessoas naturais.

É importante, ainda, ressaltar que a LGPD tem por finalidade a proteção da pessoa natural, não nos parecendo que o diploma se aplique à pessoa jurídica. De fato, enquanto o art. 1º estabelece como sendo o objeto da lei o tratamento de dados pessoais, o art. 5º, especificamente em seu inciso I, define dado pessoal como a informação relacionada à *pessoa natural*, destaque-se, desde que identificada ou passível de sê-lo. Com isso, malgrado se possa até reconhecer a pessoa jurídica como titular de alguns dos direitos da personalidade, não é ela destinatária da proteção de que cuida a norma em questão.

Outro ponto que merece relevo, na conformação do tema do consentimento, é a letra do art. 6º da LGPD, cujo teor impõe a observância da boa-fé no tratamento de dados pessoais. Observe-se que ali a referência diz com a boa-fé objetiva, na qual se enredam os deveres de proteção, informação e cooperação dos agentes envolvidos, pessoas

naturais, além de pessoas públicas ou privadas cuja atividade envolva o tratamento de dados da pessoa natural. Nesse sentido, a atuação desse grupo deve, como exige a boa-fé, guardar respeito às expectativas de todos os envolvidos na informação e no tratamento de dados. Por essa razão, a lei sob análise veda a realização do tratamento de dados mediante vício de consentimento. Em outros termos, a manifestação da vontade da pessoa natural, em casos tais, precisa ser livre, consciente, devendo o controlador entregar ao titular dos dados tratados todas as informações pertinentes, inclusive aquelas referentes ao risco inerente à operação, a finalidade objetiva do tratamento desses mesmos dados e isso em quaisquer de suas fases (coleta, produção, recepção, classificação, utilização, acesso, conforme determina o art. 5º, X, da LGPD).

Note-se, portanto, que se aplicam as disposições do art. 104, I, do Código Civil à manifestação de vontade, pelo que deve o titular estar em pleno gozo de sua capacidade civil, ou, quando menos, ser assistido em caso de incapacidade relativa. Ainda que o tema mereça que nos debrucemos mais sobre ele, parece-nos, até mesmo em razão do art. 6º da Lei, que o princípio da boa-fé objetiva, ali referido, reveste-se de bilateralidade, como já assinalamos, impondo também ao titular dos dados os deveres de proteção, informação e cooperação. Em razão disso, é de absoluta justiça que ao consentimento também se aplique a letra do art. 104 do Código Civil, a fim de se evitar o manejo espúrio da lei. Em termos mais claros, nos casos em que a pessoa física titular dos dados, a despeito da reserva mental de não consentir, consente no tratamento de seus dados, subsistirá o consentimento, já que a boa-fé objetiva não se compadece com qualquer forma de ardil.

Por fim, cumpre destacar que o tratamento de dados, na maioria das vezes, se desenvolve no âmbito das relações de consumo. Contudo, é necessário concluir que abrange a disciplina da proteção de dados pessoais não só o texto da LGPD mas também o Código de Defesa do Consumidor, além do Código Civil.

Trata-se, como bem se vê, de inovação legislativa cujos passos, ainda tímidos, dão-nos clara noção de que se trata de um valor legislativo cujo advento potencializa o microssistema de defesa do consumidor, pessoa física, tutelando-o no que concerne ao respeito à sua privacidade, intimidade, honra e imagem, exatamente como cuidado na letra do art. 5º, X, da Constituição Federal.

REFERÊNCIAS

BAUMAN, Zygmunt. *44 cartas do mundo líquido moderno*. Rio de Janeiro: Zahar, 2011.

BAUMAN, Zygmunt. *Vida para consumo*. Rio de Janeiro: Zahar, 2008.

BRASIL. *Lei n. 13.709*, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 set. 2020.

FIESP. *Cartilha LGPD* (Lei Geral de Proteção de Dados). São Paulo: FIESP/CIESP.

MONTI, Milton. *Projeto de Lei n. 4.060/2012*. Câmara dos Deputados, Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 12 set. 2020.

SAMPAIO, José Adércio Leite. *Direito à intimidade e à vida privada*: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998.

O CONCEITO DE TRATAMENTO DE DADOS PESSOAIS E O ACÓRDÃO LINDQVIST, DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA[1]

Bruno Freire de Carvalho Calabrich[2]

RESUMO

O artigo analisa o acórdão Lindqvist, do Tribunal de Justiça da União Europeia. O julgado é considerado um dos mais importantes a respeito do tema da proteção de dados pessoais. As conclusões apresentadas ressoaram no Regulamento n. 2016/679 da União Europeia e, no Brasil, na Lei n. 13.709/2018 (LGPD).

Palavras-chave: Dados pessoais, proteção. Tribunal de Justiça, União Europeia. Lei Geral de Proteção de Dados (LGPD). Acórdão Lindqvist.

---

2 Mestre em Direito pela FDV. Doutorando em Direito pela UnB. Especialista (MBA) em Gestão Pública pela FGV. Professor da Escola Superior do Ministério Público da União. Procurador Regional da República em Brasília (PRR-1ª Região).

ABSTRACT

The article examines the Court of Justice of the European Union decision on Lindqvist trial, considered one of the most important judgement on the subject of personal data protection, whose conclusions echoed in the European Union Regulation n. 2016/679 and, in Brazil, the Law n. 13.709 (LGPD).

Keywords: Personal data protection. Court of Justice of the European Union. Data Protection Law. Lindqvist judgement.

1. INTRODUÇÃO

Em 15 de agosto de 2018, foi publicada a Lei n. 13.709, dispondo sobre a proteção de dados pessoais. A Lei Geral de Proteção de Dados (LGPD) tem forte inspiração no Regulamento Geral da Proteção de Dados (GDPR, na sigla em inglês) europeu – Regulamento (UE) n. 2016/679 –, em vigor desde 28 de maio de 2018. Depois de uma série de adiamentos, a lei brasileira finalmente entrou em vigor em 18 de setembro de 2020[3].

O processo legislativo que culminou na aprovação do GDPR é fruto de uma preocupação cada vez mais candente, apesar de versar assunto debatido há anos nas cortes europeias.

O presente artigo propõe-se a analisar o acórdão do Tribunal de Justiça da União Europeia (TJUE) do processo de reenvio prejudicial n.

3 O início da vigência da LGPD se deu com a sanção da Lei n. 14.058 (decorrente da Medida Provisória n. 959), de 17 de setembro de 2020, da qual foi alterado o art. 4º – que, na redação inicialmente proposta, mais uma vez adiaria o início da vigência da lei brasileira de dados. Remanesceram adiadas para 1º de agosto de 2021 apenas as sanções da LGPD (arts. 52, 53 e 54), conforme o art. 20 da Lei n. 14.010, de 10 de julho de 2020.

C-101/01, de 6 de novembro de 2003. O "acórdão Lindqvist", como é conhecido, é considerado um dos julgados mais importantes a respeito do tema da proteção de dados pessoais na internet – hoje disciplinado pelo GDPR, no cenário europeu, e pela LGPD, no contexto brasileiro.

2. O PAPEL DO TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA

O TJUE[4] tem como uma de suas principais funções analisar a compatibilidade de atos normativos internos dos Estados-membros da União Europeia com os atos normativos da União Europeia (UE) – como tratados, diretivas e regulamentos. Pelo instrumento processual do *reenvio prejudicial*, os órgãos jurisdicionais dos Estados-membros encaminham ao TJUE casos sob a jurisdição local em que foram suscitadas dúvidas quanto a essa compatibilidade, conforme a interpretação que seja dada a determinada norma. O reenvio prejudicial pode ser feito de ofício, por juiz ou órgão jurisdicional colegiado, ou mediante provocação das partes e mesmo do Ministério Público. A submissão de um reenvio prejudicial é feita na forma de uma quesitação, por itens, nominados *questões prejudiciais.*

O acórdão Lindqvist foi um dos muitos casos submetidos à apreciação do TJUE, ao longo de suas mais de seis décadas de existência, pelo mecanismo do *reenvio prejudicial*[5].

---

4 Sobre o TJUE: https://curia.europa.eu/jcms/jcms/Jo2_6999/pt/. Acesso em: 5 maio 2019.

5 O Tribunal de Justiça da União Europeia, que tem sede em Luxemburgo, é um dos órgãos da União Europeia e não deve ser confundido com o Tribunal Europeu dos Direitos Humanos – TEDH (que tem como função julgar casos nos quais há potencial violação a princípios da Convenção Europeia dos Direitos Humanos e só aprecia processos atinentes aos países que ratificaram a referida convenção).

3. O CASO B. LINDQVIST

Como sintetizado no introito do acórdão proferido no processo n. C-101/01, o Göta Hovrätt (Tribunal de Apelação de Göta, na Suécia[6]) submeteu ao TJUE *sete questões prejudiciais* sobre a

> interpretação da Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281, p. 31).
>
> Estas questões foram suscitadas no âmbito de um processo penal pendente no referido órgão jurisdicional contra B. Lindqvist, acusada de ter violado a legislação sueca relativa à protecção dos dados de carácter pessoal ao publicar no seu sítio Internet dados de carácter pessoal relativos a um determinado número de pessoas que trabalham, como ela, a título benévolo, numa paróquia da Igreja Protestante da Suécia.

O caso concreto que ensejou a provocação do TJUE é bastante peculiar. Após ter frequentado um curso de informática, a senhora Bodil Lindqvist, que tinha um emprego regular como agente de manutenção e atuava em uma Igreja Protestante da Suécia – mais exatamente, exercendo funções de catequista na paróquia de Alseda –, criou, em sua casa e com seu computador pessoal, páginas de internet para divulgar aos membros da paróquia que se preparavam para o crisma informações do interesse da comunidade. A pedido dela, o administrador do *site* da igreja consentiu e implementou um *link* de acesso às páginas criadas pela senhora.

Ali eram exibidas informações sobre a própria B. Lindqvist e outros dezoito colegas de paróquia: nome, atividades exercidas, *hobbies*,

---

6 Sobre o Göta Hovrätt: http://www.gotahovratt.se/. Acesso em: 9 out. 2020.

situação familiar e número de telefone, entre outros dados. Informou-se até mesmo que certa pessoa havia lesionado o pé e em razão disso se encontrava afastada por licença médica. Como resumido no acórdão do TJUE, "B. Lindqvist descreveu as funções ocupadas pelos colegas e os seus hábitos dos tempos livres em termos ligeiramente humorísticos".

Tudo foi feito sem prévio conhecimento e consentimento dos envolvidos. Tampouco foi informada a criação das páginas ao órgão público da Suécia (*Datainspektion*) responsável pela proteção de dados transmitidos pela internet. Alguns de seus colegas não gostaram da divulgação de informações pessoais daquela forma. Assim, tão logo a responsável pela publicação ficou sabendo da contrariedade, retirou as páginas do ar. Cientificado do fato, o Ministério Público da Suécia processou B. Lindqvist por violação à lei daquele país relativa à proteção de dados pessoais e pediu sua condenação.

A Diretiva n. 95/46 do Parlamento e do Conselho Europeu foi transposta para o direito sueco pela *Personuppgiftslag*, SFS 1998, n. 204 (lei sueca relativa aos dados de caráter pessoal, ou simplesmente "PUL"). Foi com base nessa lei que o Ministério Público da Suécia deflagrou o processo penal contra B. Lindqvist.

Ela foi acusada por ter: a) tratado dados de caráter pessoal, no âmbito de um tratamento automatizado, sem prévia notificação por escrito à *Datainspektion* (§ 36 da PUL); b) tratado, sem autorização, dados de caráter pessoal sensíveis, relativos à lesão no pé e à licença médica de uma de suas colegas de paróquia (§ 13 da PUL); e c) transferido para países terceiros dados de caráter pessoal tratados sem autorização (§ 33 da PUL).

B. Lindqvist reconheceu os fatos, mas negou ter cometido qualquer infração. Após condenação ao pagamento de multa, ela interpôs recurso contra a decisão ao órgão jurisdicional com competência recursal local (o Göta Hovrätt, ou Tribunal de Apelações de Göta).

4. O CONTEÚDO DO ACÓRDÃO LINDQVIST E AS TESES APRESENTADAS

Considerando as imputações formuladas pelo Ministério Público sueco contra B. Lindqvist e a possível incompatibilidade da lei local com a Diretiva n. 95/46, o Poder Judiciário da Suécia provocou o TJUE, mediante o instrumento do reenvio prejudicial.

Os questionamentos feitos pela Justiça sueca foram todos baseados na Diretiva n. 95/46, notadamente no que dizia respeito à compatibilidade PUL com o diploma normativo comunitário.

A diretiva, norma europeia relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, vigeu até 24 de maio de 2018, quando entrou em vigor o GDPR, que inspirou a brasileira LGPD.

A seguir serão apresentados, de modo objetivo e sintético, os pontos controversos submetidos no processo de reenvio prejudicial n. C-101/01 e decididos pelo TJUE.

4.1 PRIMEIRA QUESTÃO PREJUDICIAL

> *A menção de uma pessoa numa página da internet constitui conduta abrangida pelo âmbito de aplicação da Diretiva n. 95/46? É saber, o fato de alguém divulgar informações sobre várias pessoas, incluindo número de telefone,* hobbies *e ocupações profissionais caracteriza um "tratamento de dados pessoais por meios total ou parcialmente automatizados", nos termos do art. 3º/1, da Diretiva n. 95/46?*

Eis a dicção do art. 3º/1 da Diretiva n. 95/46:

> Artigo 3º
> Âmbito de aplicação

> 1. A presente directiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados.

Em resposta a essa questão, a defesa de B. Lindqvist argumentou que não se pode considerar que a simples menção do nome de uma pessoa ou de outros dados de caráter pessoal num texto de uma página da internet caracterize um "tratamento automático de dados".

Sobre esse ponto, o TJUE, ao proferir seu acórdão no processo de reenvio prejudicial n. C-101/01, decidiu que a publicação, numa página de internet, a respeito de várias pessoas, com identificação pelo nome ou por outros meios, constitui, sim, um *tratamento de dados pessoais por meios total ou parcialmente automatizados*, conforme previa o art. 3º/1 da Diretiva n. 95/46.

4.2 SEGUNDA QUESTÃO PREJUDICIAL

> *Uma conduta como a praticada pela senhora B. Lindqvist poderia ser considerada como "tratamento de dados pessoais contidos num ficheiro ou a ele destinados", conforme previsto no art. 3º/1 da diretiva?*

A pergunta foi feita apenas de forma subsidiária, para o caso de o Tribunal entender que as páginas publicadas por B. Lindqvist não poderiam ser enquadradas como tratamento de dados pessoais por meios total ou parcialmente automatizados. Nessa hipótese, a Justiça sueca questionava se, ainda assim, a conduta poderia estar amoldada à Diretiva n. 95/46, como espécie de *tratamento de dados pessoais em arquivos* (3º/1), mesmo que por meios não automatizados.

Como o TJUE respondeu afirmativamente ao primeiro quesito, essa questão restou prejudicada.

4.3 TERCEIRA QUESTÃO PREJUDICIAL

> *A conduta de reunir dados de colegas de trabalho numa página de interesse privado (*i.e.*, de interesse apenas para os paroquianos), mas acessível a qualquer pessoa que tenha o endereço da página, pode ser considerada excluída do âmbito de aplicação da Diretiva n. 95/46, conforme as exceções do art. 3º/2?*

Nesse sentido, o referido dispositivo apresentava a seguinte redação:

> Âmbito de aplicação
> (...)
> 2. A presente directiva não se aplica ao tratamento de dados pessoais:
> – efectuado no exercício de actividades não sujeitas à aplicação do direito comunitário, tais como as previstas nos títulos V e VI do Tratado da União Europeia, e, em qualquer caso, ao tratamento de dados que tenha como objecto a segurança pública, a defesa, a segurança do Estado (incluindo o bem-estar económico do Estado quando esse tratamento disser respeito a questões de segurança do Estado), e as actividades do Estado no domínio do direito penal,
> – efectuado por uma pessoa singular no exercício de actividades exclusivamente pessoais ou domésticas.

Em resposta, a defesa de B. Lindqvist argumentava *não estar* o particular que, usando de sua liberdade de expressão, cria páginas de internet no âmbito de uma atividade não lucrativa ou de seus passatempos, *exercendo atividade econômica.* Sendo assim, não seria aplicável o direito comunitário (*i.e.*, da Comunidade Econômica Europeia – CEE, no âmbito da qual vigia a Diretiva n. 95/46).

Sobre isso, o TJUE, ao final, decidiu que, como as atividades exercidas pela senhora eram religiosas ou beneficentes, de fato não poderiam

ser equiparadas às referidas no art. 3º/2 da diretiva, *primeiro travessão*, e, portanto, não estavam abrangidas por aquela exceção.

Quanto à exceção prevista no art. 3º/2, *segundo travessão*, o considerando n. 12 da diretiva aponta como exemplos de tratamento de dados efetuado por uma pessoa singular, no exercício de atividades exclusivamente pessoais ou domésticas, o envio de correspondências e listas de endereços. Esse não era o caso do tratamento de dados de caráter pessoal que consiste na publicação via internet e, consequentemente, na disponibilização a um número indefinido de pessoas.

Nesse sentido, o TJUE entendeu que as regras sobre o tratamento de dados pessoais da diretiva eram aplicáveis a condutas como as praticadas por B. Lindqvist.

4.4 QUARTA QUESTÃO PREJUDICIAL

> *Os dados relativos ao fato de uma colega de trabalho, identificada pelo nome, ter uma lesão no pé e estar afastada por licença médica, são pessoais relativos à saúde, os quais, nos termos do art. 8º/1, não podem ser objeto de tratamento?*

Quanto a esse aspecto, eis o que previa o dispositivo:

> Artigo 8º
>
> Tratamento de certas categorias específicas de dados
>
> 1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual.

Sobre essa questão, o TJUE decidiu que a expressão "dados relativos

à saúde" deveria ser interpretada de forma ampla, de modo a incluir informações relativas a todos os aspectos físicos ou psíquicos da saúde de uma pessoa. Assim, o fato de alguém ter lesionado o pé e estar de licença médica constitui, sim, um dado de caráter pessoal relativo à saúde, conforme previsto no art. 8º/1 da Diretiva n. 95/46.

Em síntese, a divulgação de dados sobre a lesão e o afastamento por licença médica de uma colega de paróquia, ao tratar de informações de caráter sensível, poderia e deveria ser vedada pela legislação sueca – como de fato era –, nos termos do citado artigo.

4.5 QUINTA QUESTÃO PREJUDICIAL

A quinta questão prejudicial foi desdobrada em duas perguntas.

> *Ante o fato de a transferência de dados pessoais para países terceiros, nos termos da Diretiva n. 95/56, ser proibida, se uma pessoa na Suécia, com o auxílio de um computador, recolher dados pessoais em página armazenada em servidor sueco, por meio do qual cidadãos de países terceiros tenham acesso às informações, isso constituiria transferência de dados para países terceiros, na acepção da Diretiva n. 95/46? Essa perspectiva seria mantida mesmo se ninguém de um país terceiro tenha efetivamente acessado os dados ou a página em questão, ou se o servidor estivesse localizado num país terceiro?*

A Comissão das Comunidades Europeias (órgão executivo da CCE, sucedido pela Comissão da União Europeia) e o governo sueco também intervieram no processo n. C-101/01. Sobre a quinta questão prejudicial, a CEE e a Suécia alegaram que a inserção, por intermédio de um computador de dados pessoais numa página da internet, de modo a que estes se tornem acessíveis a nacionais de países terceiros, constitui

transferência de dados na acepção da diretiva. Também alegaram que a resposta deveria ser idêntica mesmo se nenhum nacional de um país terceiro tomasse efetivamente conhecimento desses dados, ou ainda que o servidor se encontrasse fisicamente num país terceiro.

O governo da Holanda, que também manifestou interesse no processo, alegou que o conceito de transferência não estava definido na Diretiva n. 95/46. Também argumentou que a expressão "transferência de dados" deveria ser entendida como tendo por objeto ato que visasse deliberadamente a transferir dados pessoais de um país para outro. Partindo dessa premissa, a inserção de dados de caráter pessoal numa página de internet não poderia ser considerada transferência de dados para um país terceiro, no sentido do art. 25 da Diretiva n. 95/46.

Outro governo a se manifestar no processo foi o do Reino Unido, o qual asseverou que o art. 25 da diretiva tinha por objeto a transferência de dados para países terceiros e não a simples acessibilidade a partir de países terceiros. O conceito de transferência implica a transmissão de dados de uma pessoa situada num local preciso a um terceiro situado em outro local preciso. Só nesse caso, o art. 25 da diretiva impunha aos Estados-membros velar pelo nível adequado de proteção dos dados de caráter pessoal num país terceiro.

Cotejados esses argumentos, o TJUE decidiu que os dados de caráter pessoal que chegam ao computador de uma pessoa situada num país terceiro, provenientes de uma pessoa que os carregou num *site* da internet, não foram transferidos diretamente entre essas duas pessoas, mas através da infraestrutura informática do fornecedor de serviços de anfitrião onde a página está armazenada. Se o art. 25 da diretiva fosse interpretado no sentido da "transferência para um país terceiro de dados" toda vez que são carregados dados de caráter pessoal numa página da internet, esse processo seria necessariamente uma transferência para todos os países onde existentes meios técnicos para acessar a internet.

Assim, o TJUE decidiu que o art. 25 da diretiva deveria ser interpre-

tado no sentido de as operações tais quais as efetuadas por B. Lindqvist não constituírem transferência de dados a país terceiro.

4.6 SEXTA QUESTÃO PREJUDICIAL

> *Pode-se considerar que, num caso como o de B. Lindqvist, as disposições da Diretiva n. 95/46 implicam restrição a violar os princípios gerais da liberdade de expressão ou outros direitos e liberdades que vigoram na UE e que correspondem ao art. 10º da Comissão Europeia dos Direitos do Homem?*

B. Lindqvist alegou que a diretiva e a PUL eram contrárias à liberdade de expressão, na medida em que previam condições de consentimento e notificação prévios a uma autoridade de controle, assim como proibiam o tratamento de dados de caráter pessoal de natureza sensível. A definição de *tratamentos de dados* pessoais por meios total ou parcialmente automatizados, segundo a defesa de B. Lindqvist, não atendia aos critérios de validade normativa de *previsibilidade* e *precisão*. Argumentou-se, ainda, que o simples fato de aludir nominalmente a uma pessoa singular, revelar seus números de telefone e condições de trabalho – informações que são públicas, notórias ou triviais – não constituiriam violação substancial do direito ao respeito da vida privada.

Sobre isso, o TJUE observou que o considerando n. 3 da Diretiva n. 95/46 consignava que a harmonização dos regimes nacionais deveria ter como objeto não apenas a livre circulação de dados entre Estados-membros, mas também a proteção dos direitos fundamentais das pessoas. Assim, seria necessário ponderar entre a liberdade de expressão de B. Lindqvist, no âmbito do seu trabalho como catequista, a liberdade de exercer atividades que contribuem para a vida religiosa e a proteção da vida privada das pessoas cujas informações ela publicou em seu *site*.

Ao cabo, segundo o Tribunal, as disposições da Diretiva n. 95/46 não continham, somente por isso, uma restrição contrária à liberdade de expressão. Logo, competia aos órgãos jurisdicionais nacionais assegurar o justo equilíbrio entre os direitos e os interesses em causa.

Destarte, o TJUE não acolheu a alegação de B. Lindqvist, no sentido de que suas páginas estavam abrangidas por seu direito à liberdade de expressão.

4.7 SÉTIMA QUESTÃO PREJUDICIAL

> *Pode um Estado-membro conferir proteção mais extensa aos dados pessoais ou um âmbito de aplicação mais amplo do que o resultante da diretiva, mesmo que não se verifique nenhuma das circunstâncias previstas no art. 13º?*

A Comissão e Governo sueco alegaram ser isso impossível.

O TJUE decidiu que as medidas adotadas pelos Estados-membros para assegurar a proteção de dados de caráter pessoal deveriam estar em conformidade quer com as disposições da Diretiva n. 95/46, quer com o objetivo de manter o equilíbrio entre a livre circulação dos dados de caráter pessoal e a proteção da vida privada. Em contrapartida, não havia óbice a que um Estado-membro alargasse o alcance da legislação nacional quando da transposição da diretiva a domínios não incluídos no seu âmbito de aplicação.

No acórdão do TJUE, não se identificou a existência, na legislação sueca, de regra que extrapolasse as determinações da Diretiva n. 95/46 sobre a proteção de dados pessoais.

5. CONCLUSÃO

Para o caso concreto, o resultado prático do julgamento foi o de considerar que eram hígidos e regulares o processo e a eventual condenação de B. Lindqvist pela criação de páginas nas quais eram divulgadas informações pessoais dos colegas paroquianos. Calha reiterar, entretanto, que o TJUE não julga casos concretos: ele decide sobre a compatibilidade da legislação interna dos Estados-membros com as normas da União Europeia. É nesse aspecto que o julgado aqui estudado revela sua maior importância.

Como se pode notar das conclusões do TJUE, o precedente firmado no acórdão Lindqvist – processo C-101/01, de 6 de novembro de 2003 – assentou as bases para o que se deve compreender como *dados pessoais* passíveis de proteção e para o conceito de *tratamento de dados pessoais*, à luz da então vigente Diretiva n. 95/46.

Anos mais tarde, as premissas fixadas no acórdão foram densificadas na *Carta de Direitos Fundamentais da União Europeia*, que se tornou vinculativa aos Estados-membros da UE a partir da entrada e vigor do Tratado de Lisboa, em dezembro de 2009. Em seu art. 8º, o diploma prevê:

> Artigo 8º
>
> Proteção de dados pessoais
>
> 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
>
> 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
>
> 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

A proteção de dados pessoais finalmente ganhou um regulamento específico da UE em 2016: o GDPR, Regulamento n. 2016/679, revogou a Diretiva n. 95/46.

Espelhando a jurisprudência do TJUE inaugurada pelo acórdão Lindqvist, o regulamento estatuiu:

> Artigo 4º
> Definições
> Para efeitos do presente regulamento, entende-se por:
> 1) "Dados pessoais", informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;
> 2) "Tratamento", uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

O GDPR conferiu especial proteção a determinados dados pessoais – inclusive informações sobre saúde[7] e convicções religiosas:

---

7 O conceito de dados pessoais sobre saúde consta do art. 4º, 15, do RGPD: "'Dados relativos à saúde', dados pessoais relacionados com a saúde física ou mental de

> Artigo 9º
>
> Tratamento de categorias especiais de dados pessoais
>
> 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

As definições sobre *dados pessoais* e *tratamento de dados pessoais* do GDPR foram espelhadas na LGPD brasileira, em vigor desde 18 de setembro de 2020, que em seu art. 5º prevê:

> Art. 5º Para os fins desta Lei, considera-se:
>
> I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
>
> II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
>
> (...)
>
> X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

---

uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde."

Observe-se, em especial, o inciso II do art. 5º, que define como dado pessoal *sensível* aquele "sobre origem racial ou étnica, convicção religiosa, opinião política, *filiação a sindicato ou a organização de caráter religioso*, filosófico ou político, dado referente à *saúde* ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Dados referentes à saúde e à vinculação a organização religiosa, portanto, estão entre os que merecem especial proteção, ainda maior que a oferecida aos não classificados como *dados pessoais sensíveis*[8].

Como se percebe, a abrangência dos conceitos de *dados pessoais* e *tratamento de dados pessoais*, tanto do GDPR europeu quanto na LGPD brasileira, é *amplíssima* – exatamente como compreendido em 2003 pelo TJUE no acórdão Lindqvist.

REFERÊNCIAS

BRASIL. *Lei federal n. 13.709, de 14 de agosto de 2018*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 9 out. 2020.

FRAZÃO, Ana. Nova LGPD: o tratamento dos dados pessoais sensíveis. *Jota*, 26 set. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-o-tratamento-dos-dados-pessoais-sensiveis-26092018. Acesso em: 9 out. 2020.

UNIÃO EUROPEIA. *Diretiva n. 95/46*. Disponível em: https://eur-lex.

8 Sobre dados pessoais sensíveis, Frazão (2018), analisando a LGPD, ressalta que são dados "em relação aos quais se espera um padrão ainda mais rigoroso de proteção dos titulares de dados".

europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046. Acesso em: 9 out. 2020.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. *Jornal Oficial da União Europeia*, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679. Acesso em: 9 out. 2020.

UNIÃO EUROPEIA. Tribunal de Justiça. *Acórdão de 6 de novembro de 2003* – processo C-101/01. Disponível em: http://publications.europa.eu/resource/cellar/bcc476ae-43f8-4668-8404-09fad89c202a.0009.02/DOC_1. Acesso em: 9 out. 2020.

DISCRIMINAÇÃO ALGORÍTMICA E TRANSPARÊNCIA NA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS[1]

Bruno Freire de Carvalho Calabrich[2]

RESUMO

O artigo analisa o problema da discriminação algorítmica e do dever de transparência no tratamento automatizado de dados pessoais. Examina, ainda, como a Lei Geral de Proteção de Dados Pessoais brasileira enfrenta o tema e como suas disposições podem ser interpretadas e concretamente aplicadas, de modo a conferir real efetividade aos direitos dos titulares dos dados pessoais.

Palavras-chave: Discriminação algorítmica. Decisões automatizadas. Transparência. Dados pessoais.

---

2 Mestre em Direito pela FDV. Doutorando em Direito pela UnB. Especialista (MBA) em Gestão Pública pela FGV. Professor da Escola Superior do Ministério Público da União. Procurador Regional da República em Brasília (PRR-1ª Região).

ABSTRACT

The article analyzes the problem of algorithmic discrimination and the obligation of transparency in the automated processing of personal data, how the brazilian Personal Data Protection Law addresses the issue and how its provisions can be interpreted and concretely applied, in order to enforce real effectiveness to personal data rights.

Keywords: Algorithmic discrimination. Automated decisions. Transparency. Personal data.

1. INTRODUÇÃO

O tratamento automatizado de dados pessoais, longe de ser tema de obras de ficção científica, é uma realidade atual, no Brasil e em todo o mundo.

Em 2017, causou espanto e curiosidade a notícia sobre o projeto do governo da China para monitorar, premiar e punir o comportamento de seus cidadãos[3]. Em meados de 2018, a notícia era a de que, (então) em breve, o país poderia impedir cidadãos de comprarem passagens de avião ou de trem caso tivessem notas ruins dentro desse sistema de *score* social[4]. No início de 2019, soube-se que, na verdade, o governo chinês já havia barrado cerca de 23 milhões de viagens de avião ou trem ao longo do ano anterior, com base nas notas atribuídas aos cidadãos chineses[5]. Todas as decisões desse sistema estão assentadas na coleta massiva e no tratamento automatizado de dados pessoais.

---

3 Ver BBC (2017).

4 Ver Sali (2018).

5 Ver Trindade (2019).

No Brasil, em abril de 2018, sensores instalados nas portas da linha 4-Amarela do metrô da cidade de São Paulo passaram a coletar dados biométricos e expressões corporais dos usuários, identificando suas reações à publicidade e aos informes exibidos em telas espalhadas em três estações. A ViaQuatro, concessionária responsável pela operação daquele trecho metroviário, foi processada, por meio de ação civil pública, pelo Instituto Brasileiro de Defesa do Consumidor (Idec), sob o argumento de tratamento indevido de dados pessoais. Em decisão liminar, a concessionária foi obrigada pela Justiça de São Paulo a retirar os sensores, que foram desligados em setembro daquele ano[6].

Na Bahia, câmeras com sensores biométricos instaladas pela Secretaria de Segurança Pública (SSP/BA) permitiram identificar e prender, até julho de 2019, 46 pessoas foragidas[7]. Os equipamentos identificam e comparam traços faciais de indivíduos com mandados de prisão em aberto e alertam imediatamente equipes policiais. A primeira detenção feita com o auxílio desse sistema aconteceu em março de 2019, em plena terça-feira de carnaval, em Salvador. Tratava-se de um homem investigado pela prática de homicídio, contra quem havia uma ordem de prisão decretada. O suspeito, que saía pelo bloco carnavalesco "As Muquiranas", estava maquiado e vestido com uma fantasia de mulher[8]. No ano seguinte, no mesmo período, o sistema de reconhecimento facial da SSP/BA permitiu a captura, na capital baiana, de 42 pessoas foragidas[9].

O tratamento automatizado de dados pessoais tem sido explorado mais largamente por empresas, como instrumento para a definição de perfis pessoais. Esse procedimento é especialmente relevante para as

6 Ver Demartine (2018).

7 Ver Tarde (2019).

8 Ver Correio (2019).

9 Ver Gama (2020).

relações de consumo e crédito – inclusive para práticas eventualmente abusivas. Em julho de 2018, o Departamento de Proteção e Defesa do Consumidor (DPDC), do Ministério da Justiça brasileiro, condenou a empresa *Decolar.com* a uma multa de R$ 7.500.000,00, por diferenciação de preço de acomodações e negativa de oferta de vagas de acordo com a localização geográfica do consumidor[10] – técnicas claramente discriminatórias[11], conhecidas como *geopricing* e *geoblocking* respectivamente.

Outros casos bastante conhecidos – e reveladores de tratamentos discriminatórios – são: (a) o do algoritmo de recrutamento da área de recursos humanos da Amazon, que facilitava a contratação de homens em detrimento de mulheres[12]; (b) o do algoritmo de categorização de imagens do aplicativo Google Photos, que identificava fotos de pessoas negras como "gorilas" – sendo digno de nota que a "solução" da empresa para contornar o problema foi simplesmente bloquear a palavra "gorila" dos critérios de indexação[13]; e (c) o do algoritmo do programa Compas (*Correctional Offender Management Profiling for Alternative Sanctions*), *software* de auxílio a juízes norte-americanos na avaliação da probabilidade de reincidência para fins de dosimetria da pena, criticado (i) por errar quase duas vezes mais prognósticos de *reincidência* ao identificar réus negros como futuros criminosos quando comparados aos brancos, e (ii) por errar com muito mais frequência prognósticos de *não reincidência* ao rotular réus brancos como de baixo risco quando comparados aos negros (ANGWIN *et al*., 2016).

Esses são apenas alguns exemplos do tratamento de dados pessoais de forma automatizada, pela máquina, que opera segundo algoritmos programados para seu funcionamento.

---

10 Ver Brasil (Ministério da Justiça, 2018).

11 Ver Frazão (2018a).

12 Ver Dastin (2018).

13 Ver Hern (2018).

2. ALGORITMOS E TRATAMENTO DE DADOS PESSOAIS

Algoritmo não é uma palavra nova, mas poucos costumavam usá-la até alguns anos atrás.

Segundo o dicionário *Houaiss* (2001, p. 155), algoritmo é um "conjunto de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas". Na matemática, é "uma sequência finita de regras, raciocínios ou operações que, aplicada a um número finito de dados, permite solucionar classes semelhantes de problemas". É, em suma, uma sequência de ações claras e específicas para a solução de um determinado problema. Uma receita de bolo é um algoritmo. Em linguagem computacional, "é uma sequência de instruções que informa ao computador o que ele deve fazer" (DOMINGOS, 2017, p. 24).

São tão variadas e tão presentes suas aplicações no mundo de hoje que é possível afirmar, como o faz Domingos (2017, p. 24), que vivemos *a era dos algoritmos*:

> Há apenas uma ou duas gerações, a menção da palavra algoritmo não significava nada para a maioria das pessoas. Atualmente, os algoritmos integram tudo que se faz no mundo civilizado. Eles fazem parte da trama que compõe nossa vida diária. Não estão apenas nos celulares ou *laptops*, mas nos carros, em nossa casa, nos utensílios domésticos e em brinquedos. As instituições bancárias são um imenso quebra-cabeça de algoritmos, com pessoas apertando botões do outro lado. Os algoritmos programam voos e entregam mercadorias, calculam os lucros e mantêm registros. Se todos os algoritmos parassem de funcionar, o mundo que conhecemos chegaria ao fim.

Algoritmos podem ser usados para definir perfis *pessoais, profissionais, de consumo, de crédito ou referentes a aspectos da personalidade –*

essas expressões, aliás, assim constam na Lei Geral de Proteção de Dados brasileira (LGPD) – Lei n. 13.709, de 14 de agosto de 2018, em vigor desde 18 de setembro de 2020.

Relacionados com a definição de perfis, os algoritmos também podem fazer diagnósticos, julgamentos, classificações e *rankings* – podem, em resumo, servir como ferramentas para a tomada de *decisões automatizadas*. Estas podem afetar o indivíduo em variadas dimensões de sua vida privada e social, enquanto empregado, eleitor, consumidor ou contratante (de planos de saúde, de financiamentos, de seguros etc.), réu ou parceiro sexual – para citar apenas algumas de suas praticamente incontáveis possibilidades de aplicação.

Algoritmos são, como visto, ferramentas para a tomada de decisões, usadas por Estados e empresas. São instrumentos não somente úteis, mas cada vez mais indispensáveis ao funcionamento de entes públicos e privados, num mundo em que as interações são mais e mais dinâmicas e velozes.

No entanto, não é demais lembrar: Estados e empresas existem para a satisfação de determinados interesses, não necessariamente coincidentes nem convergentes com os das pessoas – individualmente consideradas – cujos dados são tratados por seus algoritmos.

É importante destacar que algoritmos proporcionam benefícios muito além da velocidade na tomada de decisões. Como ensina Kahneman (2012, p. 280-286), estatísticas e fórmulas podem ser muito úteis, considerando que ajudam a compensar as limitações da racionalidade humana. Humanos, por exemplo, são incorrigivelmente inconsistentes em fazer julgamentos sumários de informação complexa. Estímulos despercebidos no ambiente interferem substancialmente em nossos pensamentos e ações, e essas influências flutuam de um momento a outro. Fórmulas não sofrem com tais problemas. Dado um mesmo *input*, elas sempre fornecem a mesma resposta. Frequentemente também propiciam avaliações e prognósticos mais precisos que os realizados por pessoas de carne e osso.

Entretanto, estatísticas e fórmulas podem embutir dados falsos ou imprecisos, falsas correlações – aparentes relações que não traduzem causa-efeito, com confusão entre correlação e causalidade, correlações que podem ser fruto de pura e simples discriminação, capazes de perpetuar injustiças. Como Pearl e Mackenzie (2018, p. 21) sumarizam, pessoas são mais inteligentes que seus dados. Estes, por si sós, não compreendem causas e efeitos; humanos, sim.

São notórios e caricatos os exemplos do *site*[14] e do livro *Spurious Correlations*, que mostram – em gráficos de impressionante coincidência estatística, repletos de dados precisos ano a ano – a aparente relação entre "a quantidade de filmes protagonizados por Nicolas Cage" e "o número de pessoas que se afogaram caindo numa piscina" – correspondência de 66,6% –; ou entre "a idade da vencedora do concurso *Miss America*" e "o número de assassinatos cometidos com o uso de vapor ou objetos quentes" – correspondência de 87,01% (VIGEN, 2015). Obviamente, são apenas coincidências estatísticas. Máquinas, no entanto, poderiam considerá-las verdadeiras e não meras coincidências.

Outro exemplo relativamente conhecido é o do robô Tay, um perfil feminino de inteligência artificial criado pela Microsoft para interagir com humanos no *Twitter*[15]. Tay foi retirada do ar em 24 horas, após se perceber que, ao lidar com o conteúdo postado por diversos usuários que com ela interagiam na rede social, passou a reproduzir, em suas publicações, o comportamento inadequado e os preconceitos dos usuários, com frases racistas e misóginas. As postagens dos demais perfis do *Twitter* foram captadas e tratadas pelos algoritmos de Tay como representativos de um comportamento padrão, ou "normalizado". Algo-

14 Disponível em: http://www.tylervigen.com/spurious-correlations. Acesso em: 30 nov. 2020.

15 Ver Veja (2016).

ritmos podem também confirmar e naturalizar preconceitos, a depender de quais sejam seus *inputs* e de como os processarão.

3. ALGORITMOS E PARADOXO DO *ESPELHO DE SENTIDO ÚNICO*

Em filmes policiais, é comum a cena do interrogatório realizado com o suspeito por uma dupla de policiais, enquanto diversos outros agentes acompanham tudo por detrás de um espelho de sentido único. Dentro da sala, o investigado vê na parede envidraçada apenas o reflexo de sua imagem; já no ambiente contíguo, o "espelho" se torna transparente, permitindo que o outro lado seja visto com perfeição.

Ao descrever a sociedade atual e sua relação com Estados e agentes econômicos pelos canais dos algoritmos, Pasquale observa que estes sabem tudo sobre os cidadãos, enquanto cidadãos pouco sabem o que Estados e agentes econômicos sabem sobre si nem o que fazem com essas informações. Ao ter seus dados pessoais captados e tratados, tudo o que o cidadão vê é a sua própria imagem no espelho (ou, mais exatamente, a forma como sua imagem é refletida). O indivíduo nada sabe sobre como o instrumento funciona, nem quais foram as informações captadas para que aquele "reflexo" fosse gerado. A alegoria do *one way mirror*, ou *espelho de sentido único*, baseia a sociedade da caixa-preta de que trata Pasquale (2015, p. 9): por detrás do espelho, há uma caixa repleta de segredos a que as pessoas comuns não têm acesso.

Zuboff (2019a) tem preocupação semelhante, ao discorrer sobre o que chama de "*capitalismo de vigilância*", que opera por meio de assimetrias sem precedentes no conhecimento e no poder acumulado por este. Corporações sabem tudo sobre as pessoas, mas suas operações são projetadas de modo a serem incognoscíveis para nós. Elas acumulam vastos domínios de novos conhecimentos *sobre* nós, mas não *para* nós. O capitalismo, em seu modelo atual, apropria-se da experiência humana

e a utiliza como material bruto para predizer comportamentos. Esses insumos são comprados e vendidos em um novo tipo de mercado de dados pessoais. E essas transações ocorrem quase que completamente sem nossa ciência (ZUBOFF, 2019b).

Nesse contexto, as decisões automatizadas, tomadas com base em algoritmos, são um ponto crucial. Quanto a esse aspecto, Mendes observa que a proteção do indivíduo contra a discriminação pelo processamento dos dados pessoais não se dá apenas pela proibição ou limitação do armazenamento de informações sensíveis e excessivas: "a proteção do indivíduo somente pode ser atingida com a garantia do direito de não se ficar sujeito a uma decisão individual automatizada" (MENDES, 2014, p. 160).

4. TRATAMENTO AUTOMATIZADO DE DADOS PESSOAIS E DISCRIMINAÇÃO NA LGPD

A LGPD – Lei n. 13.709, de 14 de agosto de 2018 – dispõe sobre a proteção de dados pessoais e altera a Lei n. 12.965, de 23 de abril de 2014 – Marco Civil da Internet.

Como é sabido, esse diploma tem forte inspiração no Regulamento n. 2016/679, conhecido como Regulamento Geral para a Proteção de Dados (GDPR, na sigla em inglês), do Parlamento Europeu e do Conselho da União Europeia (UE)[16].

Antes de entrar em vigor, a LGPD foi alterada pela Medida Provisória n. 869, de 27 de dezembro de 2018, e pela Lei n. 13.853, de 8

16 Vale registrar que a legislação europeia, na verdade, já aborda o tema do tratamento automatizado de dados desde muito antes. Exemplo disso é a Lei francesa n. 78-17, de 6 de janeiro de 1978, relativa ao *tratamento de dados, arquivos e liberdades*, que em seu artigo 2 e em diversos outros artigos já previa direitos do indivíduo contra o tratamento automatizado de dados pessoais. Disponível em: https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf. Acesso em: 9 out. 2020.

de julho de 2019. Ambas postergaram o início da vigência da LGPD, de 16 de fevereiro de 2020, para o segundo semestre do mesmo ano (BRUNA, 2019). Com a sanção da Lei n. 14.058, a LGPD finalmente entrou em vigor, em 18 de setembro de 2020[17].

Sobre decisões automatizadas, o art. 20 da LGPD, já com as alterações consolidadas pela MP n. 869/2018 e pela Lei n. 13.853/2019, estabelece que

> o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Da redação original, suprimiu-se a expressão "por pessoa natural"[18]. A alteração pode parecer singela à primeira vista, mas sua repercussão é muito relevante. Retirou-se a obrigação de que a revisão de uma decisão tomada exclusivamente com base no tratamento automatizado de dados seja feita por uma pessoa. Na prática, para que entes públicos ou privados atendam ao *caput* do art. 20 da LGPD num caso em que lhes seja solicitada a revisão de uma decisão automatizada, bastará que essa seja revisada por um outro algoritmo[19]. Em resumo, todo o processo de tratamento de

---

17 Ver Consultor Jurídico (2020).

18 A redação original, antes da MP n. 869/2018 e da Lei n. 13.853/2019, era a seguinte (destaque nosso): "Art. 20. O titular dos dados tem direito a solicitar revisão, *por pessoa natural*, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive de decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade."

19 Em interessante estudo sobre o processo legislativo que desaguou na Lei n. 13.853/2019 e sobre as propostas apresentadas por parlamentares para emendas à

dados pessoais poderá ser realizado por robôs, sem nenhuma interferência humana, nem mesmo quando solicitada a revisão pelo titular dos dados.

É interessante verificar que o Congresso Nacional aprovou a inclusão de um § 3º ao art. 20, a prever que

> a revisão de que trata o *caput* deste artigo deverá ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, que levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Esse dispositivo, entretanto, foi vetado pelo presidente da República, que assim apresentou suas razões de veto:

> A propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empre-

---

LGPD, identificou-se o seguinte: "O artigo 20 garante aos indivíduos o direito de solicitar a revisão de 'decisões tomadas unicamente com base em tratamento automatizado de dados pessoais'. Os parlamentares sugeriram treze emendas ao seu texto, cuja redação foi modificada com a edição da MP. A principal alteração diz respeito ao agente que deve realizar a revisão de uma decisão automatizada, quando esta for solicitada. Onze parlamentares propuseram que o artigo retornasse à sua redação original, incluindo-se, novamente, o qualificador 'por pessoa natural' às revisões previstas. A Proposta de Emenda n. 17 explica em sua justificativa que 'a Medida Provisória n. 869/2018 criou uma possibilidade bastante preocupante: a de que o direito de revisão a tratamentos automatizados de dados seja exercido, na prática, pelos mesmos mecanismos automatizados que geraram o erro em primeiro lugar'. A mesma justificativa é ecoada nas Propostas de Emenda n. 43, 50, 70, 83, 103, 130, 142, 151, e 158. A Proposta de Emenda n. 165 aponta ainda que reavaliar tais decisões, automatizadas, por processos também automatizados impede uma reavaliação efetiva, o que violaria o objetivo do próprio artigo." (FICO; MOTA; NASCIMENTO, 2019).

> sas, notadamente das *startups*, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária.

Os parágrafos do art. 20 têm a seguinte redação e não foram alterados pela MP n. 869/2018 nem pela Lei n. 13.853/2019:

> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
>
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Da leitura integral do dispositivo, tem-se que o *caput* do art. 20 da LGPD prevê um direito à revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais. Já os §§ 1º e 2º estatuem um direito à explicação sobre tais decisões. Veja-se, contudo, que o direito à revisão de decisões automatizadas já havia sido previsto, antes, no art. 5º, VI, da Lei n. 12.414/2011 – Lei do Cadastro Positivo[20].

A amplitude desses direitos – à revisão e à explicação – é assunto aberto a interpretação – como a que se propõe neste estudo.

---

20 "Art. 5º São direitos do cadastrado: (...) VI – solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados;"

A LGPD prevê expressamente o direito ao tratamento não discriminatório por decisões automatizadas. Essa previsão é extraída não só do art. 20 mas também dos arts. 1º, 2º, e principalmente do art. 6º[21], cujo inciso IX é categórico ao estatuir que as atividades de tratamento de dados pessoais deverão observar a boa-fé e o princípio da não discriminação, o qual consiste na *impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos*.

De modo diverso, o RGPD não prevê explicitamente um *princípio da não discriminação*. Todavia, o mesmo sentido das disposições da lei brasileira parece emergir de diversos dispositivos do diploma – como os arts. 5º e 22, além dos seus *consideranda* números 39 e 71 a 73 –, de modo a protegerem o titular do dado pessoal contra tratamentos potencialmente discriminatórios. Nessa linha estão os arts. 5º, 7º e 13, que versam, respectivamente, sobre tratamento adequado, livre consentimento e transparência[22]. A Diretiva (UE) n. 680/2016[23], relativa ao

---

21 "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei n. 13.853, de 2019) Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."

22 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 9 out. 2020.

23 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.POR&toc=OJ:L:2016:119:FULL. Acesso em: 9 out. 2020.

tratamento de dados pessoais *por agentes públicos* e especificamente *para fins penais*[24], também reconhece direitos ao indivíduo contra decisões individuais automatizadas (art. 11).

5. TRANSPARÊNCIA E A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A MP n. 869/2018 atendeu – ao menos em parte – a reivindicação de muitos quanto a uma relevante omissão da LGPD, acrescentando-lhe diversos dispositivos (arts. 55-A a 55-K) que criam e disciplinam o funcionamento da Autoridade Nacional de Proteção de Dados (ANPD). Os artigos que criam a ANPD foram mantidos pela Lei n. 13.853/2019.

O art. 55-A da LGPD cria a ANPD como órgão da administração pública federal, integrante da Presidência da República. A Lei n. 13.853/2019 incluiu três parágrafos no referido artigo, para declarar que a natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República (§ 1º); que a avaliação quanto a essa transformação deverá ocorrer em até dois anos da data da entrada em vigor da estrutura regimental da ANPD (§ 2º); e que o provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na Lei Orçamentária Anual e

24 Diferentemente do Regulamento, a Diretiva não tem aplicação imediata e depende da *transposição* – *i.e.*, da positivação nos ordenamentos de cada país, de acordo com os parâmetros da Diretiva. O processo de transposição da Diretiva (UE) n. 2016/680 tem sido lento, como se verifica no Relatório da Comissão Europeia divulgado em 6 de julho de 2019. Disponível em: http://europa.eu/rapid/press-release_IP-19-3030_pt.pdf. Acesso em: 9 out. 2020.

à permissão na Lei de Diretrizes Orçamentárias (§ 3º). Em seguida, o art. 55-B assegura à ANPD "autonomia técnica e decisória".

Autonomia técnica não é o mesmo que autonomia – ou independência – funcional. Sendo órgão da administração pública federal subordinado à Presidência da República, não é desprezível a possibilidade de ingerência indevida sobre questões que, a rigor, deveriam ser estritamente técnicas. Outrossim, a LGPD se dirige a qualquer pessoa, natural ou jurídica, de direito público ou privado, que promova o tratamento de dados pessoais. Dessa forma, o problema se amplia quando for o próprio Estado-Administração aquele contra quem pese a suspeita de tomar uma decisão automatizada ilicitamente discriminatória. O ideal é que seja transformada o quanto antes em entidade da administração pública federal indireta, submetida a regime autárquico especial, como prevê o § 1º do art. 55-A.

Como visto, a ANPD será o órgão responsável por realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais, nos casos em que o controlador não apresente informações claras e adequadas a respeito dos critérios e procedimentos utilizados para a decisão automatizada (art. 20, §§ 1º e 2º). A previsão de auditoria é importante, porquanto visa a impedir a recusa genericamente sustentada como segredo comercial e industrial, privando o titular dos dados de conhecer os critérios referentes à definição de seu perfil e às decisões decorrentes (BLUM; MALDONADO, 2019, p. 242).

Ao recusar a informação ao titular, o controlador poderá ser submetido a auditoria da ANPD sobre seus algoritmos. Aquele continuará a não ser informado – ao menos nesse primeiro momento – sobre os critérios utilizados no seu tratamento, mas a ANPD, promovendo a auditoria e constatando tratamento discriminatório, poderá aplicar as sanções previstas na lei. O problema é que determinadas penas muito pertinentes a tal espécie de infração, como a de *suspensão do exercício da atividade de tratamento dos dados pessoais*, foram vetadas pelo Presidente da República ao sancionar a Lei n. 13.853/2019, como se verá adiante.

Outrossim, embora não seja algo expressamente previsto, uma interpretação sistemática da LGPD permite concluir que, caso a auditoria da ANPD constate determinado tratamento automatizado de dados pessoais de cunho discriminatório, deverá informá-lo aos respectivos titulares, para que estes possam exercer seus direitos, individualmente, contra os agentes de tratamento, inclusive na esfera judicial – promovendo ações cíveis com pedidos de indenização, por exemplo. Compreensão diversa deixaria os titulares, individualmente considerados, completamente desinformados sobre as providências tomadas pela ANPD a partir de seu caso concreto e desprotegidos contra eventuais abusos praticados pelos controladores ou operadores.

O direito de ser informado a respeito de um tratamento discriminatório, aliás, deve ser reconhecido a todos os titulares dos dados tratados, e não somente àqueles que tenham solicitado informações a respeito dos critérios e procedimentos adotados para a decisão automatizada. Assim, em todos os casos de constatação de indevida discriminação no tratamento automatizado de dados pessoais, uma sanção necessária, a ser aplicada pela ANPD, é a de *publicização da infração, após devidamente apurada e confirmada a sua ocorrência* (art. 52, IV, da LGPD).

Além disso, nos termos do art. 55-J, compete à ANPD, entre diversas outras atividades, zelar pela proteção dos dados pessoais (inciso I), *editar regulamentos e procedimentos* sobre proteção de dados pessoais e privacidade (inciso XIII, incluído pela Lei n. 13.853/2019); e deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação da LGPD, as suas competências e os casos omissos (inciso XX, também incluído pela Lei n. 13.853/2019). Sucede que, conforme prevê o § 1º do mesmo artigo, a ANPD, ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, deverá observar a exigência de *mínima intervenção*, assegurados os funda-

mentos e os princípios previstos nessa lei e o disposto no art. 170 da Constituição Federal[25].

Considerando que o controlador, ao ser questionado sobre determinado tratamento automatizado, pode invocar os segredos comercial e industrial como óbice ao fornecimento de *todas* as informações pretendidas pelo solicitante (art. 20, § 1º, da LGPD), tanto a edição de normas sobre o tema (art. 55-J) quanto a realização de auditoria nos algoritmos (art. 20, § 2º) serão particularmente tormentosos, porquanto necessariamente balizados pela *mínima intervenção* e pelos princípios do art. 170 da Carta da República.

De acordo com o art. 52 da LGPD[26], os agentes de tratamento de dados, caso descumpram as normas previstas na lei, ficarão sujeitos às seguintes sanções administrativas, a serem aplicadas pela ANPD (incisos I a VI): advertência; multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil, limitada a R$ 50.000.000,00 por infração; multa diária, observado o

---

25 "Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: I – soberania nacional; II – propriedade privada; III – função social da propriedade; IV – livre concorrência; V – defesa do consumidor; VI – defesa do meio ambiente, inclusive mediante tratamento diferenciado conforme o impacto ambiental dos produtos e serviços e de seus processos de elaboração e prestação; (Redação dada pela Emenda Constitucional n. 42, de 19-12-2003) VII – redução das desigualdades regionais e sociais; VIII – busca do pleno emprego; IX – tratamento favorecido para as empresas de pequeno porte constituídas sob as leis brasileiras e que tenham sua sede e administração no País. (Redação dada pela Emenda Constitucional n. 6, de 1995) Parágrafo único. É assegurado a todos o livre exercício de qualquer atividade econômica, independentemente de autorização de órgãos públicos, salvo nos casos previstos em lei."

26 O início da vigência das sanções da LGPD (arts. 52, 53 e 54) foi adiado para 1º de agosto de 2021, conforme previsto pelo art. 20 da Lei n. 14.010, de 10 de julho de 2020.

limite total de R$ 50.000.000,00; publicização da infração, após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a sua regularização; e eliminação dos dados pessoais a que se refere a infração.

O Congresso Nacional havia aprovado três outras espécies de sanção aplicáveis pela ANPD: suspensão parcial ou total do funcionamento do banco de dados pelo período máximo de seis meses, prorrogável por igual período até a regularização da atividade de tratamento pelo controlador; suspensão do exercício da atividade de tratamento dos dados pessoais pelo período máximo de seis meses, prorrogável por igual período; e proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. Essas punições foram vetadas (incisos VII, VIII e IX do art. 52) pelo Presidente da República ao sancionar a Lei n. 13.853/2019, ao argumento de que poderiam gerar insegurança aos controladores e "impossibilitar a utilização e tratamento de bancos de dados essenciais a diversas atividades, a exemplo das aproveitadas pelas instituições financeiras (...), podendo acarretar prejuízo à estabilidade do sistema financeiro nacional".

6. ALGORITMO, DISCRIMINAÇÃO E TRANSPARÊNCIA

Segundo a Constituição Federal, um dos objetivos fundamentais da República é promover o bem de todos, "sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação" (art. 3º, IV). Mesmo no preâmbulo o constituinte já declara que seu propósito é

> instituir um Estado Democrático, destinado a assegurar o exercício dos direitos sociais e individuais, a liberdade, a segurança, o bem-estar, o desenvolvimento, a igualdade e a justiça como valores supremos de uma sociedade fraterna, pluralista e sem preconceitos.

A discriminação é repudiada também em diversos outros dispositivos da Carta Política: art. 5º ("XLI – a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais; XLII – a prática do racismo constitui crime inafiançável e imprescritível, sujeito à pena de reclusão, nos termos da lei"); art. 7º ("XXXI – proibição de qualquer discriminação no tocante a salário e critérios de admissão do trabalhador portador de deficiência"); e art. 227, *caput* ("É dever da família, da sociedade e do Estado (...) colocá-los [crianças e adolescentes] a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão"), § 1º ("II – criação de programas de prevenção e atendimento especializado para as pessoas portadoras de deficiência física, sensorial ou mental, (...) com a eliminação de (...) todas as formas de discriminação") e § 6º ("Os filhos, havidos ou não da relação do casamento, ou por adoção, terão os mesmos direitos e qualificações, proibidas quaisquer designações discriminatórias relativas à filiação"). Até em suas relações internacionais, a República Federativa do Brasil rege-se, entre outros princípios, pelo "repúdio ao terrorismo e ao racismo" (art. 4º, VIII).

Ao estatuir explicitamente a promoção do bem de todos, incompatível com preconceitos de origem, raça, sexo, cor e idade (art. 3º, IV), a Constituição Federal não apresentou um rol fechado de fatores que podem caracterizar um tratamento discriminatório. Vários aspectos podem ser utilizados para, ilicitamente, discriminar: preferências político-partidárias, convicções futebolísticas ou, até mesmo, rendimento mensal familiar.

A rigor, o texto constitucional tampouco impediu que fatores específicos, tais como origem, raça, sexo, cor e idade, sejam explorados para dispensar tratamentos diferentes a pessoas em situações distintas. Esses são apenas os exemplos mais emblemáticos, em que a discriminação costuma ser inconstitucional e ilegal. Mas é perfeitamente possível que eles, assim como quaisquer outros critérios, sejam usados para, constitucional e licitamente, oferecer tratamento diferenciado a um grupo – desde que haja motivo racionalmente demonstrável para isso.

Noutras palavras, deve haver relação lógica entre o que Celso Antônio Bandeira de Mello chama de *fator de discrímen* e o tratamento diferenciado concretamente havido. A princípio, não se pode tratar homens e mulheres de forma distinta; excepcionalmente, presente um motivo racionalmente justificável – como, por exemplo, a realização de um concurso para integrantes da polícia militar feminina – a participação de homens pode ser limitada. Qualquer critério de discriminação pode ser juridicamente válido, desde que seja racionalmente justificável. Deve haver, como ensina o jurista (2018, p. 18), "pertinência lógica com a diferenciação procedida".

É precisamente aí que reside a fragilidade das decisões automatizadas, ou tomadas com base em tratamento de dados pessoais por algoritmos. Traçar perfis pessoais, profissionais, de consumo, de crédito ou referentes a aspectos da personalidade (art. 20 da LGPD) nada mais é que identificar determinados *fatores de discrímen* que permitirão inserir pessoas ou grupos de pessoas dentro de certas categorias, para, a partir daí, tomarem-se decisões. Se a escolha desses fatores, ou de quaisquer outros, assentada numa relação de pertinência lógica, justifica a discriminação realizada, é questão que somente poderá ser aferida a partir do perfeito conhecimento a respeito do critério exatamente eleito e do tratamento concretamente dispensado.

Como ensina Frazão, sem transparência, a programação pode estar permeada de vieses e preconceitos dos programadores, intencionais ou não, que podem levar a erros de diagnóstico ou a graves discriminações. Além disso, é possível que correlações encontradas no processamento sejam consideradas equivocadamente causalidades, o que pode reforçar discriminações – não justificadas racionalmente (FRAZÃO; TEPEDINO; OLIVA, 2019, p. 39).

Decisões que afetem a esfera de direitos de alguém, automatizadas ou não, precisam ser racionalmente justificáveis. A transparência, assim, é um pressuposto para que uma decisão – tomada por uma pessoa ou

um robô – seja racionalmente justificável. Se não se conhece como foi tomada a decisão, não há como se afirmar se o procedimento foi lícita ou ilicitamente discriminatório.

7. A LGPD E A TUTELA DOS DIREITOS DO TITULAR DO DADO CONTRA TRATAMENTOS POTENCIALMENTE DISCRIMINATÓRIOS

A LGPD prevê ao titular dos dados pessoais uma série de direitos, entre os quais o de *obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição* (art. 18):

> I – confirmação da existência de tratamento;
>
> II – acesso aos dados;
>
> III – correção de dados incompletos, inexatos ou desatualizados;
>
> IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
>
> (...)
>
> § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.
>
> § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

Para que se defina a real amplitude da proteção do titular em relação ao tratamento automatizado de seus dados, o art. 18 da LGPD deve ser lido em conjunto com os demais dispositivos da lei. Com efeito, ao lado do art. 18, é precisamente para impedir o tratamento discriminatório que se erigem os arts. 1º, 2º, 6º e 20. E, para que se conceba uma tutela adequada aos direitos do titular dos dados em face de uma decisão automatizada que lhe possa causar indevido prejuízo, os referi-

dos artigos devem ser interpretados sistematicamente, correlacionados entre si e em harmonia com os diversos dispositivos da Constituição Federal sobre o tema.

Desse modo, uma interpretação possível é a de que a LGPD criou, para o titular, o direito à *explicação* – sobre quais, como e por que dados foram tratados pelo algoritmo – e o direito à *oposição* – sobre quais, de que forma e com que finalidade dados foram tratados.

Ao mesmo tempo, esse diploma criou, para o controlador que realiza o tratamento de dados para a tomada de decisões automatizadas, o dever de *transparência*. Esse dever se traduz na *explicabilidade* – ou seja, o tratamento e o seu resultado – leia-se, a decisão tomada – devem ser passíveis de explicação pelo controlador, o que pressupõe seu conhecimento sobre as operações – *inputs* e *outputs* – realizadas pelo algoritmo. Outra faceta do dever de transparência é a necessária *inteligibilidade* das informações prestadas a quem o solicite, inclusive à ANPD, se for o caso – *i.e.*, a forma de tratamento de dados e seu resultado devem ser claramente compreensíveis à autoridade ou ao usuário que solicita explicações.

Essa interpretação da LGPD está em harmonia com o estudo realizado pelo Grupo de Trabalho sobre Proteção de Dados Pessoais da Comissão Europeia (GT do art. 29 para a Proteção de Dados[27]) intitulado *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*, que recomendou uma série de práticas aos responsáveis pelo tratamento, de forma a cumprirem satisfatoriamente os requisitos constantes no GDPR relativos à definição de perfis e às decisões automatizadas.

27 Trata-se de grupo de trabalho instituído com base no art. 29 da Diretiva n. 95/46/CE. É um órgão consultivo europeu independente em matéria de proteção de dados e privacidade e suas atribuições estão descritas no art. 30 da Diretiva n. 95/46/CE e no art. 15 da Diretiva n. 2002/58/CE.

Esse estudo orienta os responsáveis pelo tratamento de dados que utilizem meios claros e abrangentes para fornecer informações ao titular, evitando explicações matemáticas complexas sobre o funcionamento dos algoritmos ou da aprendizagem automática (UNIÃO EUROPEIA, p. 35). Recomendou-se também que os responsáveis pelo tratamento de dados facilitem o acesso às seguintes informações: (a) categorias de dados usados nos perfis; (b) fontes dos dados; (c) forma de criação dos perfis, incluídas as estatísticas; (d) motivo de relevância do perfil para a decisão automatizada; (e) modo como as informações foram usadas no caso específico de determinado titular.

Ainda sobre o dever de transparência, não há como discordar das conclusões de Frazão, para quem a LGPD, assim como o GDPR, criaram um verdadeiro *ônus da prova* para os controladores a respeito da legitimidade no tratamento automatizado de dados que promoverem. Como decorrência de seu dever de transparência, recairá neles, portanto, o ônus da prova sobre:

> (i) os dados que são coletados, de que fonte e de que maneira, (ii) quais as linhas gerais de programação dos algoritmos e seus objetivos, (iii) como se deu a programação e o desenvolvimento do algoritmo, (iv) se o algoritmo pode ou não modificar seu próprio código, (v) se tais modificações são previsíveis ou ao menos verificáveis, (vi) quais as categorias relevantes dos perfis e os critérios para cada uma delas, (vii) quais são os *outputs* do processo decisório e como avaliar a sua adequação e acurácia, (viii) se há mecanismos de *feedback*, (viii) se há intervenção humana e em que nível, (ix) quais são os principais impactos e riscos para os titulares de danos, (x) que medidas foram tomadas para conter tais riscos. (FRAZÃO, 2018b)

À primeira vista pode parecer excessiva a lista de aspectos sobre os quais o controlador dos dados deverá sempre oferecer informações claras;

entretanto, essa impressão não sobrevive à constatação de que somente o controlador dispõe dessas informações e que, se é de seu interesse usufruir das facilidades e benefícios propiciados pela tecnologia, é sua responsabilidade impedir que ela cause danos aos respectivos titulares.

8. ALGORITMOS, INTELIGÊNCIA ARTIFICIAL E *MACHINE LEARNING*

O dever de transparência no tratamento automatizado de dados ganha escala ao se inserirem na equação os recursos tecnológicos de inteligência artificial (IA), redes neurais e *machine learning*.

Não sendo o foco específico do presente artigo, embora não haja consenso nem mesmo entre especialistas em relação a uma definição precisa do que seja IA (PEIXOTO; ZUMBLICK, 2019, p. 74), pode-se sucintamente afirmar tratar-se de um conjunto de métodos para detecção e aplicação de padrões em dados, de forma automática, capaz de projetar dados futuros e tomar decisões. Em suma, a IA permite que computadores aprendam por conta própria, por meio de algoritmos que identificam padrões em dados fornecidos (PEIXOTO; ZUMBLICK, 2019, p. 20-21).

Chama-se *machine learning*, por sua vez, a habilidade dos sistemas de IA de adquirir conhecimento próprio ao extrair padrões de dados não processados. Um algoritmo de *machine learning* permite identificar padrões e construir modelos para prever coisas, sem regras ou modelos explicitamente pré-programados (PEIXOTO; ZUMBLICK, 2019, p. 88-89). Redes neurais são um tipo de sistema computacional inspirado nas propriedades básicas de neurônios biológicos, composta por muitas unidades interconectadas que recebem e enviam *inputs* e *outputs*. A propriedade-chave desse tipo de sistema é a possibilidade de modificação do peso associado a cada interconexão, com base na experiência. De modo bastante simplificado, redes neurais são a forma pela qual ocorre o aprendizado de máquina profundo, ou *deep learning*,

que envolve o treinamento de redes neurais em muitas camadas e unidades. Exemplos de aplicações atuais de *deep learning* são os sistemas de carros autônomos, programas de reconhecimento facial e de tradução simultânea (PEIXOTO; ZUMBLICK, 2019, p. 97-100).

Quando se fala em tratamento automatizado de dados, não se está falando necessariamente na operação que um algoritmo isolado realiza sobre os dados de determinada pessoa. Via de regra, o processamento das informações é feito por diversos algoritmos, que trabalham com vasta quantidade de dados (*big data analysis*) em paralelo e não somente relacionados ao indivíduo específico objeto de determinada decisão. Muitos outros dados de uma miríade de fontes são utilizados como insumos para os cálculos computacionais que deságuam numa solução específica de interesse para determinada pessoa. Se já não constituiu tarefa banal atribuir transparência a esse procedimento, maior dificuldade surgirá para explicar o tratamento de dados que foi realizado por algoritmos de inteligência artificial ou que aprenderam a se redesenhar – ou seja, a reconfigurarem sozinhos a forma com que processam as informações que os alimentam.

Exatamente por isso desponta a importância atual dos estudos sobre *Explainable Artificial Intelligence* (XAI), ou *Inteligência Artificial Explicável*. São pesquisas em curso (SCHMELZER, 2019) sobre o desenvolvimento de sistemas não só inteligentes mas sobretudo *inteligíveis*, isto é, cujo funcionamento e cujos processos de auto-(re)definição possam ser explicados pelo próprio algoritmo e compreendidos pelo homem.

9. CONCLUSÃO

O tratamento de dados pessoais automatizado é uma realidade atual e que tende a repercutir ainda mais intensamente na vida de todos, como consequência do fato de que Estados e empresas empregam essa

tecnologia como ferramenta cada vez mais essencial à realização de suas atividades. Para estes, as vantagens do uso de algoritmos, sobretudo para a definição de perfis pessoais, são imensas. Para os cidadãos, em paralelo, os riscos são igualmente imensos.

A LGPD não descuidou da tutela dos interesses do titular do dado pessoal frente a um tratamento potencialmente discriminatório. Mas a lei brasileira não é imune a críticas. No plano positivo-normativo, as principais deficiências correspondem aos limites do controle a ser exercido pela ANPD e à ausência de obrigação de que a revisão de uma decisão tomada exclusivamente com base no tratamento automatizado de dados seja feita por um *ser humano*.

O maior problema que se erige sobre o tema da discriminação algorítmica, contudo, diz respeito à realização concreta dos direitos do titular que venha a ser prejudicado por um tratamento indevidamente discriminatório, sobretudo seu direito de explicação – e seu correlato dever de transparência por parte do controlador –, considerando-se as próprias peculiaridades da tecnologia hoje empregada para o tratamento de dados pessoais. Explicação – ou explicabilidade – e transparência são as palavras-chave para que qualquer decisão amparada no tratamento de dados pessoais possa ser identificada como racionalmente justificável ou ilicitamente discriminatória. Implementar tais atributos ao tratamento automatizado de dados pessoais é o desafio que se apresenta a controladores, operadores, autoridades responsáveis pela aplicação da lei e aos próprios titulares dos dados pessoais.

REFERÊNCIAS

ANGWIN, Julia; LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren. Machine Bias. There is software that is used across the county to predict future criminals. And it is biased against blacks. *ProPublica*.

Nova Iorque, 23 maio 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em: 9 out. 2020.

BBC. O plano chinês para monitorar – e premiar – o comportamento de seus cidadãos. *BBC News Brasil*, 27 nov. 2017. Disponível em: https://www.bbc.com/portuguese/internacional-42033007. Acesso em: 9 out. 2020.

BLUM, Opice; MALDONADO, Viviane Nóbrega (Orgs.). *Comentários ao GDPR*. São Paulo: Revista dos Tribunais, 2018.

BLUM, Opice; MALDONADO, Viviane Nóbrega (Orgs.). *LGPD*: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019.

BRASIL, Ministério da Justiça e Segurança Pública. *Decolar.com é multada por prática de geo pricing e geo blocking*. 18 jun. 2018. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-51. Acesso em: 9 out. 2020.

BRUNA, Sérgio Varella. A LINDB e a entrada em vigor da Lei de Proteção de Dados. *Jota*. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-lindb-e-a-entrada-em-vigor-da-lei-de-protecao-de-dados-10012019. Acesso em: 9 out. 2020.

CASEY, Bryan; FARHANGUI, Ashkon; VOGL, Roland. Rethinking Explainable Machines: The GDPR's "Right to Explanation" Debate and the Rise of Algorithmic Audits in Enterprise. *Berkeley Technology Law Journal,* v. 34, 2019. Disponível em: https://ssrn.com/abstract=3143325. Acesso em: 9 out. 2020.

CONSULTOR JURÍDICO. *Após sanção do governo, Lei Geral de Proteção de Dados começa a valer*. 18 set. 2020. Disponível em: https://www.

conjur.com.br/2020-set-18/sancao-governo-lgpd-comeca-valer-nesta-sexta. Acesso em: 9 out. 2020.

CORREIO. Salvador registra primeira prisão por reconhecimento facial. *Correio*, Salvador, 6 mar. 2019. Disponível em: https://www.correio24horas.com.br/noticia/nid/salvador-registra-primeira-prisao-por-reconhecimento-facial/. Acesso em: 9 out. 2020.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados comentada*. São Paulo: Thomson Reuters Brasil, 2018.

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*, 10 ago. 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G. Acesso em: 9 out. 2020.

DEMARTINI, Felipe. Metrô de SP cobre câmeras que coletavam dados biométricos dos usuários. *Canaltech*, 5 out. 2018. Disponível em: https://canaltech.com.br/seguranca/metro-de-sao-paulo-cobre-cameras-que-coletavam-dados-biometricos-dos-usuarios-124188/. Acesso em: 9 out. 2020.

DOMINGOS, Pedro. *O algoritmo mestre*. São Paulo: Novatec, 2017.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

FICO, Bernardo de Souza Dantas; MOTA, Juliana da Cunha; NASCIMENTO, Bárbara Emidio. LGPD: as propostas de emenda à Medida Provisória 869/2018. *Jota*, 9 abr. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lgpd-as-propostas-de-emenda-a-medida-provisoria-869-2018-09042019. Acesso em: 9 out. 2020.

FRAZÃO, Ana. Geopricing e geoblocking: as novas formas de discriminação de consumidores. *Jota*, 15 ago. 2018. Disponível em: https://www.

jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/geopricing-e-geoblocking-as-novas-formas-de-discriminacao-de-consumidores-15082018. Acesso em: 9 out. 2020.

FRAZÃO, Ana. Nova LGPD: ainda sobre a eficácia do direito à explicação e à oposição. *Jota*, 26 dez. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-ainda-sobre-a-eficacia-do-direito-a-explicacao-e-a-oposicao-26122018. Acesso em: 9 out. 2020.

FRAZÃO, Ana. Plataformas digitais, *Big Data* e riscos para os direitos da personalidade. *In*: TEPEDINO, Gustavo; MENEZES, Joyceane. *Autonomia privada, liberdade existencial e direitos fundamentais*. Belo Horizonte: Forum, 2019. p. 333-349.

FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

GAMA, Aliny. Reconhecimento facial por app captura 42 foragidos no Carnaval de Salvador. *UOL*, 26 fev. 2020. Disponível em: https://www.uol.com.br/carnaval/2020/noticias/redacao/2020/02/26/reconhecimento-facial-por-app-captura-42-foragidos-no-carnaval-de-salvador.htm?cmpid=copiaecola. Acesso em: 9 out. 2020.

HERN, Alex. Google's solution to accidental algorithmic racism: ban gorillas. *The Guardian*, 12 jan. 2018. Disponível em: https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people. Acesso em: 9 out. 2020.

HOUAISS, Antônio. *Dicionário Houaiss da Língua Portuguesa*. Rio de Janeiro: Objetiva, 2001.

KAHNEMAN, Daniel. *Rápido e devagar*. São Paulo: Objetiva, 2012.

MELLO, Celso Antônio Bandeira de. *O conteúdo jurídico do princípio da igualdade*. 3. ed. São Paulo: Malheiros, 2008.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. Cambridge: Harvard University Press, 2015.

PEARL, Judea; MACKENZIE, Dana. *The Book of Why*: the new science of cause and effect. Londres: Penguin Books, 2018.

PEIXOTO, Fabiano Hartmann; ZUMBLICK, Roberta. *Inteligência artificial e direito*. 1. ed. Curitiba: Alteridade, 2019.

SALI, Felipe. China vai barrar viagens de avião de quem tiver "pontuação social" ruim. *Super Interessante*, 19 mar. 2018. Disponível em: https://super.abril.com.br/comportamento/china-vai-barrar-viagens-de-aviao-de-quem-tiver-pontuacao-social-ruim/. Acesso em: 9 out. 2020.

SCHMELZER, Ron. Understanding Explainable AI. *Forbes*, 23 jul. 2019. Disponível em: https://www.forbes.com/sites/cognitiveworld/2019/07/23/understanding-explainable-ai/#46ffa4197c9e. Acesso em: 9 out. 2020.

TARDE, A. Homens são capturados após serem flagrados por reconhecimento facial. *A Tarde*, 1º ago. 2019. Disponível em: http://atarde.uol.com.br/bahia/salvador/noticias/2079913-homens-sao-capturados-apos-serem-flagrados-por-reconhecimento-facial. Acesso em: 9 out. 2020.

TRINDADE, Rodrigo. Grande Irmão: China proibiu 23 milhões de viagens de avião ou trem em 2018. *UOL*, Tecnologia, 3 mar. 2019. Disponível em: https://noticias.uol.com.br/tecnologia/noticias/reda

cao/2019/03/03/grande-irmao-china-proibiu-23-milhoes-de-viagens-de-aviao-ou-trem-em-2018.htm. Acesso em: 9 out. 2020.

UNIÃO EUROPEIA. Grupo de Trabalho para a proteção das pessoas no que diz respeito ao tratamento de dados pessoais. *Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679*. (Disponível também em inglês: Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679). Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053. Acesso em: 9 out. 2020.

VEJA. *Exposto à internet, robô da Microsoft vira racista em 1 dia*. 24 mar. 2016. Disponível em: https://veja.abril.com.br/tecnologia/exposto-a-internet-robo-da-microsoft-vira-racista-em-1-dia/. Acesso em: 9 out. 2020.

VIGEN, Tyler. *Spurious correlations*. Nova Iorque: Hachette Books, 2015. E-book.

ZANON, João Carlos. *Direito à proteção de dados pessoais*. São Paulo: Revista dos Tribunais, 2013.

ZUBOFF, Shoshana. *The age of surveillance capitalism*: the fight for a human future at the new frontier of power. Nova Iorque: Public Affairs, 2019. E-book.

ZUBOFF, Shoshana. "Surveillance capitalism" has gone rogue. We must curb its excesses. *The Washington Post*, 24 jan. 2019. Disponível em: https://www.washingtonpost.com/opinions/surveillance-capitalism-has-gone-rogue-we-must-curb-its-excesses/2019/01/24/be463f48-1ffa-11e9-9145-3f74070bbdb9_story.html?noredirect=on&utm_term=.a26d8b7ed89c. Acesso em: 9 out. 2020.

DADOS DE TROIA

Aline Seabra Toschi[1]
Herbert Emílio Araújo Lopes[2]

RESUMO

A Lei Geral de Proteção de Dados (LGPD) foi elaborada com o intuito de garantir a transparência e a utilização adequada de dados pessoais, bem como proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural. Diante disso, este artigo tem como objetivo analisar se o tratamento dispensado aos dados pessoais sensíveis pela aludida norma pode ensejar lesão a preceitos constitucionais relativos à proteção de dados pessoais. A ausência de restrições relativa ao tratamento desses dados pelo Estado, conforme previsão dos Decretos n. 9.662/2019 e

1 Mestre em Ciências Penais pela UFG. Doutoranda em Direito pelo UniCEUB. Professora de Processo Penal e de Processo Constitucional. Coordenadora do estágio do curso de direito do Centro Universitário de Anápolis.

2 Mestre. Advogado. Coordenador do curso de direito do Centro Universitário de Anápolis e professor nas disciplinas de Direito Civil.

10.046/2019, pode transformá-los em um cavalo de Troia para as garantias individuais constitucionais.

Palavras-chave: Lei Geral de Proteção de Dados. Dados sensíveis. Garantias individuais. Tratamento de dados.

ABSTRACT

Starting from the purpose of the General Data Protection Law (LGPD), this article aims to analyze whether the treatment of sensitive personal data by such law may cause injury to constitutional precepts related to the protection of personal data. The absence of restrictions in the treatment of sensitive data by the State, as provided for in Decrees n. 9.662/2019 and n. 10.046/2019, can make these data work as a Trojan horse to individual constitutional guarantees.

Keywords: General data protection law. Sensitive data. Constitutional individual guarantees. Data processing.

1. INTRODUÇÃO

A edição da Lei Geral de Proteção de Dados (LGPD) – Lei n. 13.709/2018 – não resolve todos os problemas relativos à captação, ao tratamento e ao compartilhamento de dados, uma vez que exclui de seu âmbito os coletados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, aos quais se exigiu a edição de um diploma legal específico.

Ainda que a LGPD represente um avanço, há que se considerar a persistência de problemas relativos ao cumprimento desse regramento, bem como o mau uso e a custódia dos dados pessoais. A questão principal abordada neste artigo refere-se ao tratamento dispensado aos dados pes-

soais e aos dados sensíveis quando utilizados pela administração pública tendo em vista a preservação e garantia da segurança pública e nacional, bem como a utilização na investigação e no processamento criminal.

Após a compreensão do conceito de dados pessoais e dados pessoais sensíveis, analisa-se a exclusão de sua proteção, quando necessário, em geral, à garantia da ordem pública e ao andamento da investigação criminal, nos termos do inciso III do art. 4º da LGPD.

O *General Data Protection Regulation* (GDPR), regulamento geral de proteção de dados da União Europeia (UE), no qual a legislação nacional se baseou, também exclui de seu âmbito de ação os dados usados para a segurança pública e nacional, assim como para a investigação criminal. Exige, ainda, a proporcionalidade na determinação de captação e tratamento das informações, o que leva à autodeterminação informativa.

Mesmo nos casos de exclusão de proteção, conforme previsto na LGPD, a proporcionalidade e a autodeterminação informativa são princípios que devem acompanhar o tratamento de dados pessoais, principalmente quando parte da atuação estatal para assuntos de seu interesse, como a segurança pública, segurança nacional e investigações criminais.

Examina-se também a necessidade de imposição de limitação ao tratamento de dados pelo Estado. Exemplo disso é o caso da *Cambridge Analytica*, o qual demonstra bem como a quebra de sigilo dos dados pessoais sensíveis e sua utilização podem causar prejuízos numa sociedade democrática.

Também serão analisadas duas ações do Supremo Tribunal Federal (STF), ocorridas antes da vigência da LGPD. a Ação Direta de Inconstitucionalidade (ADI) n. 6.387 e a Arguição de Descumprimento de Preceito Fundamental (ADPF) n. 722, nas quais o STF decidiu que, mesmo para o cumprimento dos deveres do Estado quanto à segurança pública e à nacional, não se pode prescindir dos limites constitucionais legais. A exigência de preservação da proporcionalidade e da razoabilidade no tratamento de dados pessoais, em respeito ao direito da

intimidade e da vida privada e, consequentemente, à autodeterminação informativa e à dignidade humana, deve ser observada para não se colocar em risco a democracia.

Apesar da clarividente hierarquia normativa brasileira, alguns dispositivos legais podem minar o respeito aos princípios constitucionais afetos à proteção e ao tratamento de dados pessoais, a depender da sua aplicação por parte do Estado, do qual o Decreto n. 10.046/2019 é exemplo.

2. A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Numa sociedade pautada no mundo virtual, que abrange desde as compras *on-line* às redes sociais, existe um espaço repleto de informações e dados pessoais que vagam em um universo ilimitado de possibilidades quanto a sua destinação.

A revolução digital vivenciada é marcada pela formação de conexões inteligentes entre pessoas, pessoas e coisas ou até mesmo entre coisas e coisas.

A partir dessa hiperconectividade, uma vasta quantidade de dados é coletada, processada, compartilhada, tratada e armazenada em bancos de dados utilizados por empresas de tecnologia com as mais diversas finalidades, caracterizando a figura do *Big Data*[3]. Diante da variedade de informações que chegam em volumes crescentes e com velocidade cada vez maior, o *Big Data* é uma ferramenta valiosa não só para o mercado

3 Segundo Santos (2019), "o *Big Data* é mais que um emaranhado de dados, pois é essencialmente relacional. Isso não é novo – para a tristeza daqueles que acreditam que a internet mudou todas as coisas. O que a internet fez foi dar uma nova dimensão a esse fenômeno, transformando-o. Para bem entender essas transformações, precisamos compreender que o *Big Data* somos nós".

tech mas para o Estado, já que funciona como um navegador entre o emaranhado de dados existentes na rede mundial de computadores.

A fim de garantir a transparência e a utilização adequada de dados, principalmente os relacionados à pessoa humana, a LGPD foi criada e entrou em vigor em setembro de 2020.

De acordo com o Serviço Federal de Processamento de Dados (Serpro), a autoridade nacional de proteção de dados pessoais, essa lei, ao estabelecer requisitos e responsabilidades para o tratamento de dados pessoais, acaba por definir, de forma clara, sua finalidade, que é proporcionar segurança jurídica no tratamento desses dados.

2.1 DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

De acordo com o art. 5º, I, da LGPD, dados pessoais são aqueles que permitem identificar uma pessoa. Já os sensíveis, conforme o inciso II do mesmo artigo, são os relativos à origem racial ou étnica, à convicção religiosa, à opinião política, à filiação a sindicato ou à organização de caráter religioso, à opinião filosófica ou à opinião política, à saúde ou à vida sexual, às informações genéticas e biométricas.

A importância da compreensão desses dados passa pelas exceções legais de requisitos e, consequentemente, no âmbito de proteção no tratamento. Quanto a este aspecto, a própria LGPD traz exceções, como no art. 4º, III, que exclui os dados pessoais utilizados pelo Estado com a finalidade exclusiva de segurança pública, defesa nacional, segurança do Estado ou de investigação e repressão criminal. Essas exceções não podem ser analisadas de forma isolada aos princípios relativos à informação e à privacidade, previstos na Constituição Federal, mormente quando utilizados pelo Estado.

Cumpre esclarecer que, como a LGPD não se aplica aos casos elencados no art. 4º, os fundamentos relativos ao tratamento de dados,

previstos no art. 2º[4] da Lei, também não. Todavia, isso não significa que o tratamento fora das hipóteses da LGPD não se submeta a nenhuma limitação normativa.

O tratamento de dados nas hipóteses do art. 4º submete-se aos princípios constitucionais da privacidade, do sigilo das informações, da dignidade humana e da proporcionalidade na mesma medida que o tratamento de dados regidos pela LGPD submete-se aos fundamentos previstos no art. 2º da Lei.

A UE exemplifica a limitação normativa nas hipóteses em que o tratamento de dados pessoais não se submete à proteção estatal por normativa específica, como é o caso da LGPD. Nesse sentido o GDPR, assim como a lei brasileira, excluiu do âmbito de proteção no tratamento – portanto, fora das determinações do regulamento – aqueles que possam ser utilizados para fins de prevenção, investigação, detecção e repressão de infrações penais, bem como os que possam ser utilizados para a prevenção à segurança pública (art. 2º, *d*), já que o direito à proteção desses não é absoluto.

O item 1 do art. 4º do regulamento dispõe que são considerados dados pessoais as informações que levam à identificação de uma pessoa, tais como nome, número de identificação, localização, identificadores eletrônicos, elementos sobre a identidade física, fisiológica, genética, mental, econômica, cultural e social.

Entretanto, o item 1 do art. 9º do regulamento europeu veda o

---

4 "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; II – a autodeterminação informativa; III – a liberdade de expressão, de informação, de comunicação e de opinião; IV – a inviolabilidade da intimidade, da honra e da imagem; V – o desenvolvimento econômico e tecnológico e a inovação; VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais."

tratamento de dados relativos à origem racial ou étnica, às opiniões políticas, às convicções religiosas ou filosóficas, à filiação sindical, à saúde, à vida sexual, à orientação pessoal, às informações genéticas e biométricas.

Em conformidade com a disposição do art. 2º, *d*, do GDPR, o item 2 do art. 9º explica que estão fora da proibição de tratamento os dados que forem necessários para um interesse público importante (alínea *g*, item 2, do art. 9º).

Interessante destacar que, de todas as hipóteses trazidas no item 2 do art. 9º do GDPR, o item acima se equipara aos elencados na LGPD[5], com exceção das questões ligadas à saúde pública ou à defesa em processo judicial.

Uma característica que chama atenção é a determinação do uso da proporcionalidade: se o tratamento de dados pessoais sensíveis for necessário para o interesse público, deve ser proporcional ao objetivo visado, respeitando-se, sempre, a proteção dos dados pessoais e os direitos fundamentais e interesses do titular. Dessa forma, ainda que relevante o "interesse público", este não pode sobrepor-se aos direitos fundamentais do indivíduo.

Quanto aos dados pessoais passíveis de tratamento para o interesse da segurança pública, também não abarcados pela proteção no tratamento de dados, o art. 23, item 1, *d*, do GDPR dispõe que as limitações à proteção no tratamento de dados para o fim de prevenir, investigar, detectar e reprimir infrações penais e de prevenir ameaças à segurança pública devem levar em consideração os direitos e liberdades fundamentais e a proporcionalidade da medida, principalmente em se tratando de uma sociedade democrática.

---

5 Com exceção do tratamento de dados para fins de prevenção e investigações criminais.

Portanto, o que se verifica é que, apesar de a LGPD não prever a proporcionalidade nos casos de exceção à proibição do tratamento de dados pessoais, o exemplo europeu demonstra ser totalmente exigível que essa exceção, prevista em lei infraconstitucional, amolde-se às determinações constitucionais, não o inverso.

Se a proporcionalidade não for seguida pelo próprio Estado no tratamento de dados pessoais sensíveis, mesmo que para as finalidades atinentes à segurança pública, corre-se o risco de o titular desses dados não ter o controle das associações feitas entre as informações constantes na rede, configurando um risco para a sociedade democrática.

Ressalte-se que o tratamento de dados pessoais sensíveis pelo Estado sem alguma limitação traz risco à autodeterminação informativa, ao sigilo dos dados, à intimidade, à proporcionalidade, enfim, à dignidade humana e à democracia.

Na Alemanha, a proporcionalidade foi objeto de decisão quanto ao tratamento de dados. O Tribunal Constitucional Alemão reconheceu que a liberdade do cidadão frente ao Estado somente pode ser relativizada, de modo razoável, quando imprescindível à proteção estatal, pois uma informação isolada deixa de ser insignificante quando associada a outras. A conexão de informações pessoais assume grande poderio quando empregada de forma desenfreada e sem critérios prévios de controle, inclusive, pelo Estado.

A Constituição Federal brasileira prevê, nesse âmbito de proteção, os princípios da dignidade humana, da autodeterminação informativa, do sigilo dos dados, da intimidade e o da proporcionalidade, todos eles ligados ao direito da personalidade[6]. A dignidade humana estará presente

6 O art. 21 do Código Civil brasileiro dispõe que a vida privada da pessoa natural é inviolável. O entendimento da abrangência do que seja vida privada perpassa pelas informações e dados sobre a pessoa.

quando todos os demais forem aplicados ao tratamento e utilização de dados relativos à pessoa humana.

O inciso XII do art. 5º da Constituição Federal, por seu turno, dispõe que é inviolável o sigilo dos dados, salvo por ordem judicial, para fins de investigação criminal ou instrução processual penal.

Mesmo nos casos em que se afasta a inviolabilidade do sigilo dos dados, a possibilidade de acesso, tratamento e utilização desses sofre limitações e passa pela autodeterminação informativa.

A autodeterminação informativa assegura ao indivíduo a possibilidade de agir contra o levantamento, o tratamento e o uso irrestrito de seus dados pessoais. Desse modo, é princípio que ultrapassa a previsão da LGPD. Aliás, é anterior a ela e base da estrutura de uma sociedade democrática que respeita seu cidadão, sua intimidade e a vida privada.

Isso não significa que a inviolabilidade não possa ser relativizada no caso de investigações e processos criminais e nos demais casos previstos no art. 4º da LGPD. A relação entre esses dois aspectos deve ser pautada pela proporcionalidade, medida assecuratória do bom uso e tratamento dos dados pessoais.

A régua da proporcionalidade na relativização no tratamento dos dados pessoais sensíveis passa pela exploração adequada e coerente com o resultado pretendido, até o conhecimento pelo titular de que os seus dados estão sendo tratados pelo Estado.

Pode parecer irrelevante proporcionar ao cidadão o conhecimento prévio de que seus dados pessoais sensíveis estão em tratamento pelo Estado. No entanto, essa conduta pode determinar o nível de democracia experimentada pela sociedade.

3. *CAMBRIDGE ANALYTICA*, A ADI N. 6.387, A ADPF N. 722 E O TRATAMENTO DE DADOS PESSOAIS

A empresa americana *Cambridge Analytica* foi o centro do escândalo causado pelas publicações, em 2018, de denúncias nos jornais *The New York Times* e o *The Guardian*, que expuseram a utilização de dados pessoais sensíveis de usuários do *Facebook* com o objetivo de influenciar as eleições americanas.

O lema dessa empresa de análise de dados pode explicar o furor causado pelas revelações da imprensa: "fornecer a informação certa à pessoa certa, no momento certo é mais importante do que nunca"[7].

O caso da *Cambridge Analytica* se pautou no compartilhamento de dados pessoais sensíveis adquiridos por uma pesquisa realizada com usuários do *Facebook* e o posterior tratamento deles pela empresa, que trabalhava, à época, para o candidato republicano Donald Trump.

De acordo com documentário *The Great Hack*, da *Netflix*, os dados sensíveis compartilhados com a *Cambridge Analytica* conseguiam captar, pelo perfil apresentado na plataforma do *Facebook*, as preferências e inclinações políticas de milhões de pessoas. Dessa forma, mensagens a favor de Trump e contra a candidata adversária eram impulsionadas para os usuários de forma individualizada, levando-os a agir e decidir conforme as notícias eram recebidas em seus perfis. O caso teve repercussão mundial porque se entendeu que houve manipulação e que esta interferiu na decisão eleitoral de uma sociedade democrática.

Similar a esse caso, a ADI n. 6.387, proposta ao STF pelo Conselho

7 Frase utilizada pela empresa em uma propaganda, conforme notícia veiculada na página da globo.com: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml, 2018.

Federal da Ordem dos Advogados do Brasil, visava impugnar a Medida Provisória (MP) n. 954/2020.

A ministra Rosa Weber, relatora do caso, deferiu o pedido cautelar requerida e suspendeu a eficácia do ato normativo que determinava o compartilhamento dos dados pessoais sob posse das companhias telefônicas para o Instituto Brasileiro de Geografia e Estatística (IBGE). O instituto destacava a relevância do procedimento à continuidade de levantamento de dados pelo IBGE necessários à produção de estatística oficial durante a situação de emergência de saúde pública causada pela pandemia da covid-19.

A Advocacia-Geral da União (AGU) manifestou-se pelo indeferimento do pedido, argumentando que os requisitos necessários para a edição de uma medida provisória, relevância e urgência, estavam presentes na MP n. 954/2020, em razão da necessidade de continuidade das pesquisas realizadas pelo IBGE num momento de distanciamento social, causado pela pandemia. Quanto ao aspecto da inconstitucionalidade material, a AGU ressaltou que os dados compartilhados pelas operadoras ao IBGE continuariam em sigilo, em conformidade com o teor da decisão tomada na ADI n. 2.859.

Para deferir o pedido de medida cautelar, a ministra baseou-se tanto no postulado da autodeterminação individual quanto no da proporcionalidade. Cabe ressaltar que, apesar de citar a LGPD, ao tratar da autodeterminação informativa e do respeito à privacidade, foi o fundamento sobre a proporcionalidade da MP n. 954/2020 que teve relevância para a análise de tratamento dos dados pessoais sensíveis.

A ministra Rosa Weber, em decisão monocrática de 24 de abril de 2020, afirmou que a MP n. 954/2020 carece de adequação e necessidade a ponto de justificar o tratamento de dados pessoais. Além disso, fere substancialmente a garantia do devido processo legal e, em razão de instrução normativa, o imediato compartilhamento de dados pessoais de centena de milhões de usuários poderia acarretar dano irreparável, de forma desproporcional ao combate necessário da pandemia.

Em 7 de maio de 2020, o Plenário da Corte decidiu suspender a eficácia da medida provisória. O único voto contrário ao da relatora foi o exarado pelo ministro Marco Aurélio, que entende caber ao Congresso e não ao STF a análise do diploma.

O julgamento da ADI n. 6.387 foi uma decisão de importância ímpar para a questão do tratamento de dados pessoais no Brasil, principalmente pelo fato de ter ocorrido anteriormente à entrada em vigor da LGPD. Além disso, tornou-se paradigmática ao reconhecer que a Constituição Federal de 1988 assegura aos brasileiros o direito à autodeterminação informativa, conforme destaca a ministra:

> Decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais.

Para confirmar a importância desse julgamento, o STF foi instado a decidir sobre um suposto dossiê criado pelo Ministério da Justiça, sob o argumento de prevenção de danos à segurança nacional. Nesta ação, ADPF n. 722, os preceitos fundamentais tidos como violados foram, entre outros, a liberdade de expressão e o direito à intimidade e à vida privada. Apesar da importância da análise da liberdade de expressão, o direito à intimidade e à vida privada tem importância maior ante a análise do tratamento de dados pessoais sensíveis.

De acordo com notícias veiculadas à época, esse suposto dossiê tinha como base dados pessoais sensíveis[8], especificamente, dados pessoais

8 Aqui cabe destacar que a LGPD, no art. 4º, III, exclui de seu âmbito de proteção no tratamento de dados pessoais, os dados pessoais sensíveis quando necessários para a segurança pública e segurança do Estado.

relativos à opção política de indivíduos críticos do atual governo federal, então denominados de antifascistas.

Nessa ADPF, provocada pelo partido Rede Sustentabilidade, analisa-se um relatório produzido pelo Ministério da Justiça, por meio da Secretaria de Operações Integradas (Seopi), órgão pertencente ao Ministério da Justiça. A partir das assinaturas de um manifesto, que pedia reação contra ameaças de ruptura institucional, a Seopi ampliou a investigação e listou, divididos por Estados, o total de 579 nomes. Essas pessoas foram monitoradas pelo Estado, e seus dados pessoais, considerados sensíveis, foram tratados e compartilhados entre órgãos da administração pública, tais como Polícia Rodoviária Federal, Casa Civil da Presidência da República, Abin (Agência Brasileira de Inteligência), Força Nacional e três centros de inteligência vinculados à Seopi.

Segundo o Ministério da Justiça, a elaboração desse dossiê seria justificada pela necessidade de prevenir, neutralizar e reprimir atos criminosos que atentassem contra a ordem pública e a segurança nacional[9], o que coaduna com as hipóteses de exceção de proibição de tratamento de dados pessoais previstas no art. 4º, III, da LGPD.

Em 20 de agosto de 2020, a medida cautelar foi deferida, por maioria, sendo estabelecida a suspensão de

---

9 A ADPF n. 722, do partido Rede Sustentabilidade, traz transcrições de trechos dos relatórios da Seopi que demonstram o acesso e tratamento a dados pessoais sensíveis sem a imputação, ao menos em tese, de ilícito penal praticado: "verificamos alguns policiais formadores de opinião que apresentam número elevado de seguidores em suas redes sociais, os quais disseminam símbolos e ideologias antifascistas" e "além desses servidores foi possível identificar alguns formadores de opinião, professores, juristas e o atual secretário de estado de articulação da cidadania do Pará [*sic*], defensores desse movimento". Disponível em: http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5967354, p. 4-5. Acesso em: 12 out. 2020.

> todo e qualquer ato do Ministério da Justiça e Segurança Pública de produção ou compartilhamento de informações sobre a vida pessoal, as escolhas pessoais e políticas, as práticas cívicas de cidadãos, servidores públicos federais, estaduais e municipais identificados como integrantes de movimento político antifascista, professores universitários e quaisquer outros que, atuando nos limites da legalidade, exerçam seus direitos de livremente expressar-se, reunir-se e associar-se.[10] (ADPF n. 722 MC)

De acordo com o voto da relatora, ministra Cármen Lúcia, o serviço de inteligência estatal é necessário para a segurança pública e para a segurança nacional, mas deve agir pautado nos limites constitucionais e legais, pois direitos fundamentais não são objeto de concessão estatal.

No que se refere ao direito à intimidade e à vida privada e a relação existente entre o tratamento de dados pessoais sensíveis, o ministro Gilmar Mendes pontuou, em seu voto,[11] que o serviço de inteligência estatal é importante para o Estado, mas, de acordo com o já decidido na ADI n. 6.259, a atividade de inteligência estatal não está imune à necessidade de motivação. Asseverou, ainda, ser um risco a admissão de uma devassa na vida privada das pessoas, mesmo em procedimentos formais da inteligência estatal.

Diante disso, fica claro que, mesmo para a inteligência estatal, há limites constitucionais que devem ser observados no tratamento de dados pessoais, sobretudo quanto aos aqueles sensíveis.

---

10 A decisão, por maioria, teve como voto dissidente o do ministro Marco Aurélio, que entendeu ser a via escolhida, a ADPF, inadequada. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5967354. Acesso em: 11 out. 2020.

11 Disponível em: https://www.conjur.com.br/dl/voto-gilmar-dossie-mj-antifascistas.pdf.

4. DADOS PESSOAIS SENSÍVEIS E OS DECRETOS N. 9.662/2019 E N. 10.046/2019

Antes da edição da LGPD, já havia normativas sobre o tratamento de dados pessoais sensíveis pelo Estado.

Vale lembrar que o diploma, no inciso III do art. 4º, exclui do seu âmbito de proteção o tratamento de dados pessoais, inclusive os sensíveis, quando esses forem necessários para o fim exclusivo da segurança pública, defesa nacional, segurança do Estado ou para as atividades de investigação e repressão de infrações penais.

O Decreto n. 9.662, de janeiro de 2019,[12] dispõe sobre as atribuições da Seopi, a responsável pela elaboração do suposto dossiê antifascista. Dentre as atribuições de inteligência da secretaria, destaca-se o assessoramento do ministro da Justiça nas atividades de inteligência, a integração com sistemas de inteligência e segurança pública, o estímulo de investigações de infrações penais de maneira integrada com as polícias federal e civil. Não há, nesse decreto, limite na obtenção e no tratamento de dados obtidos pela Seopi, nem mesmo a determinação de controle judicial em suas atuações.

Por sua vez, o Decreto n. 10.046/2019 dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o comitê central de governança de dados.

Ao estabelecer as normas e diretrizes para o compartilhamento de dados entre órgãos da administração pública federal, o decreto prevê como finalidades a simplificação da oferta de serviços públicos, a orientação e otimização das políticas públicas, a análise das condições de acesso e manutenção de benefícios sociais e fiscais, a promoção da melhoria da qualidade dos dados custodiados pela administração e, por último, de maior importância no que se refere aos dados pessoais sensíveis, o aumento da qualidade e eficiência de suas operações internas.

12 Arts. 29 e 31, IV.

Nesse último item, podem ser incluídas as operações que visam à manutenção da ordem pública e prevenção de danos à segurança nacional. Importante destacar que o art. 3º, ao tratar sobre o regramento no compartilhamento de dados, especifica no inciso VI que a coleta, o tratamento e o compartilhamento de dados serão realizados de acordo com o disposto no art. 23 da LGPD.

Ocorre que dados pessoais podem ser tratados pelo Estado quando tiver alguma das finalidades disposta no inciso III do art. 4º da LGPD. Portanto, o regramento do art. 23 da LGPD não se aplica nas hipóteses do art. 4º da lei.

No tocante à limitação na captação e no tratamento de dados pessoais pelo Estado nas hipóteses do inciso III do art. 4º da LGPD[13], a situação se agrava quando se verifica que o art. 4º do Decreto n. 10.046/2019 categoriza o compartilhamento de dados de acordo com sua confidencialidade. São três as categorias: (i) compartilhamento amplo, quando os dados públicos não estão sujeitos a nenhuma restrição; (ii) compartilhamento restrito, quando os dados são protegidos por sigilo nos termos legais com concessão de acesso a órgãos e entidades responsáveis na execução de políticas públicas; e (iii) compartilhamento específico, quando os dados são protegidos por sigilo nos termos legais. Nesse terceiro nível, a concessão de acesso a órgãos e entidades específicos ocorrerá nas hipóteses e para os fins previstos em lei, em que as regras de compartilhamento sejam definidas pelo gestor dos dados.

O problema observado no Decreto n. 10.046/2019 deve-se à redação do inciso III, que dispõe sobre o compartilhamento específico. Da forma como redigido, permite interpretação ampla e, por conse-

13 "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: (...) III – realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais;"

guinte, aplicação por demais abrangente nos processos de captação, tratamento e compartilhamento de dados, principalmente pelo fato de que os órgãos e entidades com acesso ao compartilhamento podem ser definidos *a posteriori*, ou, ainda, nos casos em que a finalidade seja, genericamente, colocada, como a manutenção da segurança pública e da segurança nacional. Tal situação revela claro desrespeito aos princípios da dignidade humana, da autodeterminação informativa, do sigilo dos dados, da intimidade e da proporcionalidade.

5. CONCLUSÃO

Paradoxalmente, em tempos de dataísmo,[14] deve-se tomar cuidado para que a importância dos dados não suplante a normatividade constitucional. De nada adianta a regulamentação no tratamento de dados se se relevam os direitos e princípios constitucionais atinentes à pessoa humana. Afinal, a proteção no tratamento dos dados tem por objetivo maior proporcionar segurança jurídica e proteger a dignidade humana em seus direitos mais básicos, o da personalidade.

Os direitos e garantias fundamentais, especificamente intimidade, vida privada e sigilo de dados, não são absolutos. Assim, não é objeto de proteção e pode ser tratado pelo Estado os dados cuja finalidade seja a garantia da segurança pública, segurança nacional e a necessidade para a investigações e processos criminais.

Apesar de os princípios previstos na LGPD não se aplicarem aos casos acima, por força do disposto no inciso III do art. 4º, o Estado não pode agir, de forma ilimitada, no tratamento de dados pessoais e no de dados pessoais sensíveis, por mais que a justificativa seja importante para a sociedade.

---

14 Uma ideologia baseada no *Big Data*.

Pode-se afirmar que, da mesma forma que os princípios da LGPD são aplicados ao tratamento de dados autorizados por ela, os princípios constitucionais da dignidade humana, da proporcionalidade, da autodeterminação informativa e os direitos da intimidade e da vida privada devem ser aplicados no tratamento e custódia de dados pessoais excluídos pela LGPD.

As decisões formalizadas na ADI n. 6.387 e na ADPF n. 722 demonstram que o STF entende que o tratamento de dados pessoais por parte do Estado, mesmo nas hipóteses excluídas pela LGPD, submete-se aos princípios constitucionais já explicitados pela própria estrutura do estado democrático de direito que experimenta o Brasil desde a promulgação da Constituição Federal de 1988.

Nesse sentido, legislações anteriores e posteriores à LGPD que vinculem a captação, o tratamento e o compartilhamento de dados pelo Estado ao gestor de dados, sem levar em consideração, principalmente, os princípios da proporcionalidade e da autodeterminação informativa, devem ser interpretados na conformidade constitucional, sob pena de servirem como dados de Troia para a democracia.

REFERÊNCIAS

BRASIL. *Decreto n. 9.662/2019*. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Justiça e Segurança Pública, remaneja cargos em comissão e funções de confiança e transforma cargos em comissão do Grupo-Direção e Assessoramento Superiores – DAS. Disponível em: http://planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9662.htm. Acesso em: 2 out. 2020.

BRASIL. *Decreto n. 10.046/2019*. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e

institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 2 out. 2020.

BRASIL. *Lei Geral de Proteção de Dados*. Dispõe sobre a Lei de Proteção de Dados e altera a Lei 12.965, de 24 de abril de 2014 (Marco Civil da Internet). Lei Geral de Proteção de Dados (LGPD). Redação dada pela Lei 13.853, de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 7 out. 2020.

BRASIL. *Lei n. 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 8 out. 2020.

BRASIL. Supremo Tribunal Federal. *ADPF n. 722/DF*. Disponível em: http://redir.stf.jus.br/estfvisualizadorpub/jsp/consultarprocessoeletronico/ConsultarProcessoEletronico.jsf?seqobjetoincidente=5967354. Acesso em: 12 out. 2020.

BRASIL. Supremo Tribunal Federal. ADPF n. 722/DF. *Voto do ministro Gilmar Mendes na ADPF n. 722*. Disponível em: https://www.conjur.com.br/dl/voto-gilmar-dossie-mj-antifascistas.pdf. Acesso em: 11 out. 2020.

BRASIL. Supremo Tribunal Federal. *Decisão monocrática de deferimento da medida cautelar na ADI n. 6.387/DF*. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf, 2020. Acesso em: 2 out. 2020.

GLOBO. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml, 2018. Acesso em: 30 set. 2020.

HARARI, Yuval Noah. *21 lições para o século 21*. Tradução de Paulo Geiger. 1. ed. São Paulo: Companhia das Letras, 2018.

PESTANA, Márcio. *Os princípios no tratamento de dados na Lei Geral de Proteção de Dados Pessoais*. Disponível em: https://www.conjur.com.br/2020-mai-25/marcio-pestana-principios-tratamento-dados-lgpd, 2020. Acesso em: 8 out. 2020.

SANTOS, Maike Wile dos. *O Big Data somos nós*: a humanidade de nossos dados. Jota, 16 mar. 2017. Disponível em: https://jota.info/colunas/agenda-da-privacidade-e-da-protecao-de-dados/o-big-data-somos-nos-a-humanidade-de-nossos-dados-16032017, 2017. Acesso em: 30 set. 2020.

SCHWABE, Jürgen. *Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão*. KonradAdenauer-Stiftung, 2005.

SERPRO. Serviço Brasileiro de Processamento de Dados. Disponível em: https://www.serpro.gov.br/lgpd/menu/arquivos/infografico-lgpd-em-um-giro, 2020, *on-line*. Acesso em: 20 set. 2020.

UNIÃO EUROPEIA. *Regulamento geral sobre a proteção de dados*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1559280280904&uri=CELEX:32016R0679#d1e40-1-1. Acesso em: 1º out. 2020.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: QUESTÕES PENAIS

George Neves Lodder[1]

RESUMO

Na abordagem de investigações criminais, a autoridade nacional de proteção de dados pode ser, não obrigatoriamente, a prevista pela Lei Geral de Proteção de Dados. No que concerne às questões penais, ela atuará, em um primeiro enfoque, como entidade responsável pela consolidação e notificação dos órgãos de persecução penal acerca das infrações a normas que lhe pareçam penalmente típicas. A ação desses órgãos, nesse contexto, completa o sistema de *compliance* preconizado pela Lei n. 13.709/2018. Noutro feixe, sem inviabilizar a eficiência da execução, deve controlar a conformidade digital das investigações penais e demais atividades do Ministério Público e da polícia judiciária que envolvam dados pessoais (ressalvada a atividade estritamente processual).

---

1 Procurador da República no Estado do Tocantins. Coordenador criminal do Ministério Público Federal no Estado do Tocantins. Ex-coordenador criminal do Ministério Público no Estado do Amapá. Bacharel em Direito pela Universidade de Brasília. Integrante do grupo de trabalho do CNMP destinado à elaboração de estudos e propostas voltadas à política de acesso às bases do Ministério Público brasileiro.

Palavras-chave: Autoridade nacional de proteção de dados. Lei Geral de Proteção de Dados. Diretiva n. 2016/680 do Conselho da União Europeia. *Compliance* digital. Apoio às investigações criminais. Determinação legal da autoridade de controle nas investigações criminais. Princípios da legalidade e proporcionalidade. Importância e viabilidade da persecução penal.

ABSTRACT

The Brazilian Data Protection Authority, when criminal issues are concerned, functions primarily as the entity responsible for receiving information about data processing misconducts and notifying law enforcement when it identifies these misconducts as criminal behavior. Prosecuting and punishing those crimes is part of the compliance system created to prevent illegal data sharing. On the other hand, the authority is mandated to supervise the adequacy of criminal investigations, as well as other investigative activities performed by prosecutors and police agents, without hindering the procedures.

Keywords: Brazilian data protection authority. General Data Protection Law. Directive n. 2016/680 of the European Parliament. Compliance. Support to criminal investigations. Legal mandate of the data protection authority in criminal matters. Due process. Relevance of prosecutorial activities.

1. INTRODUÇÃO

Criada pelos arts. 55-A e seguintes da Lei de Proteção de Dados Pessoais (com a redação dada pela Lei n. 13.853/2019), a Autoridade Nacional de Proteção de Dados (ANPD) foi incumbida, em linhas

gerais, de zelar pela estrutura de proteção de dados pessoais instituída pela norma.

Nas palavras de Teffé (2020):

> O cenário de assimetria informacional que nos rodeia exige que sejam estabelecidos órgãos que visem a promover maior equilíbrio na relação entre os titulares dos dados e os agentes, bem como que fomentem uma cultura mais informada e centrada na proteção de dados e na segurança da informação.

Com efeito, a grande maioria da população brasileira sequer sabe que seus dados são tratados por pessoas e sociedades com quem negociam e quase a totalidade não sabe de que forma isso se aperfeiçoa, tampouco qual o resultado dessas operações ou a consequência desse fenômeno em suas vidas. As violações aos dados pessoais recolhidos por empresas e aplicações, imputáveis a elas ou não, passam ao largo do cotidiano de seus titulares, sem que eles consigam sequer perceber a relação entre esses eventos e suas repercussões.

Outrossim, diferentemente do que ocorre na Europa – onde o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) foi elaborado a partir da consolidação das boas práticas edificadas naquele continente, ao longo dos anos –, no Brasil partiremos de uma cultura que desconhece, quiçá repele, a proteção de dados pessoais, a dificultar ainda mais a complexa missão de que se incumbe a ANPD.

Sob a perspectiva das relações entre a autoridade nacional e os órgãos de persecução criminal, antecipam-se maiores tensões, ante a natureza e o objetivo dos dados manipulados, assim como a confidencialidade do conteúdo de parcela das investigações que poderá redundar descompasso entre os requerimentos do órgão regulador e a compreensão daquilo que se sujeita efetivamente à sindicância. A vinculação

direta de sua estrutura à Presidência da República[2] pode acentuar essa mútua desconfiança, notadamente acerca de dados e/ou apurações que envolvam agentes ou interesses do Poder Executivo.

Afigura-se fundamental que tais arestas sejam aparadas, pois assaz importantes as funções da ANPD concernentes à regulação de dados destinados aos órgãos de *law enforcement* e por eles tratados, bem como a promoção de ações conjuntas para atingir objetivos comuns.

Para abordar essa temática, serão examinadas as funções da ANPD como agente promotor de *compliance* – com foco na importância do arcabouço de responsabilização penal para a eficácia do sistema – e como garante do adequado uso dos dados pessoais no transcurso das investigações, assim como, em outros contextos, pelos órgãos delas incumbido.

---

2 A ANPD, hoje, faz parte da estrutura da Presidência da República, embora o § 1º do art. 55-A da LGPD autorize sua conversão em entidade da administração pública federal indireta, submetida a regime autárquico especial. Ante a inconveniência dessa alocação, Pfeiffer (2019) alertou a respeito da medida provisória que resultou no texto atual, *in verbis*: "Com efeito, o órgão previsto no texto vetado possuía a natureza de autarquia especial, vinculada ao Ministério da Justiça, sendo caracterizada pela independência administrativa, ausência de subordinação hierárquica, mandato fixo e estabilidade de seus dirigentes e autonomia financeira. Por seu turno, a Medida Provisória 869/2018 confere à ANPD a natureza de órgão da administração direta federal, subordinada à Presidência da República. Assim, a distinção de natureza é impactante: enquanto a autarquia especial possui autonomia administrativa, financeira e hierárquica, o órgão da administração direta é destituído de tais características, tendo em vista a sua subordinação hierárquica direta ao presidente da República. Esta estrutura enfraquecida traz diversas consequências negativas. Por exemplo, coloca em xeque a sua autonomia decisória, já que o artigo 56 da Lei 9.784/1999 estabelece o direito de recurso contra todas as decisões administrativas no âmbito federal, trazendo o risco das decisões da ANPD estarem sujeitas a revisão por meio de recurso administrativo hierárquico endereçado ao presidente da República."

2. AUTORIDADE DE PROTEÇÃO DE DADOS, *COMPLIANCE* E APOIO À INVESTIGAÇÃO CRIMINAL

Basta a simples leitura do art. 55-J da Lei n. 13.709/2018 para perceber que as atribuições da ANPD não se resumem à regulação, à fiscalização e ao sancionamento de controladores e operadores de dados pessoais.

Extraem-se do plexo de competências medidas concernentes à construção de um código de ética de tratamento de dados pessoais, uma política de boa governança nessa atividade, bem como o estabelecimento de canais de comunicação com os titulares desses dados, órgãos e entidades públicas cujas competências estejam entrelaçadas com suas funções e com o público externo em geral.

Na elaboração da Política Nacional de Proteção de Dados Pessoais, a ANPD delimitará as balizas dentro das quais deverão movimentar-se os controladores para produzirem seus próprios regulamentos internos de segurança dos dados[3]. Em momento posterior, editará regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção desses dados. Realizará, ainda, auditorias sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público, e celebrará compro-

3 "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular."

misso com esses agentes para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos.

Nota-se, pois, que a LGPD pretende que a autoridade induza e estimule a implementação de programas de *compliance*[4] no âmbito das empresas e entidades que performam o tratamento de dados pessoais, a fim de que os próprios gestores e empregados se ocupem de cumprir e averiguar o atendimento dos regulamentos, tanto internos quanto externos – legais e infralegais –, com o intuito de evitar o cometimento de infrações, inclusive penais.

Ao adotar um programa de integridade empresarial, calcado na boa-fé e nos demais princípios do art. 6º da LGPD, o agente controlador previne a ocorrência de eventos danosos à sua imagem, reduz o risco da incidência de sanções administrativas – que podem chegar ao patamar de cinquenta milhões de reais – e se beneficia do acesso a mercados internacionais que condicionam certos negócios jurídicos à adequação

4 Constitui pedra angular de programa de *compliance* o *Data Protection Officer* (DPO) ou encarregado (art. 41 da LGPD). Entre as funções desse profissional (ou escritório), incluem-se atividades impregnadas de nítida natureza de conformação das ações da entidade à legislação a que deverá estar adstrita, tais como as elencadas pelo art. 39 do GDPR: "a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-membros; b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes; c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do art. 35; d) Coopera com a autoridade de controlo (...)."

dos estatutos da empresa a padrões de segurança digital. Nesse sentido, impende acrescentar que

> uma empresa pode optar por não adotar um programa de *compliance*. Porém, caso isso ocorra, mas a lei (*hard law*) ou o setor econômico onde ela atue (*soft law*) exija a adoção de um programa de *compliance*, como ocorre em casos onde há o risco de branqueamento de capitais, corrupção de funcionários públicos, poluição ambiental, acidentes de trabalho, fabricação ou distribuição de produto defeituoso, etc., a atribuição de responsabilidade, a título de autoria, ao dirigente que se omitiu do controle ficaria mais evidenciada. Nesse sentido, há uma sintonia entre a situação de *non-compliance* e a imputação de autoria pela posição de garantidor, fundamentando-se uma omissão punível dos dirigentes. (SOUZA, 2016, p. 999)

Entre as responsabilidades subjacentes à assunção de um programa de *compliance* digital está o dever de perquirir[5], fazer cessar, remediar[6] e comunicar irregularidades aos órgãos com atribuição para tomar as medidas subsequentes. A esse respeito, não deixa espaço para dúvidas o art. 48 da LGPD, *in verbis*: "Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares."

---

5 Assume especialmente percuciente o uso de canais de representação abertos ao público, titulares de dados ou não, e que lhes assegure confidencialidade e agilidade na apuração dos fatos e a execução das medidas correspondentes.

6 Remediar possíveis danos causados por condutas ilícitas é uma preocupação que deve fazer parte do programa de *compliance*. Para além de demonstrar seriedade e comprometimento, a remediação pode auxiliar a empresa até mesmo em termos financeiros se violações vieram a ocorrer. Remediação não deve ser confundida com punição. Uma empresa pode ser punida e multada por uma conduta, mas isso não a isentará de remediar os danos causados (UBALDO, 2017, p. 125).

De posse desses informes, a ANPD deverá avaliar as repercussões das ações narradas, promovendo, quando procederem dolosa ou culposamente, a responsabilização dos controladores, operadores e encarregados do tratamento de dados pessoais (art. 52 e seguintes da Lei n. 13.709/2018).

Todavia, algumas condutas reclamam responsabilidade para além das esferas civil e administrativa, sobretudo quando se detecta a participação de agente invasor, estranho ao círculo de legitimados ao tratamento dos dados captados/modificados/destruídos. Nesse cenário, afigura-se indispensável para o êxito desse sistema de proteção e conformidade que a ANPD relate as infrações em tese penalmente típicas ao Ministério Público ou às polícias judiciárias, não só por imperativo lógico do sistema mas também por expresso comando do inciso XXI do art. 55-J da LGPD[7 e 8].

Essa atividade não está impregnada de conteúdo investigativo. Ao revés, a autoridade apenas coopera com os órgãos responsáveis pela investigação criminal, ante a percepção de ato suspeito. Converte-se, outrossim, em uma espécie de ponte entre as entidades responsáveis pelo tratamento de dados pessoais – as quais estão obrigadas a lhe

---

7 "Art. 55-J. (...) XXI – comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;"

8 Em fala sobre o Coaf, que pode ser aqui aplicada analogicamente, explica Vladimir Aras: "Art. 15. O Coaf comunicará às autoridades competentes para a instauração dos procedimentos cabíveis, quando concluir pela existência de crimes previstos nesta Lei, de fundados indícios de sua prática, ou de qualquer outro ilícito. A UIF não tem opção, segundo a lei brasileira. Não se usa um 'poderá'. O verbo é outro. Uma vez identificados sintomas de uma possível 'infecção' no sistema financeiro, o Coaf deve alertar o sistema de defesa (os órgãos de persecução e congêneres do *law enforcement*), para que aqueles sinais sejam examinados em busca de uma enfermidade, que, nessa alegoria, corresponde ao crime de lavagem de dinheiro e às condutas antecedentes." (ARAS, 2019)

comunicar os incidentes de segurança – e o *law enforcement*, sempre quando proeminentes sinais indicativos da prática de um delito.

Não há nesse agir qualquer violação de sigilo, senão o reforço das garantias individuais do titular do dado – ainda naquelas hipóteses que se cogite de seu vazamento ou mau uso. A ação estatal punitiva, efetiva e expedita, é, precisamente, o instrumento capaz de proteger a inviolabilidade dessas informações[9].

A ANPD não deve, contudo, alertar os envolvidos na conduta ilícita – ressalvados os casos em que estes se confundam com os responsáveis pela comunicação de que cuida o art. 48 acima citado – de que suas ações prejudiciais a terceiros e seus dados são objeto de investigação criminal. Trata-se de mecanismo essencial ao *compliance* digital (BLAGITZ; LODDER, 2020).

Cumpre acrescentar que, diferentemente do que fizeram normas congêneres em outros países, a LGPD não inovou a legislação penal. Entretanto, com a provável ratificação da Convenção de Budapeste sobre cibercrime, será imprescindível a criação de tipos penais concernentes ao acesso ilegítimo de sistemas e dados informáticos; à interceptação ilegítima desses dados; sabotagem informática; interferência em sistemas; falsidade e burla informática; entre outros delitos[10].

---

9 Assim como também devem se reportar ao Ministério Público, diante de potenciais crimes: Coaf, CVM, Anatel, Aneel, ANP, Ibama, ICMBio, DNPM, Receita Federal do Brasil, Banco Central do Brasil, TC, INPI, Iphan, Funai, Funasa, entre outros órgão e entidades federais.

10 O capítulo ao qual refere-se o direito penal substantivo – arts. 2º ao 13 – define nove crimes agrupados em quatro categorias distintas, seguidos pela responsabilidade acessória e respectivas sanções. De acordo com o Tratado de Budapeste, são considerados crimes cibernéticos, sendo que cada parte deverá adotar as medidas legislativas e outras que se revelem necessárias para classificação da infração penal. (ALEXANDRE JR., 2019)

Posto que assim não fosse, vigoram hodiernamente tipos penais relacionados à matéria, tais como os arts. 154-A[11] e 266[12] do Código Penal e o art. 10 da Lei. 9.296/1998[13], de cuja possível configuração devem ser notificados os órgãos atribuídos dessa avaliação.

3. TRATAMENTO DE DADOS PESSOAIS PELOS ÓRGÃOS DE PERSECUÇÃO PENAL, FORA DAS INVESTIGAÇÕES PENAIS

Os órgãos de persecução penal não coletam e tratam dados pessoais apenas no âmbito de investigações criminais. Também o fazem em relação a seus servidores, fornecedores, visitantes e de quem demanda seus serviços, entre outros. Em tal moldura, estarão sujeitos ao controle da ANPD, assim como qualquer outra pessoa jurídica de direito público (e seus órgãos), a teor do art. 23 da Lei n. 13.709/2018.

Nessa função, estarão autorizados a tratar dados, inclusive os sensíveis (art. 11, II, da LGPD), tendo em vista a execução de políticas públicas e a prestação de serviços públicos. Entretanto, estarão jungidos aos princípios

---

11 "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa."

12 "Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena – detenção, de um a três anos, e multa. § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento."

13 "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei: Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa."

e às diretrizes da norma, notadamente no que tangencia à eliminação de dados desnecessários e aos cuidados na transferência dos bancos de dados[14].

Cabe à ANPD, portanto, além de aferir se a análise é norteada pelo interesse público, assim como se atende às finalidades do tratamento, propor o estabelecimento de mecanismos e a adaptação da regulamentação interna, para promover maior segurança aos dados e assegurar aos titulares as prerrogativas conferidas pelo estatuto.

Assinale-se, de outra banda, que o Conselho da União Europeia recomenda aos Estados-membros que excluam do escopo das autoridades de controle os tratamentos de dados pessoais efetuados pelo Ministério Público, no bojo de sua atividade processual, como mecanismo para privilegiar a autonomia e independência de seus pronunciamentos[15]. Esse o rumo seguido pela legislação portuguesa[16]. Sem dúvida, contempla-se

---

14 Merece especial cuidado os programas de acesso massificado de dados, que vêm sendo incentivados, sobretudo no âmbito do Poder Judiciário, para custear os sistemas de governança que se pretende instalar nos tribunais e que tendem a ser replicados por outros órgãos de estrutura semelhante.

15 "Embora a presente diretiva se aplique também às atividades dos tribunais nacionais e outras autoridades judiciais, a competência das autoridades de controlo não deverá abranger o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência dos juízes no desempenho das suas funções jurisdicionais. Esta exceção deverá ser estritamente limitada às atividades judiciais relativas a processos judiciais, não se aplicando a outras atividades a que os juízes possam estar associados por força do direito do Estado-membro. Os Estados-membros podem também prever a possibilidade de a competência das autoridades de controlo não abranger o tratamento de dados pessoais efetuado por outras autoridades judiciais independentes no exercício da sua função jurisdicional, nomeadamente o Ministério Público. Em todo o caso, o cumprimento das regras da presente diretiva pelos tribunais e outras autoridades judiciais independentes deverá ficar sempre sujeito a uma fiscalização independente nos termos do art. 8º, n. 3, da Carta." (UNIÃO EUROPEIA, 2016)

16 Art. 43 da Lei portuguesa n. 59/2019: "Autoridade de controlo: 1 – Incumbe à CNPD

missão em que o *parquet* não pode ter seu raio de ação restringido pelos riscos de responsabilização pela aplicação de dados cruciais para o resultado da demanda.

4. INVESTIGAÇÃO CRIMINAL E AUTORIDADE(S) DE PROTEÇÃO DE DADOS

Como cediço, o art. 4º da LGPD[17] optou por não disciplinar o tratamento de dados feito com o exclusivo propósito de investigar e reprimir investigações penais.

Isso não significa que o Estado atuará sem regulamentação nessa atividade – ou pelo menos sem outra espécie de controle que não a própria submissão dessas investigações ao Poder Judiciário. Tanto que notória a criação de uma comissão de juristas vinculada à Câmara dos Deputados para engendrar uma nova norma a respeito do tema.

Uma das questões que deverá ser enfrentada pela mencionada comissão consubstancia-se na determinação da autoridade que deverá implementar o controle do tratamento dos dados no âmbito das investigações estatais.

A esse respeito, sublinhe-se que o Parlamento Europeu e o Conselho da União Europeia (UE), por meio da Diretiva (UE) n. 2016/680 – relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de

---

a garantia e fiscalização do cumprimento da presente lei; 2 – O disposto do número anterior não se aplica ao tratamento de dados pessoais efetuado pelos tribunais e pelo Ministério Público no exercício das suas competências processuais. (...)"

17 "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: (...) III – realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais."

sanções penais, e à livre circulação desses dados – admitem que essa função seja acometida tanto à mesma autoridade criada para o escopo do Regulamento (UE) n. 2016/679 (*General Data Protection Regulation* – GDPR) como a outra que reflita a estrutura constitucional, organizativa e administrativa, consoante dispõe o art. 41, abaixo transcrito:

> Artigo 41.
> Autoridade de controlo
> 1. Cada Estado-membro prevê que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação da presente diretiva, a fim de proteger os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e de facilitar a livre circulação desses dados na União ("autoridade de controlo").
> (...)
> 3. Os Estados-membros podem prever que uma autoridade de controlo criada pelo Regulamento (UE) 2016/679 seja a autoridade de controlo a que se refere a presente diretiva e assuma as funções de autoridade de controlo a definir nos termos do n. 1 do presente artigo.
> 4. Se for criada mais do que uma autoridade de controlo num Estado-membro, o Estado-membro em questão designa a autoridade de controlo que representa as demais no Comité a que se refere o artigo 51.

Com base nessas diretrizes, à guisa de exemplo, a Assembleia da República Portuguesa promulgou a Lei n. 59, de 8 de agosto de 2019, que, em seu art. 43, preceituou:

> Artigo 43.
> Autoridade de controlo
> 1 – Incumbe à CNPD a garantia e fiscalização do cumprimento da presente lei.
> (...)

> 3 – Para efeitos do n. 1, a CNPD integra um magistrado judicial, designado pelo Conselho Superior da Magistratura, e um magistrado do Ministério Público, designado pelo Conselho Superior do Ministério Público.
>
> 4 – Cabe exclusivamente aos magistrados a que se refere o número anterior, sem prejuízo das competências do presidente da CNPD, o exercício das atribuições da CNPD que impliquem o acesso a dados objeto de tratamento ou aos registos cronológicos das operações de tratamento.

Extrai-se do texto legal que, embora haja confiado à Comissão Nacional de Proteção de Dados[18] a tarefa de garantir e fiscalizar o tratamento de dados no ambiente das investigações criminais, o legislador português designou membros do Poder Judiciário e do Ministério Público para atuarem, nesse mister, sempre que premente o revolvimento de dados investigatórios ou o reexame das operações de tratamento.

É digna de encômios a referida disposição, pois preserva a autonomia e a independência de ambos os órgãos, que poderia ser cerceada pela atuação de autoridade vinculada a outro Poder – mormente no caso brasileiro, em que esta integra a Presidência da República – interessada nos rumos ou no conteúdo de uma apuração. Ao mesmo tempo, não mitiga o direito inerente aos titulares dos dados, que merecem, também, a proteção estatal.

Decerto, solução semelhante poderia ser perfilhada por nosso ordenamento. No entanto, uma alternativa, talvez mais proveitosa, seria delegar a missão ao Conselho Nacional de Justiça (CNJ) e ao Conselho Nacional do Ministério Público (CNMP)[19], que cumprem os requisitos

---

18 Equivalente portuguesa à ANPD.

19 Ressalte-se que esse modelo de conselho não existe na estrutura judicial europeia, de maneira que é inadequada eventual afirmação de que aquele sistema haveria rechaçado a hipótese.

de integrarem a estrutura do Poder Judiciário[20] e do Ministério Público e a expertise de promover o controle externo – ainda que, neste caso, se conjugue parcial intervenção na atividade-fim, mas sem que se aceite imiscuição no mérito das decisões tomadas na inquirição.

Além disso, poder-se-ia encarregar o Ministério Público de promover a avaliação do tratamento de dados pessoais no curso das investigações policiais, como manifestação do controle externo instituído pelo art. 129, VII, da Constituição. Desse modo, seria salvaguardado o conteúdo da investigação de agentes externos, sem o embotamento dos desígnios legais, frente à fiscalização de cunho administrativo, mas não disciplinar, performada pelo *parquet.* A propósito, afirma Emerson Garcia:

> Os organismos policiais, quer sob o prisma de sua atividade de polícia administrativa, quer sob a ótica da atividade de polícia judiciária, não estão sujeitos ao poder disciplinar dos membros do Ministério Público. Estão, sim, sujeitos à efetiva fiscalização deste, o que é mero consectário dos múltiplos mecanismos de equilíbrio existentes em um Estado de Direito. Exercendo os órgãos policiais uma função administrativa e nitidamente auxiliar ao Ministério Público, cabe a este exercer uma função correicional extraordinária, coexistindo com a atividade correicional

20 Assim se pronunciou o Supremo Tribunal Federal, no julgamento da ADI n. 3.367, rel. min. Cezar Peluso. Pertinente a citação de trecho do *Informativo* n. 383, que remete ao referido acórdão: "Com base nisso, esclareceu-se que o CNJ é órgão próprio do Poder Judiciário (CF, art. 92, I-A), composto, na maioria, por membros desse mesmo Poder (CF, art. 103-B), nomeados sem interferência direta dos outros Poderes, dos quais o Legislativo apenas indica, fora de seus quadros e, assim, sem vestígios de representação orgânica, dois dos quinze membros, não podendo essa indicação se equiparar a nenhuma forma de intromissão incompatível com a ideia política e o perfil constitucional da separação e independência dos Poderes." (BRASIL, 2005)

> ordinária, inerente à hierarquia administrativa e que é desempenhada pela própria administração. (GARCIA, 2008, p. 241)

Em qualquer hipótese, é imprescindível que a autoridade responsável seja escolhida por procedimentos predeterminados e cristalinos, bem como que os agentes escolhidos possam desempenhar seus deveres em um ambiente livre de pressões injustificadas e pautados apenas pelo interesse público, como bem delineado pelo considerando 79 da Diretiva (UE) n. 2016/680:

> As condições gerais aplicáveis aos membros da autoridade de controlo deverão ser definidas pelo direito do Estado-membro e deverão prever, em especial, que os referidos membros sejam nomeados por procedimento transparente pelo Parlamento, pelo Governo nacional ou pelo Chefe de Estado do Estado-membro, com base numa proposta do governo ou de um dos seus membros ou do parlamento ou da sua câmara competente, ou por um organismo independente incumbido da nomeação nos termos do direito do Estado-membro. A fim de assegurar a independência da autoridade de controlo, os membros que a integram deverão atuar com integridade, abster-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não deverão exercer nenhuma ocupação, seja ou não remunerada, que com elas seja incompatível. A fim de assegurar a independência da autoridade de controlo, o pessoal deverá ser selecionado pela autoridade de controlo, eventualmente com a intervenção de um organismo independente incumbido nos termos do direito do Estado-membro.

Essa, em última análise, é a única forma de garantir ao administrado – potencial titular de dados, investigado e/ou interessado no bom andamento dos serviços jurídico-criminais – equilíbrio e proficiência.

5. ATUAÇÃO DA(S) AUTORIDADE(S) DE PROTEÇÃO DE DADOS NAS INVESTIGAÇÕES CRIMINAIS

Em linhas gerais, a principiologia da proteção de dados pessoais a serem tratados e aplicados para perscrutar a materialidade e autoria de delitos pouco difere da alusiva às relações ordinárias. A distinção entre os regramentos que deverão ser elaborados, na prática, é consequência direta da importância da persecução penal para a paz social, a prevenção de infrações e a reparação dos direitos das vítimas, a implicar inarredável choque entre direitos e interesses fundamentais do Estado e de seus súditos, que demandará múltiplas concessões para que ambas as franquias se acomodem harmonicamente.

Se o bom resultado das investigações – em especial os crimes de feição financeira e os levados a efeito por organizações criminosas – depende do uso e tratamento de dados pessoais[21], seria contraproducente e prejudicial à própria sociedade que aos órgãos investigadores fosse vedada a legitimidade para fazê-lo.

A resolução desse conflito é o essencial embasamento dos métodos investigativos em legislação específica, mas não taxativa, que possa instituir *standards* suficientes para respaldar a interpretação de investigadores e operadores, bem como esclarecer os titulares dos dados a respeito de seus direitos. Para as situações não expressamente reguladas – que não serão incomuns, mercê da dinâmica própria dos meios tecnológicos oferecidos pelo mercado –, o juízo acerca da utilidade, necessidade e proporcionalidade da diligência deverá prevalecer.

---

21 A propósito, o considerando 27 da Diretiva (UE) n. 2016/680 define: "Para efeitos de prevenção, investigação ou repressão de infrações penais, é necessário que as autoridades competentes tratem os dados pessoais, recolhidos no contexto da prevenção, investigação, deteção ou repressão de infrações penais específicas para além desse contexto, a fim de obter uma melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detetadas."

Quanto a esse assunto, o Conselho da Europa orienta:

> O tratamento de dados pessoais tem de ser feito de forma lícita, leal e transparente para com as pessoas singulares em causa, e exclusivamente para os efeitos específicos previstos na lei. Tal não obsta, em si mesmo, a que as autoridades de aplicação da lei exerçam atividades tais como investigações encobertas ou videovigilância. Tais atividades podem ser executadas para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, desde que estejam previstas na lei e constituam uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os interesses legítimos da pessoa singular em causa. A lealdade de tratamento, que constitui um dos princípios da proteção de dados, é uma noção distinta do direito a um tribunal imparcial, tal como definido no art. 47º da Carta e no art. 6º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH). As pessoas singulares deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos seus dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente ao tratamento desses dados. Em especial, os efeitos específicos do tratamento deverão ser explícitos e legítimos, e deverão estar determinados no momento da recolha dos dados pessoais. Os dados pessoais deverão ser adequados e relevantes para os efeitos para os quais são tratados. É especialmente necessário garantir que os dados pessoais recolhidos não sejam excessivos nem conservados durante mais tempo do que o necessário para os efeitos para os quais são tratados. Os dados pessoais só deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados são conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar prazos para o

> seu apagamento ou revisão periódica. Os Estados-membros deverão prever garantias adequadas aplicáveis aos dados pessoais conservados durante períodos mais longos a fim de fazerem parte de arquivos de interesse público ou de serem utilizados para fins científicos, estatísticos ou históricos. (UNIÃO EUROPEIA, 2016)

A par da vinculação aos princípios da legalidade e proporcionalidade, constitui encargo da ANPD[22] produzir campanhas de informação e conscientização dos cidadãos; aferir a pertinência dos dados recolhidos para as investigações em que forem empregados; supervisionar a política de conservação e eliminação de dados instituída por cada um dos órgãos.

Ademais, não se pode olvidar a atenção à cadeia de custódia (arts. 158-A a 158-F do Código de Processo Penal, inseridos pela Lei n. 13.964/2019); à manutenção de registros dos procedimentos de tratamento dos dados (*record keeping*); bem como o estabelecimento de instrumentos de controle das decisões automatizadas e sua submissão à revisão humana[23].

Importante destacar, ainda, que o sistema reserva à autoridade de controle papel relevante na avaliação da transmissão de dados a terceiros, com mais ênfase quando almejados fins econômicos. Assim também deverá agir quanto aos dados investigativos não suscetíveis de trans-

---

22 Por ANPD, entenda-se a autoridade escolhida pela legislação pertinente, que, como se antecipou no capítulo anterior, poderá ser outra que não a prevista pela LGPD.

23 Art. 11 da Lei n. 59/2019 de Portugal: "Decisões individuais automatizadas: 1 – São proibidas as decisões tomadas exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produzam efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa, exceto quando autorizadas por lei, desde que seja previsto o direito de o titular dos dados obter a intervenção humana do responsável pelo tratamento; 2 – As decisões a que se refere o número anterior não podem basear-se nas categorias especiais de dados pessoais previstos no artigo 6º."

ferência a outros órgãos – mesmo que integrem o *law enforcement* –, entidades ou particulares, sem a observância dos devidos critérios.

Ressalte-se que são essencialmente diferentes os dados pessoais baseados em fatos ou apreciações pessoais, a repercutir nas respectivas transmissibilidades. Eis o que preconiza o art. 10 da Lei portuguesa n. 59/2019 sobre o assunto:

> Artigo 10.
> Distinção entre dados pessoais e verificação da qualidade dos dados pessoais
> 1 – Sempre que possível, os dados pessoais baseados em factos devem ser distinguidos dos dados pessoais baseados em apreciações pessoais.
> 2 – Não podem ser transmitidos nem disponibilizados dados pessoais inexatos, incompletos, desatualizados ou não confiáveis.
> 3 – Para os efeitos previstos no número anterior, as autoridades competentes verificam, sempre que possível, a qualidade dos dados pessoais antes de estes serem transmitidos ou disponibilizados.
> 4 – Nos casos de transmissão de dados pessoais, as autoridades competentes que os transferem devem fornecer, sempre que possível, as informações necessárias para que as autoridades competentes que os recebem possam apreciar se os dados são exatos, completos, atuais e fiáveis.[24]

Da mesma sorte, apartam-se os dados conforme seus titulares, nas seguintes categorias: (i) acusados do cometimento de uma infração penal; (ii) condenados pela prática de um crime; (iii) vítimas de um

24 Internaliza o art. 7º da Diretiva (UE) n. 2016/680.

delito; e (iv) terceiros envolvidos em um fato criminoso, tais como testemunhas, contatos ou associados do(s) acusado(s)[25].

De todo modo, tal como disciplinado pelos arts. 33 e seguintes da LGPD, a ANPD avaliará o nível de proteção dos dados pessoais conferido por país ou organismo internacional (decisão de adequação). Regras para a transmissão excepcional desses dados, quando não certificado seu nível de proteção, também deverão aconselhar a atuação da autoridade de controle, quando necessário avalizar o procedimento[26].

6. CONCLUSÃO

Como resulta patente de toda a exposição, a autoridade de controle – independentemente do órgão/entidade a que essa identidade for emprestada –, no cumprimento de seus deveres institucionais, não se coloca em rota de colisão com os órgãos de persecução penal.

Ao inverso, há de estabelecer com eles ampla parceria, da qual depende o próprio sucesso do regime de conformidade que a LGPD

---

25 Art. 6º da Diretiva (UE) n. 2016/680.

26 Art. 40 da Lei portuguesa n. 59/2019: "Derrogações aplicáveis em situações específicas: 1 – Na falta, revogação ou suspensão de uma decisão de adequação ou de garantias adequadas nos termos dos artigos anteriores, a transferência ou as categorias de transferências de dados pessoais para um país terceiro ou para uma organização internacional só podem ser efetuadas se forem necessárias: a) Para proteger os interesses vitais do titular dos dados ou de outra pessoa; b) Para salvaguardar os legítimos interesses do titular dos dados; c) Para prevenir uma ameaça imediata e grave contra a segurança pública de um Estado-membro ou de um país terceiro; d) Em casos específicos, para a prossecução das finalidades estabelecidas no artigo 1º; ou e) Em casos específicos, para declarar, exercer ou defender, no âmbito de um processo judicial, um direito relacionado com as finalidades estabelecidas no artigo 1º."

projeta, uma vez que depende de ambos o sistema de apuração e sancionamento das infrações contra ela cometidas.

Noutra toada, a cooperação entre tais órgãos e a autoridade de proteção de dados propiciará maior conhecimento e respeito, no âmbito das investigações criminais e demais atividades, a todas as diretrizes, aos princípios legais e, sobretudo, aos constitucionais alusivos à matéria.

Não se deve esquecer, contudo, da relevância do arranjo penal e processual penal, como estrutura basilar do Estado de Direito e pressuposto inafastável para a maximização da paz social. Tendo sempre em mente a valia do trabalho do Ministério Público (mencionado em diversas ocasiões) e dos órgãos policiais, o Conselho da União Europeia elaborou a Diretiva (UE) n. 2016/680, a qual, atenta às peculiaridades das incursões de cunho criminal, compatibilizou os fundamentos da proteção de dados pessoais a essa atividade, que tem como marca indelével a demanda pelo acesso a muitas informações de feição pessoal.

Deve-se resistir, portanto, aos impulsos de impor limitações que, na prática, inviabilizam o poder-dever persecutório estatal, sem elastecer, ao menos substancialmente, a salvaguarda aos dados pessoais.

Essa tarefa se tornará mais fácil, à medida que se perceba a especialização dessa autoridade no escopo investigativo e sua aptidão para proceder ao controle, com mínima intrusão.

REFERÊNCIAS

ALEXANDRE JR., Júlio César. Cibercrime: um estudo acerca do conceito de crimes informáticos. *Revista Jurídica*, Franca, 1º jun. 2019, Faculdade de Direito de Franca. Disponível em: http://www.revista.direitofranca.br/index.php/refdf/article/download/602/pdf. Acesso em: 19 set. 2020.

ARAS, Vladimir. O COAF de um paraíso tropical. *Jota*, 19 set. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/o-coaf-de-um-paraiso-tropical-19072019. Acesso em: 19 set. 2020.

BLAGITZ, Melissa; LODDER, George. Procedimento de moderação do Projeto de Lei n. 2630/2020: objetividade e controle. *Jota*, 28 ago. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/procedimento-de-moderacao-do-projeto-de-lei-no-2630-2020-objetividade-e-controle-29082020. Acesso em: 19 set. 2020.

BRASIL. Supremo Tribunal Federal. *Informativo STF*, Brasília, n. 383, 11-15 abr. 2015. Disponível em: http://www.stf.jus.br//arquivo/informativo/documento/informativo383.htm. Acesso em: 19 set. 2020.

GARCIA, Emerson. *Ministério Público*: organização, atribuições e regime jurídico. 3. ed. Rio de Janeiro: Lumen Juris, 2008.

PFEIFFER, Roberto Augusto Castellanos. ANPD em busca de sua autonomia: é preciso aperfeiçoar a MP 869/2018. *Cojur*, 1º maio 2019. Disponível em: https://www.conjur.com.br/2019-mai-01/garantias-consumo-anpd-busca-autonomia-preciso-aperfeicoar-mp. Acesso em: 13 set. 2020.

PORTUGAL. Lei n. 59, de 26 de julho de 2019. Aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. *Diário da República Eletrônico*, n. 151/2019, Série I de 2019-8-8. Disponível em: https://dre.pt/home/-/dre/123815983/details/maximized. Acesso em: 27 nov. 2020.

SOUZA, Arthur de Brito Gueiros. Programas de *compliance* e a atribuição de responsabilidade individual nos crimes empresariais. *In*: VITORELLI, Edilson (Coord.). *Temas atuais do Ministério Público Federal*. 4. ed. Salvador: JusPodivm, 2016.

TEFFÉ, Chiara Spadaccini de. Por que precisamos de uma Autoridade Nacional de Proteção de Dados? *Jota*, 7 jan. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/por-que-precisamos-de-uma-autoridade-nacional-de-protecao-de-dados-07012020. Acesso em: 9 set. 2020.

UBALDO, Flávia Safadi. Lei Anticorrupção: a importância do programa de *compliance* no cenário atual. *In*: PORTO, Vinicius; MARQUES, Jader. *O compliance como instrumento de prevenção e combate à corrupção*. Porto Alegre: Livraria do Advogado, 2017.

UNIÃO EUROPEIA. Parlamento Europeu e do Conselho da União Europeia. *Diretiva (UE) 2016/680, de 27 de abril de 2016*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=EN#d1e1048-89-1. Acesso em: 27 nov. 2020.

UNIÃO EUROPEIA. Parlamento Europeu e do Conselho da União Europeia. *General Data Protection Regulation* – GDPR, 27 abr. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 27 nov. 2020.

VERÍSSIMO, Carla. *Compliance*: incentivo à adoção de medidas anticorrupção. São Paulo: Saraiva, 2017.

TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS PARA FINS DE INVESTIGAÇÕES CRIMINAIS À LUZ DAS LEIS DE PROTEÇÃO DE DADOS PESSOAIS

Fernanda Teixeira Souza Domingos[1]
Melissa Garcia Blagitz de Abreu e Silva[2]
Neide M. Cavalcanti Cardoso de Oliveira[3]

RESUMO

A Lei Geral de Proteção de Dados (LGPD) brasileira tem várias semelhanças com o quadro europeu de proteção de dados, tanto o Regulamento Geral de Proteção de Dados (GDPR) como a Diretiva (UE)

---

1 Procuradora da República em São Paulo. Coordenadora do Grupo de Apoio sobre Criminalidade Cibernética da 2ª Câmara de Coordenação e Revisão Criminal do MPF. Coordenadora do Grupo de Combate a Crimes Cibernéticos da Procuradoria da República em São Paulo. Graduada em Direito na Universidade de São Paulo. Especialista em direitos difusos e coletivos pela Escola Superior do Ministério Público/SP. Especialista em direitos humanos e trabalho pela ESMPU. Mestranda em direito transnacional na *Faculté de droit, de sciences politique et de gestion* da *Université de Strasbourg*.

2 Procuradora da República em São Paulo. Membro do Grupo de Combate a Crimes Cibernéticos da Procuradoria da República em São Paulo. Ex-coordenadora do

n. 2016/680, que regula a proteção de dados e a transferência de dados em matéria penal. O novo regime de proteção de dados influenciará a transferência de informações em matéria penal, tal como concebida pela Convenção sobre Cibercriminalidade – Convenção de Budapeste –, que inclui a cooperação internacional e o acesso direto em determinadas circunstâncias. O Brasil ainda não solicitou uma decisão de adequação por parte da Comissão Europeia, o que permitiria a livre circulação de dados com a Europa. A falta dessa decisão pode dificultar, no futuro próximo, o fluxo de informações entre empresas europeias e autoridades brasileiras, apesar das disposições da Convenção de Budapeste e do art. 11 do Marco Civil da Internet. Uma solução para evitar a interrupção poderia ser a solicitação, pelo Poder Judiciário e o Ministério Público, da adequação, de modo a se permitir a transferência mais rápida de dados para investigações criminais.

Palavras-chave: Transferência Internacional de Dados de Investigação. Investigação Criminal. Convenção de Budapeste. LGPD. GDPR. Diretiva (UE) n. 2016/680.

Grupo de Combate a Crimes Cibernéticos da Procuradoria da República em São Paulo. Graduada em direito pela Universidade de São Paulo. Mestre em direito pela Universidade de Chicago.

3 Procuradora Regional da República da Procuradoria Regional da República na 2ª Região. Procuradora Regional Eleitoral Substituta no Estado do Rio de Janeiro. Coordenadora adjunta do Grupo de Apoio sobre Criminalidade Cibernética da 2ª Câmara de Coordenação e Revisão Criminal do MPF. Graduada em direito pela Universidade do Estado do Rio de Janeiro. Especialista em direitos humanos nas relações de trabalho pela Universidade Federal do Rio de Janeiro.

ABSTRACT

The Brazilian Data Protection Law (LGPD) has several similarities with the European Data Protection framework, both the General Protection Data Regulation (GDPR) and the Directive 2016/680, that regulates data protection and data transfer in criminal matters. The new data protection regime will influence the transfer of information for criminal matters as devised by the Convention on Cybercrime (Budapest Convention), which includes international cooperation and direct access under certain circumstances. Brazil has yet to apply for an adequacy decision from the European Commission, what would permit the free flow of data between Europe and Brazil. The lack of an adequacy decision might hinder, in the near future, the flow of information between European companies and law enforcement authorities in Brazil, despite the provisions of the Budapest Convention and of article 11 from Brazilian Civil Rights Framework for the Internet (Marco Civil da Internet). A solution to avoid the interruption could be for a specific sector, the Criminal Justice System, to apply for adequacy, allowing the transfer of data for criminal investigations.

Keywords: Data Protection. International Data in Criminal Matters. Criminal Investigation. Budapest Convention. LGPD. GDPR. Directive (UE) n. 2016/680.

1. INTRODUÇÃO

Para discorrer sobre proteção aos dados de investigação e cooperação jurídica internacional criminal é essencial contextualizar a Lei Geral de Proteção de Dados (LGPD) brasileira e seus desdobramentos, no âmbito da cooperação jurídica internacional. Nesse contexto, relativamente à matéria penal, é necessário informar que o Brasil se encontra

em processo de adesão à Convenção do Conselho da Europa contra a Cibercriminalidade, também conhecida como Convenção de Budapeste.

A Convenção sobre Cibercriminalidade do Conselho da Europa – ETS n. 185 (CONSELHO DA EUROPA, 2001) é atualmente o principal instrumento internacional para a persecução de crimes cibernéticos e obtenção de provas eletrônicas. As principais economias do mundo já a ratificaram, ou estão em processo de adesão, excetuando-se China e Rússia. São membros da Convenção, além dos países do Conselho da Europa, Estados Unidos, Austrália, Japão, Canadá, Argentina, Chile, entre outros. O Brasil foi convidado a aderir em dezembro de 2019 e, atualmente, enquanto em processo de ratificação[4], possui *status* de observador.

Além de conter a tipificação de condutas penais referentes a crimes cibernéticos próprios e de outros facilitados pelo meio eletrônico (arts. 2º a 10º), a Convenção traz em seus arts. 14º a 35º instrumentos de investigação e compartilhamento de dados e provas eletrônicas entre os Estados-membros.

O pedido de adesão do Brasil, encaminhado por meio do Ministério das Relações Exteriores (MRE), foi resultado de anos de trabalho do Ministério Público Federal junto a esse órgão, analisando-se os benefícios a serem proporcionados ao Brasil pela Convenção e sobre sua compatibilidade com a legislação brasileira[5]. A principal vantagem será o estabelecimento de uma cooperação jurídica internacional, mais eficiente e confiável, com os países membros da Convenção.

---

4 O pedido de ratificação foi encaminhado à Câmara dos Deputados, no dia 22 de julho de 2020, após convite do Conselho da Europa para a adesão pelo Brasil à referida Convenção.

5 Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/notas-tecnicas. Acesso em: 14 out. 2020.

Além disso, espera-se conseguir mais agilidade na transferência de provas relacionadas a crimes cibernéticos, bem como de provas eletrônicas, o que inclui, na maioria das vezes, a transferência de dados pessoais de investigados. Necessário, assim, analisar os dois regimes de proteção de dados pessoais, o brasileiro e o europeu, a fim de se determinar o arcabouço atual de transferência de dados para fins penais.

2. O REGIME BRASILEIRO DE PROTEÇÃO DE DADOS

A LGPD, Lei n. 13.709, foi aprovada em 14 de agosto de 2018, com um período de *vacatio legis* de dois anos. Após a indefinição sobre sua entrada em vigor, inicialmente prevista para 14 de agosto de 2020 e posteriormente adiada, pelo disposto no art. 4º da Medida Provisória (MP) n. 959, para maio de 2021, a norma passou a ter vigência em 18 de setembro, quando sancionada em lei a MP, que restou aprovada sem aquele dispositivo. No entanto, as sanções administrativas (arts. 52 a 54) nela previstas foram postergadas para 1º de agosto de 2021, devido à aprovação da Lei n. 14.010/2020, que trata do Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado.

Seguindo o Regulamento Geral de Proteção de Dados Europeu – *General Data Protection Regulation* (GDPR) – Regulamento (UE) n. 2016/679 do Parlamento Europeu e do Conselho da União Europeia, a LGPD prevê várias regras com o fim de garantir máxima proteção e segurança na transferência internacional de dados. Da mesma forma que a legislação europeia, a brasileira disciplina três regimes diferentes de salvaguardas para transferências internacionais de dados, que seriam:

> (i) a declaração de existência de grau de proteção de dados pessoais adequado ao previsto na LGPD;
>
> (ii) a existência de garantias de cumprimento dos preceitos da LGPD;

> (iii) derrogações específicas do regime da LGPD, casuisticamente listados com vistas a promover algum objetivo de interesse público. (...) a manutenção de três regimes diferentes está – ao menos em tese – em consonância com o ponto de vista de que a proteção de dados pessoais está intimamente relacionada à proteção de direitos fundamentais. (CARVALHO, 2019, p. 624)

Para melhor compreensão do assunto aqui tratado, faz-se necessária uma breve análise de cada um deles.

2.1 TRANSFERÊNCIA DE DADOS PARA PAÍSES COM REGIME ADEQUADO DE PROTEÇÃO

No inciso I do art. 33 da LGPD está prevista a permissão de transferência internacional de dados para países ou organismos internacionais que proporcionem nível adequado de proteção. Esse dispositivo, entretanto, não esclarece os detalhes para a qualificação de determinado sistema legal como "adequado" aos preceitos da lei brasileira. Tal função é reservada à autoridade nacional, no art. 34, que em seus incisos prevê as bases a serem levadas em consideração.

Assim, a lei brasileira não exige que ordenamentos estrangeiros contem com uma legislação específica sobre proteção de dados, mas que, "em última análise, o núcleo fundamental da LGPD possa ser encontrado, ainda que difusamente, no ordenamento destinatário dos dados a serem transferidos" (CARVALHO, 2019, p. 626).

Essa análise caberá à Autoridade Nacional de Proteção de Dados. Sua decisão, com efeitos amplos e gerais, determinará a postura do Brasil em relação ao órgão estrangeiro e representará uma declaração de idoneidade do regulamento em questão por determinado período, após o qual o posicionamento pode ser alterado (CARVALHO, 2019, p. 626).

2.2 TRANSFERÊNCIA DE DADOS QUANDO HÁ GARANTIAS DE CUMPRIMENTO DOS PRECEITOS DA LGPD

O segundo regime de transferência internacional de dados, trazido no art. 33, II, do diploma, prevê essa possibilidade mediante "a existência de garantias de cumprimento dos preceitos da LGPD". Isso permite, mesmo em um quadro normativo com um nível de proteção menor que a legislação brasileira, a transferência de dados com base em salvaguardas apresentadas pela parte requerente dos dados, aprovadas pela autoridade nacional, conforme previsto na LGPD, em observância aos padrões fixados por autoridades de controle independentes e desvinculadas de governos (CARVALHO, 2019, p. 627).

Nesse caso, mesmo que o país estrangeiro para onde os dados se destinem não apresente todas as salvaguardas necessárias ao atendimento dos padrões protetivos previstos pela LGPD, é possível que o controlador específico ofereça e comprove garantias de cumprimento dos preceitos da lei brasileira, seja por meio de cláusulas contratuais – padrão ou específicas –, normas corporativas globais, ou selos, certificados e códigos de conduta regularmente emitidos.

2.3 TRANSFERÊNCIA DE DADOS EM RAZÃO DO INTERESSE PÚBLICO

Por fim, a LGPD prevê um terceiro regime para a transferência internacional de dados, disposto nos seus incisos III a VIII do art. 33, que são situações específicas, não abrangidas pelos anteriores, que visam outros objetivos de interesse público, *in verbis*:

> III – quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;

IV – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

V – quando a autoridade nacional autorizar a transferência;

VI – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VII – quando for necessária para a execução de política pública ou atribuição legal do serviço público;

VIII – quando o titular tiver fornecido o seu consentimento específico para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente essa de outras finalidades;

IX – quando necessário para atender às hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

2.4 TRANSFERÊNCIA DE DADOS EM RAZÃO DA SEGURANÇA PÚBLICA, ATIVIDADES DE INVESTIGAÇÃO E REPRESSÃO DE INFRAÇÕES PENAIS

Nos termos do art. 4º, III, da LGPD, os dados pessoais destinados à segurança pública e às atividades de investigação e repressão de infrações penais, bem como à defesa nacional estão excepcionados das regras de proteção previstas na LGPD, à semelhança da redação do GDPR. Em ambos os regimes, há a previsão da edição de normas específicas para regulamentar a proteção e transferência de dados pessoais para fins de persecução penal.

A União Europeia já tem um regulamento próprio trazido pela Diretiva (UE) n. 2016/680 (UNIÃO EUROPEIA, 2016) do Parlamento Europeu e do Conselho da União Europeia, que trata da proteção dos dados referentes à prevenção, investigação e persecução penal, bem como repressão de infrações penais e execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Mas o Brasil, não. Embora o art. 33 faça expressa menção à possibili-

dade de transferência internacional de dados quando "necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional", entre outras situações, o art. 4º, § 1º, da LGPD dispõe que deve haver legislação específica para a matéria.

Assim, em notícia publicada pela Câmara dos Deputados (JÚNIOR, 2019), em novembro de 2019, foi criada, pelo seu presidente, uma Comissão Parlamentar na Câmara dos Deputados formada por juristas renomados no tema, para propor projeto de lei sobre o uso de dados pessoais em investigações penais e segurança pública.

Com a entrada em vigor da LGPD e a aguardada ratificação pelo Brasil da Convenção de Budapeste, almeja-se a célere retomada dos trabalhos, interrompidos pela pandemia da covid-19. Pretende-se que o projeto de lei sobre a proteção de dados pessoais referentes a segurança pública, defesa nacional e investigações criminais seja finalizado e aprovado o mais breve possível.

As previsões das exceções devem observar os princípios previstos no art. 6º da lei, principalmente os da finalidade e segurança. Alguns preceitos presentes na LGPD também constam em outras leis de primeira e segunda geração, de acordo com Doneda (2011), uma vez que são universais e facilitam a transferência internacional de dados.

3. O REGIME EUROPEU DE TRANSFERÊNCIA INTERNACIONAL DE DADOS

Conforme exposto, a LGPD se inspira em diversos dispositivos do GDPR para regular a proteção de dados. Em linhas gerais, em seu art. 45, o regulamento europeu também permite a transferência de dados quando se reconhece que o ordenamento jurídico do país recipiente oferece nível de proteção adequado, ou quando o controlador dispõe de salvaguardas apropriadas – art. 46.

Entretanto, conforme descrito acima, a transmissão de dados para fins de persecução penal entre países regidos pelo GDPR e outros deverá obedecer ao regramento próprio trazido pela Diretiva (UE) n. 2016/680 do Parlamento Europeu e do Conselho da União Europeia.

3.1 O REGIME DA DIRETIVA "POLICIAL" (UE) 2016/680

Com a regulação da proteção dos dados pessoais no âmbito da União Europeia, surge a questão relativa ao tratamento a ser dispensado aos dados pessoais coletados com os fins de prevenção, investigação, detecção ou repressão de infrações penais, ou ainda execução de sanções penais – salvaguardas e prevenção de ameaças à segurança pública.

Evidente que tais dados não poderiam seguir o mesmo regime de outros comuns, delineado no GDPR, uma vez que, para dados que tenham finalidade específica voltada à segurança pública, há imposição na coleta e tratamento que não se coaduna com o consentimento, um dos pilares da nova regulação. Logo, o consentimento do titular dos dados não pode ser o fundamento jurídico do tratamento deles pelas autoridades competentes. Isso não significa que estarão isentos de proteção nas fases de coleta, tratamento e compartilhamento.

Dessa maneira, os dados coletados pelas autoridades competentes com os fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais – salvaguardas e prevenção de ameaças à segurança pública devem circular entre as autoridades competentes congêneres justamente para permitir a eficiência na manutenção da ordem e segurança públicas. É isso que a Diretiva (UE) n. 2016/680 aponta no item (4) da explanação de motivos, ao afirmar que a transferência desses dados para países terceiros e organizações internacionais deve ser facilitada, assegurando-se simultaneamente um elevado nível de proteção das informações pessoais.

Assim, a segurança de dados pessoais no domínio da cooperação jurídica em matéria penal e da cooperação policial assenta-se em garantir que as autoridades estrangeiras e/ou organismos internacionais dispensarão aos dados compartilhados o mesmo nível de proteção e tratamento que lhes é dispensado pelas autoridades que os detêm. Isso diz respeito, por exemplo, à finalidade específica de uso dos dados pessoais, que deve ser permitida pela autoridade que os compartilha, não podendo ser reutilizados para outros fins sem sua prévia autorização; à confidencialidade e segurança que devem ser garantidos a tais dados, de forma que o acesso desses dados e do equipamento empregado para o seu tratamento somente estejam franqueados a pessoas autorizadas.

O item 31 da explanação de motivos da diretiva esclarece ainda que, ao se levar em conta a circulação desses dados em cooperação jurídica em matéria penal e em cooperação policial, é esperada, quando aplicável, a distinção entre dados pessoais de diferentes categorias de titulares, tais como, suspeitos, pessoas condenadas, vítimas, terceiros, assim entendidos testemunhas e informantes e outras pessoas consideradas relevantes para as investigações. Podem, ainda, ser previstas condições reputadas necessárias pelas autoridades transmissoras dos dados, como proibição de notificação do titular ou garantias adicionais quando o material transmitido for considerado sensível, referentes aos direitos e às liberdades fundamentais.

A autoridade competente para remessa e recebimento dos dados pessoais regulados pela diretiva, nos termos do art. 3º, número 7, são precisamente as autoridades públicas competentes para exercer as atividades de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Assim, o diploma apresenta como formas de validar a transferência internacional dos dados a ela pertinentes:

- a decisão de adequação, que reconhece no país terceiro, no organismo internacional ou em um ou mais setores específicos desse país terceiro um nível de proteção de dados pessoais adequado;
- o fornecimento de garantias adequadas para a proteção mediante um instrumento juridicamente vinculativo;
- a derrogação das regras da diretiva no caso de situações específicas: se a transferência for necessária para proteger interesses vitais do titular dos dados e/ou seus legítimos interesses, para prevenir ameaça iminente e grave contra a segurança pública de um Estado-membro ou país terceiro, e em outros em que haja justificativa, inclusive exercício ou defesa de um direito num processo judicial.

De notar-se que a decisão de adequação pode ser dada relativamente a um país terceiro ou a um ou mais setores específicos desse país.

Esse dispositivo se encontra descrito no art. 36 da diretiva e nos itens 66 a 70 da Explanação de Motivos. Ele traz os critérios adotados para decidir pela adequação, abrindo a possibilidade para a transferência de dados pessoais para um setor específico do país que já atenda o nível esperado de proteção, mesmo que o país não tenha completamente se adequado a todas as regras de proteção. Ele possibilita, portanto, que as transferências de dados pessoais para esse setor do país terceiro ocorram sem necessidade de autorização específica, facilitando sobremaneira a circulação dos dados pessoais e permitindo a fluidez tão desejada e necessária no âmbito da prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Embora as disposições mais estritas concernentes à transferência internacional de dados pessoais para fins de investigações criminais ainda não estejam sendo aplicadas na prática, à medida que alguns Estados se movimentaram para aumentar o grau de proteção desses dados, os demais passaram a reformular suas legislações para acompanhar a evolução na sofisticação das medidas.

4. OS MECANISMOS DE TRANSFERÊNCIA INTERNACIONAL DE DADOS PREVISTOS NA CONVENÇÃO DE BUDAPESTE

A Convenção de Budapeste indica, basicamente, duas formas de transferência internacional de dados para fins de investigações criminais, por meio de cooperação internacional e por meio de acesso direto.

4.1 COOPERAÇÃO INTERNACIONAL

A cooperação internacional prevista na Convenção é regida pelos arts. 23 e seguintes, podendo caracterizar-se pela transmissão espontânea de dados, art. 26[6], quando um Estado-parte identifica elementos que possam justificar o início de investigação criminal por outro Estado-parte, e pelo cumprimento de pedidos de cooperação. Nesse contexto, regulado pelos arts. 27 e seguintes, a própria Convenção pode servir como tratado disciplinador da cooperação, caso os dois envolvidos optem por utilizá-la ou caso não possuam entre si instrumento próprio de cooperação internacional.

A cooperação jurídica em matéria penal regida pela Convenção dispõe de mecanismos próprios para assegurar a rapidez na execução dos pedidos, como a possibilidade de transmissão das solicitações entre autoridades judiciais diretamente responsáveis pelo pedido e cumprimento[7],

---

6 Art. 26. Uma Parte pode, dentro dos limites de sua legislação interna e sem pedido anterior, transmitir, para outra Parte, informações obtidas por seu próprio sistema investigativo, quando considerar que o encaminhamento de tais informações pode auxiliar a Parte destinatária a iniciar ou a levar adiante investigações ou procedimentos relativos a crimes tipificados de acordo com esta Convenção ou possa levar a um pedido de cooperação por aquela Parte, em conformidade com este capítulo (...). (Tradução livre)

7 Art. 27, 9a.

com simples aviso para a autoridade central em caso de urgência, e a preservação rápida de provas[8], tudo em razão da natureza volátil das provas eletrônicas. Entretanto, de maneira geral, a cooperação prevista na Convenção segue os mesmos preceitos da cooperação jurídica em matéria penal, com análise de cabimento caso a caso e atendimento individualizado, com ou sem a imposição de condições para uso da prova.

4.2 O ACESSO DIRETO TRANSFRONTEIRIÇO

Já os mecanismos de acesso direto trazidos pela Convenção contêm avanços considerados significativos na época de sua elaboração, em 2001, embora hoje necessitem de revisão.

Os arts. 18 e 32 permitem o acesso direto a dados:

> Artigo 18 – Requisição
>
> 1. Cada Estado-Parte adotará as medidas legislativas e outras providências necessárias para dar poderes a suas autoridades competentes para ordenar:
>
> a. a qualquer pessoa em seu território a entrega de dados de computador especificados sob seu controle ou posse, que estejam armazenados em um sistema de computador ou em qualquer meio de armazenamento de dados de computador;
>
> b. a qualquer provedor de serviço que ofereça serviços no território da Parte para entregar as informações cadastrais de usuários relacionadas a tais serviços, que estejam sob a posse ou controle do provedor.
>
> 2. Os poderes e procedimentos referidos neste artigo estão sujeitos aos artigos 14 e 15.

8 Art. 29.

> 3. Para fins deste artigo, o termo "informações cadastrais do usuário" indica qualquer informação em forma eletrônica ou em qualquer outra, que esteja em poder do provedor de serviço e que seja relativa a usuários de seus serviços, com exceção dos dados de tráfego e do conteúdo da comunicação, e por meio da qual se possa determinar:
>
> a. o tipo de serviço de comunicação utilizado, as medidas técnicas tomadas para esse fim e o período de serviço;
>
> b. a identidade do usuário, endereço postal ou geográfico, o telefone e outros números de contato e informações sobre pagamento e cobrança, que estejam disponíveis de acordo com os termos de prestação de serviço;
>
> c. qualquer outra informação sobre o local de instalação do equipamento de comunicação, disponível em razão dos termos de prestação de serviço;
>
> Artigo 32 – Acesso transfronteiriço a dados de computador armazenados mediante consentimento ou quando acessíveis publicamente
>
> Uma Parte pode, sem autorização de outra Parte:
>
> a. acessar dados de computador armazenados disponíveis ao público (fonte aberta), independentemente de onde os dados estejam geograficamente localizados; ou
>
> b. acessar ou receber, por meio de um sistema de computador em seu território, dados de computador armazenados localizados no território de outra Parte, se a Parte obtiver o legítimo e voluntário consentimento de uma pessoa que tenha autoridade legal para entregar os dados à Parte por meio daquele sistema de computador. (Tradução livre – UNIÃO EUROPEIA, 2016)

O segundo dispositivo lida com situações aparentemente corriqueiras, mas que eram de grande valia quando da entrada em vigor da Convenção.

A alínea *a* reconhece que as autoridades dos Estados-parte podem acessar, de seu território, dados disponíveis ao público, mas que sejam

guardados em outro território. A alínea *b* permite que esse acesso se estenda a dados privados desde que haja expresso consentimento do titular.

Em outras palavras, o dispositivo permite que autoridades de um país acessem e coletem como prova válida dados publicados em sítios mantidos em outro país. A condição para isso é que esses dados sejam públicos, ou seu uso seja consentido, de modo "legítimo e voluntário", pelo titular.

Ao condicionar o acesso à natureza pública dos dados ou ao consentimento do titular, o dispositivo não distingue quanto ao tipo, permitindo o acesso direto transfronteiriço a qualquer dado eletrônico, inclusive conteúdo de comunicações, desde que observadas as duas condições mencionadas.

Por outro lado, o art. 18 determina que os Estados-parte, em suas legislações locais, estabeleçam mecanismo que permita às autoridades judiciais a requisição de quaisquer dados armazenados sob a posse ou controle de provedores localizados em seu território (1.a) e de dados cadastrais de usuários que estejam sob a posse ou controle de provedores que prestam serviço em seu território, ainda que estrangeiros (1.b).

Há aqui, portanto, duas situações: uma que permite o acesso, mediante o cumprimento da legislação local, a todos os dados armazenados por provedores locais, incluindo conteúdo; e outra que permite acesso a dados cadastrais de usuários controlados por provedores estrangeiros, desde que estes prestem serviço no território do Estado requisitante. Admite-se, assim, o acesso direto a dados localizados em outro território e controlados por provedor estrangeiro desde que: a) as informações buscadas se restrinjam a dados cadastrais; e b) o provedor estrangeiro preste serviço no território da autoridade requisitante.

A legislação brasileira, mesmo antes da adesão formal à Convenção, já permite o acesso direto a dados eletrônicos localizados fora do território brasileiro em termos semelhantes, porém mais amplos. O art. 11 do Marco Civil da Internet, Lei n. 12.965, de 23 de abril de 2014, determina que, mediante prévia ordem judicial, as autoridades brasileiras tenham acesso a dados armazenados, inclusive conteúdo de comunicações, por

empresas brasileiras ou estrangeiras, desde que: a) ofereçam serviços ao público brasileiro ou b) tenham ao menos um integrante do grupo econômico com estabelecimento no Brasil.

O citado dispositivo é, portanto, mais amplo que a previsão do art. 18. Enquanto este permite o acesso apenas a dados cadastrais de usuários controlados por empresas estrangeiras que prestam serviço no território do Estado-parte, aquele permite o acesso a todos os dados, inclusive conteúdo armazenado por empresa estrangeira, desde que ela oferte serviços a brasileiros ou aqui mantenha estabelecimento de um dos componentes de seu grupo econômico.

5. AS CONSEQUÊNCIAS DO REGIME DE PROTEÇÃO DE DADOS PARA A TRANSFERÊNCIA DE DADOS EM INVESTIGAÇÕES CRIMINAIS – NOVA PROPOSTA

O atual sistema de proteção de dados, mesmo com regras específicas para a persecução penal, afeta diferentemente o regime de transferência de dados, dependendo do tipo de transferência utilizada.

Para as transferências por meio de cooperação internacional, os acordos de cooperação continuam servindo como base, pois a Diretiva (UE) n. 2016/680, no art. 61, expressamente ressalvou a manutenção dos tratados internacionais em vigor até que sejam alterados, substituídos ou revogados[9].

Essa disposição permite a continuidade da troca de informações no âmbito da cooperação policial e da cooperação judiciária internacional.

---

9 "Art. 61. Os acordos internacionais que impliquem a transferência de dados pessoais para países terceiros ou para organizações internacionais, celebrados pelos Estados-membros antes de 6 de maio de 2016, e que sejam conformes com o direito da União tal como aplicável antes dessa data, continuam a vigorar até serem alterados, substituídos ou revogados."

Se tal não fosse, toda a circulação de dados para fins de persecução penal a prevenção às infrações penais estaria paralisada em razão das exigências dessa normativa, uma vez que o nível de proteção exigido dos países terceiros não é passível de ser alcançado no curto prazo, devido às inúmeras adequações que precisam ser feitas.

Tal solução, porém, é provisória, sendo indispensável buscar uma definitiva que passe pela decisão de adequação.

Quanto ao acesso direto, os efeitos da ausência de decisão de adequação podem começar a ser sentidos imediatamente. Como mencionado, a Convenção de Budapeste prevê dois tipos. O previsto no art. 32 não é afetado pelas disposições da diretiva porque referente a dados públicos, não abrangidos pelo regime de proteção de dados, ou a dados privados acessados mediante o consentimento do titular. Não há, assim, problema para a transferência.

Entretanto, o assunto adquire outra relevância quando se trata de acesso direto à prova eletrônica, nos termos do art. 18 da Convenção de Budapeste e do art. 11 do Marco Civil. Nesses casos, sem decisões prévias de adequação ou de reconhecimento de salvaguardas, as empresas europeias que aqui prestam serviços a usuários brasileiros podem se considerar impedidas de transferir os dados, com sérias consequências para investigações penais em andamento.

Enquanto a decisão sobre a adequação do regime brasileiro de proteção de dados não vem, e na pendência da ratificação da Convenção de Budapeste, que poderá servir como respaldo jurídico para a transferência de dados pessoais, faz-se necessário o estabelecimento de outro modelo que permita que o fluxo de dados para fins de persecução penal não seja interrompido[10]. Nesse sentido, propõe-se ao Ministério Público Federal

10 Tratados internacionais podem servir de base legal para permitir a transferência de dados, incluindo a Convenção de Budapeste (CETS 185 – CONSELHO DA EUROPA, 2001).

a adequação ao quanto exigido pela diretiva e pelo GDPR, recebendo em nome próprio a decisão de adequação.

Como exposto, nos termos do art. 36 da Diretiva (UE) n. 2016/680, a decisão de adequação pode ser concedida a países terceiros e a territórios, ou, ainda, a um ou mais setores específicos de um determinado país. Exemplo disso é a decisão de adequação, ainda vigente apesar de baseada na antiga Diretiva (UE) n. 95/46 – substituída pelo GDPR –, que reconhece apenas os setores abrangidos pela lei canadense de dados pessoais e documentos eletrônicos como adequados à regulação europeia[11]. É possível, assim, que determinados setores sejam reconhecidos como adequados, ainda que o país como um todo não o seja.

Nesse ponto é que se propõe que o sistema nacional de Justiça, em especial o Ministério Público e o Poder Judiciário, busque a adequação exigida pelo GDPR e pela Diretiva (UE) n. 2016/680.

Enquanto o Brasil, como Nação, não obtém a decisão de adequação, o que hoje depende, em grande parte, da estrutura da Autoridade Nacional de Proteção de Dados (ANPD), tanto o Ministério Público quanto o Poder Judiciário podem buscá-la para fins de acesso direto de dados em investigações criminais, como um setor específico.

Embora ainda não tenha sido editada lei que regulamente a proteção de dados relativos à segurança pública e investigações criminais, é certo que o sistema de justiça brasileiro tem todas as condições de se adequar ao regime da diretiva. O acesso a dados pessoais somente é feito mediante ordem judicial, por meio de decisão fundamentada, em casos específicos e para a investigação de condutas determinadas. Os dados obtidos são mantidos sob sigilo durante todo o processo penal, com acesso restrito às partes. O uso em outros feitos depende também

11 Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002D0002&from=en. Acesso em: 14 out. 2020.

de autorização judicial, o que estabelece sistema robusto de proteção. Ademais, o titular é informado da obtenção e do uso, ainda que de forma diferida, dispondo de mecanismos legais para excluir os dados a qualquer momento, seja nos próprios autos, seja por meio de ações autônomas, como *habeas corpus* e mandado de segurança.

Importante notar que o sistema legal em vigor não precisa ser cópia do modelo europeu, basta que as proteções sejam equivalentes. Ademais, a análise da adequação do setor funda-se nos aspectos específicos deste. O item 67 da exposição de motivos determina que:

> De acordo com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou de um setor específico num país terceiro, ter em consideração em que medida um determinado país respeita o primado do Estado de direito, o acesso à justiça, bem como as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. *A adoção de uma decisão de adequação relativa a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro*. Este deverá dar garantias de assegurar um *nível adequado de proteção, essencialmente equivalente ao segurado na União*, em particular quando os dados são tratados num ou em vários setores específicos. Em especial, o país terceiro deverá garantir o controle efetivo e independente da proteção dos dados e estabelecer mecanismos de cooperação com as autoridades de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial. (UNIÃO EUROPEIA, 2016 – Grifos nossos)

Vê-se, portanto, que, para fins de investigações e processos criminais, o arcabouço legal em vigor no Brasil já atende ao quanto exigido pela diretiva e pelo GDPR. Embora ainda não haja legislação específica sobre o assunto, como exigido pela LGPD, as limitações impostas pela Constituição Federal, pelo Marco Civil e pela legislação processual penal já são suficientes para assegurar proteção adequada aos dados e demonstrar adequação ao sistema europeu. Assim, o reconhecimento desta é medida que pode ser buscada pelo Poder Judiciário e Ministério Público, como um setor à parte.

6. CONCLUSÃO

O novo sistema de proteção de dados pessoais introduzido pelo GDPR, pela Diretiva (UE) n. 2016/680 e pela LGPD precisa ser levado em consideração na busca de provas em investigações e processos criminais.

Esse sistema pode gerar consequências para a correta aplicação do art. 11 do Marco Civil da Internet, em especial, quanto à obtenção de dados de empresas europeias que prestam serviço no Brasil e que, por estarem submetidas ao diplomas normativos da UE, podem criar empecilhos para o acesso direto aos dados, na forma da lei brasileira.

Solução de longo prazo, e que precisa ser buscada, é o reconhecimento da adequação da legislação brasileira ao quanto exigido pelas normas europeias. Enquanto isso não ocorre, o Poder Judiciário e o Ministério Público podem buscar o reconhecimento da adequação como setor específico.

Isso permitirá que os dados sejam transferidos sem interrupção para fins de persecução penal, possibilitando a continuidade de investigações em andamento e assegurando a celeridade exigida pela natureza da prova eletrônica.

REFERÊNCIAS

BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 out. 2020.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados brasileira (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 out. 2020.

BRASIL. *Lei n. 14.010, de 10 de junho de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm#:~:text=Disp%C3%B5e%20sobre%20o%20Regime%20Jur%C3%ADdico,coronav%C3%ADrus%20(Covid%2D19).&text=Art.&text=3%C2%BA%20Os%20prazos%20prescricionais%20consideram,30%20de%20outubro%20de%2020. Acesso em: 14 out. 2020.

BRASIL. *Medida Provisória n. 959, de 29 de abril de 2020*. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 14 out. 2020.

BRASIL. Ministério Público Federal. *Notas técnicas 4 e 5*. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/notas-tecnicas. Acesso em: 14 out. 2020.

CARVALHO, Angelo Gamba Prata de. Transferência internacional de dados na Lei Geral de Proteção de Dados – Força normativa e efetividade diante do cenário transnacional. *In*: FRAZÃO Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coords.). *A Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro*. São Paulo: Thompson Reuters do Brasil, 2019.

CONSELHO DA EUROPA. Convenção de Budapeste. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Acesso em: 8 out. 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico*, Joaçaba, v. 12, n. 2, p. 91-108, jul.-dez. 2011.

JÚNIOR, Janary. *Maia cria comissão de juristas para propor lei sobre uso de dados pessoais em investigações*: Colegiado terá 120 dias para elaborar o anteprojeto que, depois, será analisado pelo Congresso. Brasília, Câmara dos Deputados, 27 nov. 2019. Disponível em: https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/. Acesso em: 14 out. 2020.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho. *Diretiva (UE) 2016/680, de 27 de abril de 2016*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016L0680&from=EN#d1e1048-89-1. Acesso em: 14 out. 2020.

UNIÃO EUROPEIA. Parlamento Europeu e Conselho. *General Data Protection Regulation* – GDPR, 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 14 out. 2020.

GARANTÍAS REQUERIDAS EN LA UE PARA LA TRANSFERENCIA INTERNACIONAL DE DATOS A TERCEROS PAÍSES EN LA COOPERACIÓN JUDICIAL PENAL INTERNACIONAL

Rosa Ana Morán Martínez[1]

RESUMEN

El nuevo régimen de protección de datos de la UE tendrá un impacto muy significativo en la transmisión de datos a terceros países en el ejercicio de la actividad de cooperación internacional. El articulo identifica las principales dificultades que pueden resultar de su aplicación y las posibles soluciones contenidas en la Directiva 2016/680.

Palabras clave: Protección de datos de la UE. Directiva de aplicación de la ley de protección de datos. Transferencias de datos personales a terceros países u organizaciones internacionales.

---

1 Fiscal de Sala del Tribunal Supremo en España. Fiscal Jefe y Coordinadora de la Cooperación Judicial internacional en la Fiscalía General del Estado. Licenciada en derecho por la Universidad de Oviedo. Cursos Master de derechos fundamentales en la UAB. Profesora universitaria en varias universidades. Responsable de la Secretaria General de la Asociación Iberoamericana de Ministerios Públicos (AIAMP).

ABSTRACT

The new EU regime of data protection has a significative impact on data transmission towards third states for purposes of international criminal justice cooperation. This article aims to identify the main difficulties that might arise and the potential solutions as contained on the EU Directive.

Keywords: EU data protection. Data protection law enforcement Directive. Transfers of personal data to third countries or international organizations.

1. INTRODUCCIÓN

El objeto de estas líneas es exponer algunas limitaciones y dificultades que el nuevo régimen de protección de datos de la Unión Europea (UE) puede conllevar para el intercambio de datos a través del sistema de asistencia legal mutua con países terceros y especialmente en este caso con los países del ámbito iberoamericano.

La cooperación judicial internacional en el ámbito penal consiste esencialmente en el intercambio de datos, pruebas, informaciones etc. entre las autoridades judiciales competentes de dos países lo que implica la necesidad de tener en cuenta el debido tratamiento de los datos personales que se transfieren en los dos Estados implicados.

En la UE, la protección de datos es un derecho fundamental de los ciudadanos reconocido en el art. 8 de la Carta de Derechos Fundamentales (CDF) lo que conlleva la imposición de estrictas obligaciones a los poderes públicos en el tratamiento y protección de los datos personales. Se exige también a las autoridades judiciales de los países europeos extremar el cuidado y realizar las debidas comprobaciones a la hora de remitir datos personales reclamados en una comisión rogatoria y

examinar si existen suficientes garantías de que los mismos vayan a ser sometidos en el país receptor a un tratamiento adecuado.

El garantista sistema adoptado por la UE debe a la vez permitir la cooperación transfronteriza en los procedimientos penales por lo que, para facilitar la comprobación de esas garantías, prevé realizar evaluaciones y declaraciones de adecuación de los sistemas de distintos países no miembros de la UE. Sin embargo, el régimen de protección de datos exigido en la Directiva UE 2016/680, de 20 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, es de aplicación desde el 6 de mayo de 2018, sin que hasta ahora se hayan realizado *declaraciones de adecuación*. Esta situación eleva el nivel de preocupación de las autoridades judiciales competentes de los países de la UE a la hora de remitir datos a autoridades de terceros Estados, especialmente cuando no se cuenta con un Convenio multilateral o bilateral aplicable para la obtención o solicitud de la asistencia judicial mutua.

Estar al tanto del régimen europeo de protección de datos y sus exigencias y a la vez permitir a las autoridades de los Estados miembros de la UE conocer el sistema de tratamiento de datos en terceros Estados con los que se pretende cooperar puede facilitar los actos de ejecución de la cooperación judicial internacional y favorecer a su vez el cumplimiento de las garantías de un tratamiento adecuado tanto para las autoridades concernidas en el intercambio de datos como para los ciudadanos cuyos datos van a ser trasladados a través del mecanismo de la cooperación judicial internacional.

2. BREVE RESEÑA DEL SISTEMA DE PROTECCIÓN DE DATOS EN EL CONSEJO DE EUROPA (COE)

La evolución tecnológica y la globalización, que tantos beneficios y avances aportan a nuestras sociedades, comportan una capacidad de almacenamiento, tratamiento y transmisión de datos personales que amenazan derechos individuales relacionados con la privacidad.

El derecho a la protección de datos personales se reconozca o no como un derecho fundamental autónomo en la UE (art. 8 del CDF[2]) o bien obtengan una protección derivada del concepto de privacidad como se contempla aun en el sistema del Consejo de Europa (vinculado al art. 8 del CEDH) o en el sistema de NNUU, (vinculado al art. 12 de la DUDH), encierra un valor esencial que debe protegerse. La creciente capacidad tecnológica para recopilar, procesar y usar datos personales supone un riesgo cada vez mayor para la privacidad y para el control de los datos por sus titulares por lo que debe ser regulado imponiendo límites y vinculando el tratamiento a objetivos lícitos tanto para las empresas privadas como para las autoridades públicas.

La preocupación por el tratamiento y la protección de datos comenzó en Europa en la década de los 70, de forma que en ya 1981 el Consejo de Europa adoptó el primer *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos personales*[3]. Es este un Convenio pionero en la materia que se aplica a todo tratamiento de datos realizado por el sector privado y por el público, incluido el realizado por las autoridades policiales y judiciales en el ámbito de una investigación criminal.

El Convenio establece la necesidad del tratamiento licito y adecuado

---

2 Carta de Derechos Fundamentales de la Unión Europea, DO 2012 C-326.

3 Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, CoE. STCE n. 108, 1981.

de los datos, impone la obligación de seguridad y considera necesario un tratamiento más limitado de datos sensibles. A la vez, y por primera vez, se reconoce el derecho de las personas físicas a conocer los datos que sobre ellas se conservan y se tratan y sobre todo se reconoce el derecho de los titulares de los datos a solicitar su rectificación y supresión cuando corresponda.

El Convenio 108 del CoE se complementó en 2001 con un *Protocolo adicional* que introdujo disposiciones concretas sobre las transmisiones de datos trasfronterizos[4] a Estados que no forman parte del mismo.

Es importante señalar que, a partir de 1999, este Convenio está abierto a la firma de países no europeos lo que puede resultar de enorme interés a la hora de valorar como adecuado el sistema de protección de datos de cara a autorizar el intercambio y traslado de informaciones por parte de la autoridad competente[5].

El Convenio ha sido recientemente modernizado a través del Protocolo de modificación, adoptado el 18 de abril de 2018. En esta actualización necesaria del Convenio para adaptarlo a las nuevas circunstancias de la tecnología se preserva su carácter general para todo tipo de actividades privadas y públicas y se refuerza su potencial como instrumento universal de regulación de la protección de datos, a la vez que se introducen nuevas disposiciones sobre los flujos de datos transfronterizos a los Estados no Partes, los denominados terceros países. Se establece que los datos en el contexto de la investigación criminal solo pueden ser transferidos a autoridades competentes extranjeras en base a disposiciones jurídicas especiales –acuerdos internacionales– salvo que la transferencia resulte necesaria para evitar un peligro inminente.

---

4 Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, en lo que respecta a las autoridades de control y los flujos de datos transfronterizos, CoE. STCE n. 181, 2001.

5 Países como Argentina, México y Uruguay son parte de este Convenio.

Otras novedades significativas tratan de reforzar la protección de la privacidad en el ámbito digital y sobre todo establecer y de fortalecer mecanismos de control independiente para el control efectivo del cumplimiento de las normas.

Esta adaptación y modernización del Convenio se ha realizado en un trabajo coordinado con la UE alineando sus disposiciones con la reforma normativa de la protección de datos que ha realizado la UE y que dió lugar, esencialmente en el 2016, al paquete normativo que vamos a analizar seguidamente. Los reguladores del CoE y de la UE han tratado de asegurar la coherencia y la compatibilidad entre estos dos marcos jurídicos.

En el ámbito del CoE se han producido los primeros pronunciamientos relativos al tratamiento de datos por las autoridades policiales y la necesidad de que los mismos tengan un sistema de conservación y tratamiento adecuados. La Recomendación (87) 15[6] sobre el manejo de datos por la Policía ha sido un hito en el tratamiento de los datos en la investigación policial.

3. MARCO LEGAL DE LA UE EN RELACIÓN CON LA PROTECCIÓN DE DATOS EN LAS ACTIVIDADES DE COOPERACIÓN INTERNACIONAL

La protección de datos en la UE es un derecho fundamental reconocido en el art. 8 de la Carta de Derechos Fundamentales que establece que "toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan". Además, en su apartado segundo establece los principios clave de la protección de datos y exige que la protección de dichos principios esté sujeta al control de una autoridad independiente.

6 Disponible en esta dirección: https://rm.coe.int/168062dfd4.

Además de ser un derecho fundamental, el Tratado de Lisboa lo contempla como principio fundamental en el art. 16 y establece la base jurídica para que la UE legisle sobre protección de datos de una forma integral comprendiendo todas las materias competencia de la UE, también por tanto la investigación en materia penal.

La Directiva UE 2016/680, de 20 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos, por la que se deroga la DM 2008/977/JAI, –en adelante Directiva 2016/680– establece el nuevo marco legal en la UE en relación con la protección de datos en el ámbito general de la investigación criminal.

Esta Directiva es aplicable desde el 6 de mayo de 2018, fecha que su propio texto establece como límite para su desarrollo en los ordenamientos internos. La falta de implementación de esta Directiva no exime por tanto en este momento a ningún país de la UE de su aplicación[7]. Por ello, aunque no todos los países de la UE, España entre ellos, han implementado aun su contenido las obligaciones que contiene son directamente vinculantes y los derechos que de la misma derivan directamente invocables ante los Tribunales[8]. Además, cualquier normativa que regule la protección de datos en este ámbito debe interpretarse a

7 Conforme al régimen jurídico de la UE, las Directivas no son de aplicación directa, sino que deben ser transpuestas a las legislaciones nacionales de los Estados miembros.

8 El TJUE Tribunal de Justicia ha afirmado el llamado "efecto útil" de las Directivas de forma que se reconoce el derecho de los particulares a invocarla directamente cuando ésta sea clara e incondicional y le concediera un derecho particular si habiendo transcurrido el plazo de implementación no se hubiera implementado (STJUE 4 de diciembre de 1974, Van Duyn).

la luz de las disposiciones de esta Directiva conforme al principio de interpretación conforme establecido por el Tribunal de Justicia de la Unión Europea (TJUE) en el famoso "Caso Pupino"[9].

Esta Directiva forma parte de un paquete de normas de la UE sobre protección de datos que pivota especialmente en la norma general que es el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE –en adelante, RGPD–. Este Reglamento es la norma central en la materia y regula la protección de datos en relación con cualquier actividad no excluida expresamente. La Directiva 16/680 viene a complementar el paquete regulatorio en relación con la investigación penal, una actividad que, por sus características especiales, debe tener un tratamiento especial que permita una mayor flexibilidad en el tratamiento de datos y excluya la aplicación de algunos principios generales. En todo caso, Reglamento y Directiva son normas complementarias y su vinculación queda también patente en la coincidencia de la fecha de su aprobación.

El Reglamento, que, como tal, es directamente aplicable se refiere principalmente a actividades del ámbito privado y comercial por lo que impone unas normas muy estrictas en el tratamiento de los datos que las compañías obtienen y manejan en sus actividades comerciales. La UE estimó más oportuno y conveniente extraer de esta regulación a las actividades relacionadas con el proceso penal y regularlas en una Directiva en la que las normas particulares van dirigidas a cada Estado para que pueda realizar su particular adaptación normativa teniendo en cuenta su propio sistema de investigación y enjuiciamiento penal.

9 STJUE de 16 de junio de 2003, C-105/03, Caso Pupino.

De esta forma, todas aquellas actividades relacionadas con el proceso penal, definidas de forma tan amplia que comprenden todas las realizadas por las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales y a la libre circulación de dichos datos, se dotan de una regulación diferente más adecuada a los fines de interés general y público de la actividad de investigación criminal.

Por otro lado, hay que tener en cuenta que coexiste otro orden de actividad extraído tanto del Reglamento como de la Directiva y es el ámbito relativo al tratamiento efectuado por las instituciones, órganos y organismos de la Unión, al que se aplica una norma diferente, el *Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n. 45/2001 y la Decisión n. 1247/2002/CE*.

Es importante esta salvedad y atender a esta regulación cuando se aborda la cooperación judicial internacional en tanto que es una actividad en la que participan de forma habitual agencias y órganos de la UE como Eurojust, la RJE o la futura Fiscalía Europea. Estos órganos o agencias de la UE intervienen muy directamente en la actividad de cooperación judicial internacional en relación con procedimientos penales auxiliando a sus autoridades nacionales tienen, además del marco legal del mencionado Reglamento 2008/1725, normas específicas y complementarias relativas a la protección de datos en sus particulares regulaciones. Esas normas conforman también parte relevante del marco normativo aplicable a las actividades de cooperación judicial internacional.

En relación con la cooperación judicial que nos ocupa, entre estas normas que desarrollan el Reglamento 2008/1725 es importante tener en cuenta el Reglamento de Eurojust 2018/1727, de 14 de noviembre

de 2018, que dedica todo su Capitulo IV al tratamiento de la información, una regulación que se complementa con un *Reglamento interno de Eurojust relativo al tratamiento y a la protección de datos personales* publicado en el DOUE el 24 de febrero de 2020. También es relevante a estos efectos el Reglamento 2017/1939 de la Fiscalía Europea y que contiene reglas concretas respecto a la protección de datos en su Capítulo VIII. La Fiscalía europea, a diferencia de Eurojust que solo auxilia a las autoridades en procedimientos nacionales y por tanto que no son responsabilidad de la agencia, tendrá sus propias investigaciones y tratará directamente datos propios obtenidos en sus propias investigaciones.

Hay que matizar también y tener en cuenta además no solo el órgano actuante, se trate de un policía o un juez o un fiscal, si no el tipo de actividad que se lleva a cabo, puesto que estas autoridades pueden tratar datos personales con fines distintos de los concretos referidos en la Directiva, por ejemplo, cuando las actividades no vayan dirigidas a la investigación, enjuiciamiento o ejecución de sanciones, sino que se refieran a medidas de organización interna, relaciones institucionales, etc. En estos casos será de aplicación el régimen general establecido por el Reglamento general de protección de datos y no el de la Directiva.

Por otro lado, también hay otras normas relevantes referidas a la protección de datos para los sistemas comunes de información de la UE para el intercambio transfronterizo entre las autoridades policiales y judiciales. Entre ellos destaca el Sistema de Información de Schengen II o el sistema de información de Visados y EURODAC que recopila los datos de impresiones dactilares de nacionales de terceros países que solicitan asilo en la UE.

El objeto de este análisis no se centrará en las normas concretas de estos órganos y agencias europeas del ámbito judicial o policial o las referentes a los sistemas de información, sino que se abordarán las condiciones y limitaciones que impone la Directiva para el intercambio de datos en el ámbito de la cooperación judicial penal en relación con

terceros Estados. En todo caso conviene no olvidar todo este entramado que conforma un completo sistema de garantías y que implica limitaciones y obligaciones muy amplias y exigentes para las autoridades del ámbito general de la investigación penal en el ejercicio de las tareas de tratamiento de datos.

4. PRINCIPIOS BÁSICOS DE LA PROTECCIÓN DE DATOS EN LA DIRECTIVA 2016/680

La Directiva 2016/680 establece unos estándares comunes mínimos para los Estados miembros en cuanto al tratamiento de los datos obtenidos y gestionados para, y dentro, del proceso penal, entendido este en un sentido extenso y que comprende desde las actividades de prevención a las más iniciales de investigación, instrucción y enjuiciamiento. También engloba las actividades de ejecución de las decisiones judiciales y el cumplimiento de las penas y medidas impuestas en la resolución que pone fin al proceso.

Como se decía, los intereses que se sustancian en el proceso penal exigen un tratamiento equilibrado entre los fines legítimos de la investigación y los derechos de las personas físicas en relación con sus datos. Uno de los aspectos más relevantes es el incremento de los mecanismos de control y las obligaciones creadas para las instituciones y autoridades como responsables del tratamiento de estos datos. Unas obligaciones que cobran especial entidad cuando se trata de trasladar datos fuera de la UE, aun cuando se utilicen los mecanismos autorizados y previstos en los Tratados para regular la cooperación judicial internacional.

La Directiva 2016/680 lleva a cabo una tarea de armonización de las garantías referentes al tratamiento de datos en todos los países de la UE, lo que conduce a que el traslado de estos datos entre los Estados miembros se facilite extraordinariamente. La confianza de que todos los países respetan esas garantías mínimas en el tratamiento de los datos

que se solicitan y trasladan a través de los mecanismos de cooperación internacional y reconocimiento mutuo permite que la entrega y transmisión de esos datos se realice sin necesidad de realizar ulteriores comprobaciones sobre el destino y uso de esos datos.

Aunque estos principios básicos se inspiran en el Reglamento General de Protección de datos, como se apuntaba arriba, la naturaleza especifica de autoridades policiales y judiciales modifica algunas cuestiones, de forma que, en comparación con el tratamiento de datos con fines comerciales, regulado por el Reglamento, el tratamiento en el procedimiento penal permite una comprensión menos rígida en relación con algunos principios. Por ello, por ejemplo, la Directiva no impone el principio de transparencia ya que la confidencialidad del proceso penal y sus objetivos no pueden concebir un acceso incondicionado de los interesados a conocer el manejo de sus datos en el proceso. Igualmente teniendo en cuenta los fines del procedimiento penal no puede exigirse de forma absoluta el principio de minimización de datos.

Para comprender la exigencias y garantías en el tratamiento de datos, es importante recordar cuales son los principios y obligaciones que para el tratamiento de datos establece la Directiva y que son, en esencia, los mismos principios y garantías aplicables en la normativa general de la UE a otras actividades reguladas en el derecho de la Unión Europea aun, como se mencionaba, con matizaciones.

Muy resumidamente se exponen algunos de estos principios:

• *Licitud del tratamiento*

El art. 8 de la Directiva recuerda la necesidad de asegurar la licitud del tratamiento, los datos deben ser exclusivamente tratados para los objetivos establecidos en la Directiva, es decir para la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales, o, en general, por motivos vinculados a la seguridad pública.

• *Control de la fiabilidad de los datos*

El art. 7 de la Directiva se establece una obligación de controlar la calidad y fiabilidad de los datos personales objeto de tratamiento. De esta forma, se aconseja no remitir a terceros datos inexactos o incompletos y, en su caso, se obliga a remitir junto a los datos toda la información sobre las circunstancias que afecten a esos datos para que permitan a la autoridad receptora valorar el carácter exacto, completo y fiable de los datos en cuestión.

• *Derechos de los interesados*

Al igual que en el Reglamento, la Directiva reconoce los clásicos derechos de los interesados en relación a sus datos en los arts. 12 a 18. Resumidamente son: derechos de acceso, rectificación, supresión y protección a través de la autoridad de control. Los derechos de los interesados en relación con los datos tratados en el transcurso de una investigación penal podrán ejercerse de conformidad con el Derecho procesal nacional.

• *Diferencia de tratamiento de los datos de los diferentes intervinientes en el proceso*

Lo primero que hay que señalar es que en el art. 6 de la Directiva se exige un tratamiento diferenciado de los datos personales de las diferentes categorías de afectados en el proceso, atendiendo a la razón y naturaleza de su intervención en el mismo. De esta forma se distingue entre: sospechosos, condenados, víctimas o posibles víctimas, testigos de la comisión de una infracción penal o personas asociadas a sospechosos o acusados.

• *Tratamiento especial de datos sensibles*

Se exige un tratamiento especial para datos especialmente sensibles que son aquellos a los que el art. 10 de la Directiva se refiere como "*categorías*

especiales de datos" entre los que se menciona al origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, datos de naturaleza genética o biométrica y datos de salud o vida sexual. El tratamiento de estos datos sólo será posible cuando esté autorizado por el derecho de la Unión Europea o de un Estado miembro y sea preciso para proteger los intereses vitales del afectado, o el propio interesado los haya hecho públicos de forma manifiesta.

• *Nombramiento de delegados de protección de datos*

Las instituciones responsables del tratamiento están obligadas a la adopción de políticas internas dirigidas a asegurar medidas organizativas oportunas y eficaces para asegurar el tratamiento adecuado de los datos. Con el objeto de favorecer el cumplimiento, el responsable del tratamiento designará a una persona con conocimientos especializados como delegado de protección de datos. Este delegado debe asesorar y prestar ayuda al responsable y a los encargados del tratamiento. Los órganos judiciales y demás autoridades independientes pueden ser eximidas del nombramiento de este delegado cuando actúen en su función jurisdiccional.

• *Autoridad de control independiente*

El establecimiento de mecanismos de supervisión del sistema exige la creación de autoridades de control con plena independencia.

5. PROTECCIÓN DE DATOS Y ASISTENCIA JUDICIAL PENAL EN LA UE

El concepto de actividad de cooperación judicial internacional penal, entendido en sentido amplio, abarca toda actividad procesal por la que se solicita y obtiene colaboración de las autoridades judiciales de otros Estados miembros para la práctica de diligencias, obtención de pruebas, ejecución de resoluciones, entrega de sujetos procesales, siempre

a los efectos de un procedimiento penal implica muy frecuentemente el traslado trasnacional de datos.

Dicha actividad comprende tanto la actividad tradicional de cooperación internacional a través de las comisiones rogatorias, como el reconocimiento mutuo dentro de la UE y también la obtención de datos a través de sistemas comunes de información como el ECRIS, el SIS, PRÜM que se basan precisamente en la obtención y almacenamiento e intercambio de datos específicos.

Sin duda, si hay una actividad a la que afecta la protección de datos, es precisamente la cooperación internacional que mayoritariamente consiste en la transferencia de datos personales de la autoridad de un país a otro. Una actividad plenamente legitima y de interés puesto que ese traslado de datos es imprescindible para la lucha contra la delincuencia y especialmente la más grave que es la criminalidad transnacional y organizada. Por ello, la mayoría de los Convenios de asistencia judicial más recientes o las normas de reconocimiento mutuo de los últimos años tienen preceptos dirigidos concretamente a la protección de datos.

Sin embargo, la aplicación de Convenios de fechas anteriores que, como es obvio, no tienen normas específicas de protección de datos, deben aplicarse también conforme a la nueva normativa que afecta a toda la actividad de cooperación internacional en los Estados miembros de la UE. Es importante tener en cuenta que el art. 61 de la Directiva hace una especial salvaguarda a los Convenios anteriores al 6 de mayo de 2016. Es una salvaguarda que no se refiere obviamente a los Convenios entre países de la UE.

Algunos Convenios de la UE aun anteriores a 2016 hacían ya mención a la protección de datos el Convenio de Asistencia Judicial Penal entre los países miembros de la UE de 29 de mayo de 2000 –en adelante Convenio 2000– en su art. 23 recogía ya reglas concretas.

Las normas de reconocimiento mutuo y concretamente la Directiva 41/2014 sobre la Orden de Investigación Europea –en adelante OEI–,

que viene a sustituir al Convenio 2000 en lo relativo a la práctica de diligencias y obtención de información y pruebas a través de la asistencia internacional, con la introducción en esta materia del principio de reconocimiento mutuo, contiene también una norma específica dedicada a la protección de datos y al principio de especialidad que se menciona más adelante y que impide también en la cooperación dentro de la UE la ulterior transmisión de datos transmitidos, sin el consentimiento expreso y previo de la autoridad que remitió originariamente esos datos.

6. LA PROTECCIÓN DE DATOS EN LAS ACTIVIDADES DE COOPERACIÓN JUDICIAL CON TERCEROS PAÍSES Y ORGANIZACIONES INTERNACIONALES

La necesidad de asistencia mutua internacional no finaliza en las fronteras de la UE, sino que los Estados miembros requieren la colaboración de autoridades judiciales de países que no son miembros de la UE y estas autoridades no europeas a su vez también solicitan cooperación y requieren el envío de datos e informaciones a los Estados miembros a través de los mecanismos de cooperación internacional.

Habida cuenta de que estos terceros Estados no están vinculados por las normas de protección de datos aprobadas por la UE, no existe, *a priori*, la seguridad y confianza en la adecuación de las garantías con que en estos países se tratan estos datos. La ausencia de normas internacionales que armonicen esas garantías y por tanto la situación de desconocimiento del sistema de protección de los terceros Estados puede generar desconfianza en relación con las actividades de cooperación que impliquen el traslado de datos. La Directiva 2018/680 ha decidido establecer unas condiciones generales para poder llevar a cabo esas transferencias de datos a terceros. Son condiciones que deben ser comprobadas –exista o no en la práctica esa desconfianza concreta–

para que las autoridades puedan transmitir datos en las actividades de cooperación judicial internacional.

Con el fin de garantizar la concurrencia de esos estándares mínimos en el tratamiento de los datos por parte de estos Estados no miembros de la UE con los que se plantea una actividad de cooperación judicial internacional, la Directiva 2018/680 plantea tres escenarios alternativos que deben concurrir para asegurar la existencia de un tratamiento de datos adecuado que permita que el acto de cooperación y transmisión de datos se puede llevar a cabo. Se trata de asegurar que en el acto de asistencia judicial internacional concreto se tomen en el tercer Estado afectado una serie de precauciones dirigidas a garantizar la debida protección de esos datos.

El tema es sin duda uno de los más relevantes de los que aborda la Directiva 2018/680 y por ello recibe un tratamiento específico en el Capítulo V. En este Capítulo, la Directiva plantea los tres distintos escenarios en los que debe encontrarse el tercer Estado para que pueda llevar a cabo el traslado de datos que se requiere en la solicitud de cooperación.

Es importante tener en cuenta que, aunque la Directiva lo plantea principalmente desde el punto de vista pasivo, es decir, establece las condiciones que las autoridades competentes de los Estados miembros deben exigir para poder transmitir datos a las autoridades del país requirente, la exigencia se da también desde el punto de vista activo, cuando se demandan datos de uno de esos terceros países a un Estado miembro. Podría suceder que la autoridad competente del Estado requerido no haya tenido en cuenta las condiciones de respeto en el tratamiento y traslado de datos lo que podría dar lugar a invalidar su uso en el proceso penal en el que fueron solicitados y obtenidos.

En todo caso, cualquiera que sea el estándar de protección de datos del tercer país, los presupuestos para que se pueda proceder a la transmisión de datos personales son en primer lugar que se trate de un acto de cooperación judicial internacional en el ámbito penal en el que se

requieran práctica de diligencias y conocimiento de datos que obren en otro país.

Los presupuestos de la actividad son los siguientes, tal y como están descritos en el art. 35 de la Directiva 2018/680:

1. Que la transferencia sea necesaria en relación con los fines establecidos en el art. 1.1 de la Directiva. El art. 1.1 define el ámbito de la Directiva, es decir que se trata de una actividad dentro del procedimiento penal, desde un acto de prevención o investigación al enjuiciamiento o la ejecución de la sanción.
2. Que la transferencia de datos se realice solo entre autoridades competentes a los fines de la Directiva.
3. Que se dé la garantía de que el tercer Estado al que pertenece la autoridad judicial concernida se encuentre en alguno de los tres supuestos que posteriormente se describen.
4. Respeto al principio de especialidad.

6.1 ÁMBITO DE ACTUACIÓN DE UN PROCEDIMIENTO PENAL

Para concretar estos principios es bueno tener presente que el considerando 64 de la Directiva empieza exigiendo que el traslado de datos se produzca siempre efectivamente en una actividad relativa al ámbito penal y se realice cuando el responsable del tratamiento (es decir la autoridad receptora) sea una autoridad competente en el sentido definido en esta Directiva.

Hay que tener en cuenta que, aunque se incluyen actividades de prevención, el punto central de la definición es la investigación y el proceso penal. La definición y el concepto de procedimiento penal en la UE ha sido abordado por el TJUE y no permite, por ejemplo, incluir algunos procedimientos sancionadores en el ámbito administrativo.

El TJUE ha interpretado el concepto de sanción penal en casos como Bonda, C489/10 y Franssen asunto C617/10, siguiendo la ya clásica triple condición exigida por el TEDH en la Sentencia Engel[10] cuyos requisitos son: la calificación jurídica de la infracción en Derecho interno, el segundo la propia naturaleza de la infracción y el tercero la naturaleza y gravedad de la sanción que puede imponerse al interesado. El procedimiento penal se vincula al concepto de sanción penal como consecuencia final del proceso.

6.2 AUTORIDADES COMPETENTES

Las autoridades competentes se describen en el art. 3.7 de la Directiva 2018/680. El considerando 11 de la Directiva aclara que en el concepto de autoridad competente deben incluirse no solo autoridades públicas como las autoridades judiciales, la policía u otras fuerzas y cuerpos de seguridad sino también cualquier otro organismo o entidad a la que el derecho del Estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas a los efectos de la presente Directiva.

Este concepto de autoridad competente a los efectos del traslado de datos se impone también a los terceros Estados, de forma que los demandantes y destinatarios de estos datos deben ser esencialmente autoridades policiales o judiciales o aquellas otras que tengan encomendando el ejercicio de competencias públicas relacionadas con las actividades del procedimiento penal.

El concepto de autoridades policiales y cuerpos de seguridad cuando actúen en actuaciones de investigación o prevención por si mismos o por cuenta y delegados por la autoridad judicial se define por cada

10 TEDH, sentencias Engel y otros c. Países Bajos de 8 de junio de 1976.

Estado que les otorga esas competencias, pero debe atenderse también al concepto de autoridad judicial en la UE.

Pero el concepto da autoridad judicial, incluyendo al Ministerio Fiscal, es un concepto definido en el derecho europeo. Efectivamente el TJUE ha establecido que el concepto de autoridad judicial es un concepto autónomo del derecho europeo que comprende no solo a Jueces y Tribunales sino a otros órganos, como el Ministerio Fiscal, que participan con un grado suficiente de independencia en las tareas de la Administración de Justicia[11]. Así lo afirma en las Sentencias de los Asuntos Poltorak C-452/16 y Kovalkovas C-453, de 10 de noviembre de 2016. En estas sentencias el Tribunal aclara que para que una autoridad entre dentro del concepto europeo de autoridad judicial no es suficiente con que se trate de un órgano que participe en la Administración de Justicia sino que además tiene que tener un *grado suficiente de autonomía* que lo vincule de alguna forma al poder judicial que, conforme al principio de separación de poderes, que determinan el Estado de Derecho, se distingue del poder ejecutivo, en el que están incluidos otras autoridades administrativas o los servicios de policía.

Es decir que las autoridades competentes a las que se refiere la directiva son autoridades esencialmente policiales y judiciales, comprendido el Ministerio Público y aquellos organismos o entidad en que el Derecho del Estado miembro haya confiado el ejercicio de la autoridad y las competencias públicas a los efectos de las actividades penales comprendidas en el ámbito de la presente Directiva.

---

11 Vide Requejo Pagés, Juan Luis. Jurisprudencia del Tribunal de Justicia sobre cooperación penal: Orden de Detención Europea (ODE) y concepto de autoridad judicial. Ponencia impartida en las Jornadas de Fiscales especialistas de Cooperación Internacional en Oviedo 3 y 4 de marzo 2019. Publicación en versión *on-line* el Centro de Estudios Jurídicos (CEJ).

Entre las autoridades a quienes se ha confiado competencias en este sentido podrían comprenderse las autoridades centrales de naturaleza administrativa y no judicial, como los Ministerios de Justicia que siguen en muchos países ejerciendo el rol de autoridad central. Ello obliga al Ministerio de Justicia a cumplir estrictamente con las garantías de tratamiento exigidas en esta Directiva. Sin duda los principios de adecuación y minimización de datos deberían ser tenidos en cuenta para modificar las designaciones de autoridades centrales en autoridades que no participan en modo alguno en la investigación y que deberían estar excluidas de estos procesos evitando un paso burocrático más de uno datos que, sin duda, corren un riesgo extra e incensario al ser puesto en conocimiento de una nueva autoridad cuya intervención no es imprescindible.

6.3 ESCENARIO DE GARANTÍAS QUE DEBEN CONCURRIR EN EL TERCER ESTADO

La Directiva 2018/680 proporciona tres alternativas de forma escalonada, que son tres distintas formas de comprobar la suficiencia de las garantías del tratamiento de datos en el país u organización internacional con la que se va a cooperar y a la que se van a solicitar o transferir los datos.

Parten las opciones del escenario de mayor seguridad para la actividad de cooperación, basado en una *decisión de adecuación* de las condiciones del país; se trata de una decisión expresa de adecuación de la Comisión tras una evaluación por la UE de las condiciones de un determinado país tercero. La decisión de adecuación es además específica a los efectos de esta Directiva, de forma que no es automáticamente aplicable la decisión de adecuación que se haya realizado respecto a ese país a efectos del Reglamento general.

Se plantea un segundo escenario basado en la valoración y la com-

probación de la existencia de unas *garantías adecuadas* realizada por el responsable de tratamiento en el caso concreto.

Finaliza los supuestos con una tercera posibilidad de que, incluso en ausencia de una decisión general de adecuación o la imposibilidad de comprobación de las garantías adecuadas o cuando estas claramente no concurren, se puedan autorizar *excepciones para situaciones específicas* en atención a que la cooperación tenga unos fines concretos, que la Directiva enuncia y describe de forma tan amplia que en la práctica puede permitir la cooperación para los fines recogidos en el amplio ámbito de la directiva.

Lo cierto es que la forma de concretar estas evaluaciones de los estándares exigidos para el tratamiento de datos no será fácil ni pacifica, ni parece que se esté siendo lo suficientemente ágil por parte de la Comisión Europea que, aunque ya trabaja con varios países para la posible declaración de adecuación, aún no ha concretado ninguna a los efectos de esta Directiva.

La UE plantea unas exigencias de forma unilateral a terceros Estados para llevar a cabo unos actos de cooperación judicial internacional que vienen realizándose durante años sin necesidad de comprobación de estos requisitos; actos de asistencia mutua basados en convenios bilaterales y multilaterales de los que derivan compromisos internacionales y que en su articulado no contemplan por el tiempo en que fueron acordados y ratificados el escenario de estas nuevas exigencias.

Por eso, es importante tener en cuenta que la Directiva tendrá especial incidencia en el futuro mientras que de alguna forma santifica el *statu quo* en relación con los Convenios vigentes. Efectivamente, el art. 61 de la Directiva establece que

> Los acuerdos internacionales que impliquen la transferencia de datos personales a terceros países u organizaciones internacionales que hubieren sido celebrados por los Estados miembros antes del 6 de mayo de 2016 y que cumplan lo dispuesto en el Derecho de la Unión aplicable

> antes de dicha fecha seguirán en vigor hasta que sean modificados, sustituidos o revocados.

Por tanto, los acuerdos internacionales celebrados por los Estados miembros con terceros estados antes del 6 de mayo de 2016 mantienen su completa aplicación y permiten la transferencia de datos personales, aunque exigen que cumplan el derecho de la UE aplicable en la fecha en que fueron firmados.

La Directiva con esta excepción viene a reconocer la imposibilidad de irrumpir en las relaciones de cooperación judicial bilaterales de los Estados miembros con terceros países con los que tienen firmados convenios bilaterales, o incluso multilaterales en el seno de NNUU, CoE, OCDE, etc. y mantiene su completa vigencia lo que, de alguna forma, puede resultar incongruente. El art. 61 de la Directiva 2018/680 permite por el momento trabajar a las autoridades competentes sin hacer en este momento ulteriores comprobaciones, pero sin duda impone una mayor cautela en la forma de transmisión de los datos, no debe olvidarse que se trata de un derecho fundamental de los ciudadanos.

Las consecuencias de un rígido cumplimiento de estas condiciones, aunque se proyectan principalmente en el futuro pueden ser ya visibles especialmente en relación con actividades de cooperación informal y el intercambio de datos sin la existencia o al margen de los convenios internacionales de cooperación judicial en materia penal.

En ausencia de convenio aplicable y, a la hora de realizar una actividad de cooperación judicial penal fundamentada en la reciprocidad, corresponderá a la autoridad competente para la demanda o ejecución de la solicitud de auxilio, como autoridad responsable o encargada de la protección de datos realizar las valoraciones para la comprobación de la existencia de alguno de los tres escenarios.

En todo caso, para comprender mejor la nueva situación en la que la Directiva sitúa a la cooperación internacional es necesario examinar

las condiciones y esas tres posibilidades abiertas para que se pueda llevar a cabo el traslado de datos, a través de las comisiones rogatorias y otros mecanismos de cooperación internacional, a terceros Estados.

6.3.1 PRIMER ESCENARIO: TRANSFERENCIAS BASADAS EN UNA DECISIÓN DE ADECUACIÓN

El art. 36 de la Directiva 2018/680 establece el mejor escenario que ofrecerá la mayor amplitud para la transferencia de datos, se trata del caso en que el tercer país o la organización internacional hayan sido objeto de una declaración especifica de la Comisión Europea por la que se garantiza que el nivel de protección de datos de ese país u organización es adecuado.

Se trata de que la Comisión haya realizado un estudio, supervisión y valoración de las condiciones de tratamiento de datos en el país u organización afectados y considera que alcanzan el nivel exigido por la UE.

La valoración que la Comisión debe llevar a cabo, conforme al art. 36 de la Directiva, va mucho más allá de un examen centrado en el sistema de tratamiento de datos y entra a valorar parámetros como: el Estado de derecho, el respecto a los derechos y libertades fundamentales tanto en general como sectorial, incluidas la seguridad pública, la defensa y seguridad nacional, el Derecho penal. Por supuesto también las normas de protección de datos, incluida la jurisprudencia y especialmente la existencia en el país de posibles recursos de los afectados. Realmente este ejercicio de valoración que se propone en la Directiva enfrenta a los Estados no miembros de la UE importantes retos a la hora alcanzar un sistema de protección equivalente al de la UE, un ejercicio que sin duda redundará en beneficios para los ciudadanos pero que va a suponer largas y complicadas negociaciones con la UE.

El considerando 68 de la Directiva 2018/680 se refiere a los factores a tener en cuenta para llegar a esta declaración de adecuación. Entre

estos se valora expresamente la participación del país en sistemas multilaterales o regionales, en particular en relación con la protección de datos, y especialmente valora la adhesión del país al Convenio del CoE de 28 de enero de 1981 para la protección de las personas con respecto al tratamiento automatizado de datos personales y su Protocolo adicional. Se prevé que la Comisión consulte al Comité Europeo de Protección de datos y propone tener en cuenta las declaraciones de adecuación adoptadas de conformidad con el art 45 del Reglamento 2016/679[12].

Sobre el exigente concepto de nivel adecuado, al menos en relación con el Reglamento es importante conocer los recientes fallos del TJUE. La sentencia del TJUE, de 6 de octubre de 2015, en el asunto C-362/14, caso *Screms* 1[13], dice que hay que atender a que

> es el ordenamiento jurídico del tercer país al que se refiere la decisión de la Comisión el que debe garantizar un nivel de protección adecuado. Aunque los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas

12 La Comisión Europea ha adoptado decisiones de adecuación en relación con el Reglamento de los siguientes países: Andorra, Argentina, Canadá, EEUU (limitado al marco de *Privacy Shield*) Guernsey, Isla de Man, Islas Feroe, Israel, Japón, Jersey, Nueva Zelanda, Suiza y Uruguay. Actualmente, también se están manteniendo conversaciones de adecuación con Corea del Sur. Se trata de adecuación en relación con las actividades comerciales a las que se refiere el Reglamento y no a efectos de la Directiva para cuya aplicación aún no se ha hecho ninguna declaración de adecuación.

13 La STJUE C-362/14, de 6 de octubre de 2015, en el Asunto *Schrems I* anuló la Decisión 2000/ 520, de 26 de julio (Decisión de Puerto Seguro), por la que se había declarado que EEUU ofrecía un nivel adecuado de protección. Recientemente el TJUE en una nueva Sentencia de 16 de julio de 2020 *Asunto Schrems II* vuelve a anular la declaración de adecuación de la protección conferida por el escudo de privacidad de UE-EUU que había sido adoptada por la Decisión 2016/1250.

> de esa Directiva entendida a la luz de la Carta, deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión (apartado 74).

El nivel adecuado, exigido a un tercer país u organización internacional, en los términos previstos en el Reglamento (UE) 2016/679, significa *un nivel equivalente al de la UE* y así lo expresa el TJUE en esta sentencia, que mantiene que ello

> exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta (apartado 73).[14]

Las exigencias de la UE para estas declaraciones sin duda no son fáciles de cumplir. Una de las condiciones más relevantes para la declaración de adecuación es el aseguramiento de la tutela judicial efectiva y los derechos de los particulares al recurso a mecanismos efectivos de protección con la existencia de autoridades de control independiente de protección datos en el país o en la organización internacional. Así,

14 El Comité Europeo de protección de datos (EDPB) ha adoptado el 18 de enero de 2020 un documento que contiene las orientaciones 2/2020 para realizar las declaraciones de adecuación en relación con Reglamento 2016/679. Aunque se refieren al Reglamento y no a la Directiva sin duda son orientaciones de utilidad no solo para la declaración de adecuación en relación con la Directiva sino para las valoraciones que los responsables de tratamiento deban hacer para decidir la transferencia de unos datos. Disponible en esta dirección: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_es.

la sentencia C-311/18, de 16 de julio de 2020, en el *Asunto Schrems II* vuelve a anular la declaración de adecuación de la protección conferida por el escudo de privacidad de UE-EUU (en relación con el Reglamento y no con la Directiva) que había sido adoptada por la Decisión 2016/1250 y lo hace particularmente por la ausencia de tutela judicial efectiva. Considera el Tribunal de Luxemburgo que la tutela que supone la posibilidad de recurso ante el defensor del Pueblo en los EEUU no proporciona a los titulares de los datos un recurso ante un órgano que ofrezca garantías sustancialmente equivalentes a las exigidas en el Derecho de la Unión que puedan asegurar tanto la independencia del Defensor del Pueblo como las potestades de éste para adoptar decisiones vinculantes con respecto a los servicios de inteligencia estadounidenses.

Además, la obtención de la declaración de adecuación no es permanente y el considerando 69 de la Directiva impone también la necesidad de un seguimiento y vigilancia periódicas de las condiciones de los países que hayan obtenido la declaración de adecuación y permite en cualquier momento en que se dejan de dar las condiciones adecuadas declarar que un país o un sector concreto del mismo ha dejado de cumplir las condiciones de adecuación.

6.3.2 TRANSFERENCIA BASADA EN GARANTÍAS ADECUADAS

En caso de que no exista una decisión formal de adecuación del país concreto, que es la situación actual en la que aún no se ha realizado aún ninguna declaración de adecuación por parte de la Comisión, el segundo escenario en el que se puede consentir el traslado de datos a través de los mecanismos de cooperación requiere la constatación por parte del responsable de la existencia de garantías adecuadas.

El art. 37 de la Directiva 2018/680 se refiere a las condiciones para

las transferencias en este caso de existencia de garantías adecuadas. Estas garantías adecuadas se pueden constatar de dos formas:

1. El art.37.1b se refiere a cuando esas garantías en un instrumento jurídicamente vinculante. El considerando 72 no aclara a qué tipo de instrumento jurídicamente vinculante se refiere, pero menciona los acuerdos bilaterales entre los Estados, de forma que se garantice el cumplimiento de los requisitos de protección de datos y el respeto a los derechos de los interesados entre los que se incluye el derecho a la tutela administrativa o tutela judicial efectiva. También deben ser tomados en cuenta las cláusulas de confidencialidad y el principio de especialidad previstos en los Convenios bilaterales. Igualmente se mencionan las normas internas para la protección de datos, derechos de los interesados en relación con sus datos y recursos efectivos. Especial interés tiene, como ya se mencionaba la existencia en el tercer país de agencias de protección de datos y autoridades de control independientes.
2. El segundo supuesto es que el responsable de tratamiento considere, tras evaluar las circunstancias que concurren en el Estado concreto, que concurren las garantías apropiadas para la protección de esos datos. En este supuesto, el considerando 71 hace mención a que el responsable del tratamiento tenga en cuenta los acuerdos que ese tercer Estado pueda tener con Eurojust[15] o Europol[16] como factores para valorar la adecuación de ese tratamiento.

---

15 Los Estados que en este momento tienen acuerdo con Eurojust son: Islandia, Noruega, USA, Suiza, Macedonia, Liechtenstein, Moldavia, Ucrania, Montenegro, Albania, Georgia, Serbia y Dinamarca.

16 Europol tienen acuerdos de distinto tipo, en el ámbito regional que nos ocupa cuenta con un acuerdo operativo con Colombia y uno estratégico con Brasil.

Un problema añadido de estas valoraciones concretas e individuales es que cada responsable de tratamiento puede valorar de forma diferente las garantías concurrentes en cada país.

6.3.3 EXCEPCIONES PARA SITUACIONES ESPECIFICAS

La tercera situación en que se pueden llevar a cabo las transferencias de datos se recoge en el art. 38 de la Directiva 2018/680 y se refiere a situaciones especificas. Esta última vía para permitir el traslado supone una valoración caso a caso que podrá darse siempre que se de alguno de los fines que se mencionan en el propio articulo y que son:

a) Para proteger los intereses vitales del interesado u otra persona;
b) Para salvaguardar intereses legitimo del interesado;
c) Para prevenir una amenaza grave e inmediata para la seguridad pública de un Estado miembro o de otro país;
d) En casos individuales a efectos del art. 1 apartado 1, o sea para los fines generales del proceso penal a los que se refiere la Directiva en el sentido más amplio.

En todo caso, se impone una valoración de la autoridad competente para la transferencia sobre todas las condiciones y garantías del Estado en relación con el tratamiento de datos y también atender a la prioridad de los derechos y libertades fundamentales del interesado y su prevalencia sobre el interés público.

6.4 PRINCIPIO DE ESPECIALIDAD Y TRASLADO DE DATOS

El principio de especialidad en relación con la transmisión de datos se contiene en el art. 35 de la Directiva 16/680 que establece que

> cuando se trate de una transferencia ulterior a otro tercer país u organización internacional, la autoridad competente que haya efectuado la transferencia inicial u otra autoridad competente del mismo Estado miembro autorice la transferencia ulterior, una vez considerados debidamente todos los factores pertinentes, entre estos la gravedad de la infracción penal, la finalidad para la que se transfirieron inicialmente los datos personales y el nivel de protección de los datos personales existente en tercer país u organización internacional a los que se transfieran ulteriormente los datos personales.

El principio de especialidad es un principio clásico de la cooperación internacional que nace en relación con la extradición y que supone la imposibilidad de la persecución o enjuiciamiento de la persona entregada en virtud de una extradición por hechos distintos y anteriores a los que hubieran provocado la entrega. En la asistencia judicial, este principio puede tener un mayor o menor alcance y supone que la información solicitada a través de una demanda de auxilio judicial se entrega exclusivamente para el procedimiento en la que fue emitida y se concede solo y exclusivamente en relación a una petición concreta. El posible uso de esta información o datos en otros procedimientos exige el expreso consentimiento de la autoridad que los transmitió. La mayor o menor exigencia de este principio depende de las disposiciones de los Convenios aplicables y también en muchos casos de las declaraciones y reservas que el Estado haya realizado al ratificar el Convenio de que se trate.

Como ejemplo, el art. 23 del Convenio 2000 en la UE contiene una

regulación muy precisa, pero también muy amplia y generosa en la admisión del uso de datos en otros procesos:

> 1. Los datos de carácter personal comunicados con arreglo al presente Convenio podrán ser utilizados por el Estado miembro al que se hayan transmitido:
>
> a) para los procedimientos a los que se aplica el presente Convenio;
>
> b) para otros procedimientos judiciales y administrativos directamente relacionados con los procedimientos a que se refiere la letra *a*);
>
> c) para prevenir una amenaza inmediata y grave para la seguridad pública;
>
> d) para cualquier otra finalidad, únicamente previa autorización del Estado miembro transmisor, a menos que el Estado miembro de que se trate haya obtenido el consentimiento de la persona interesada.

La Directiva 14/41 sobre la Orden europea de investigación, en su art. 20, remite a los principios del Convenio 108 del CoE y a la regulación europea de protección de datos, por lo que se admite el uso de datos en diferentes procedimientos penales del Estado receptor, pero, sin embargo, se limita el traslado ulterior a terceros Estados.

Es importante tener en cuenta que el principio de especialidad tiene un fundamento jurídico diferente a la limitación del uso de datos personales transferidos. El principio de especialidad busca asegurarse la soberanía y el control de los datos por el país que los transmite y alcanza a informaciones que no tengan que ver con datos personales. Mientras las limitaciones en los traslados de datos personales tratan de la protección de un derecho fundamental individual garantizando un adecuado uso de los datos transmitidos.

En todo caso, el principio de especialidad en el tratamiento de datos personales, tal y como se plasma en la Directiva 2016/680, exige que toda transferencia trasnacional ulterior de datos personales este

supeditada a la autorización previa de la autoridad que llevo a cabo la transferencia inicial.

Deben tenerse en cuenta también que habitualmente existen otras limitaciones a transferencias a distintas autoridades dentro del propio Estado receptor o incluso al uso de datos por la misma autoridad en un procedimiento distinto de aquel en el que se solicitaron que están impuestas por las normas internas, los Convenios internacionales en los que se basó la ejecución de la solicitud o incluso en condiciones expresas impuestas legalmente y en el caso particular por la autoridad de ejecución.

7. CONCLUSIÓN

El nuevo marco jurídico de protección de datos de la UE, en cuanto se proyecta sobre terceros Estados a los que exige determinadas condiciones para poder transmitir datos en materia de cooperación internacional, tiene un indudable potencial efecto transformador de las normas y procedimientos sobre tratamiento de datos de eso terceros Estados. Se trata de un impulso exterior que desencadena un proceso de mejoras que traerá enormes beneficios a los ciudadanos en relación con la mejor protección de sus datos personales.

Este impulso transformador, que se une a un conjunto de iniciativas legislativas para la regulación de la protección de datos, que ya se vienen tramitando en muchos países fuera de la UE, no se dirige solo al legislador si no que puede ser tenido en cuenta por instituciones públicas como pueden ser las Fiscalías, interesadas en mantener el mayor nivel de cooperación judicial internacional con los Estados miembros de la UE, a la vez que comprometidos a otorgar la mayor protección de los derechos de los ciudadanos en relación con su intimidad y la protección de sus datos personales.

Algunos avances organizativos internos en los Ministerios Públicos como por ejemplo: fortalecer la formación de los fiscales en relación con el tratamiento de datos personales, el establecimiento de sistemas organizativos adecuados en relación con los ficheros con datos personales que manejan o el nombramiento de delegados de protección de datos o incluso la creación dentro de los Ministerios Públicos de una autoridad de control independiente propia y diferente de otras autoridades de control administrativas pueden avanzar en la dirección adecuada y coadyuvar a una mayor facilidad para alcanzar la consideración de la existencia de garantías adecuadas a la hora de recibir datos de un país de la UE.

REFERENCIAS

REQUEJO PAGÉS, Juan Luis. *Jurisprudencia del Tribunal de Justicia sobre cooperación penal*: Orden de Detención Europea (ODE) y concepto de autoridad judicial. Ponencia impartida en las Jornadas de Fiscales especialistas de Cooperación Internacional en Oviedo 3 y 4 de marzo 2019l. Publicación en versión *on-line* el Centro de Estudios Jurídicos (CEJ). Disponible en esta dirección: www.cej-mjusticia.es.

SANCHEZ DOMINGO, Maria Belen. La protección de datos personales en el espacio de libertad, seguridad y justicia: especial consideración a las transferencias de datos a terceros países y organizaciones internacionales según la directiva 2016/680. Universidad de Valladolid. *Revista de estudios europeos*, 2017, n. 69, p. 17-36.

UNIÓN EUROPEA. *Carta de los Derechos Fundamentales de la Unión Europea*, 26 octubre 2012, disponible en esta dirección: https://www.refworld.org.es/docid/5c6c40d04.html. Accesado el: 26 oct. 2020.

UNIÓN EUROPEA. STJUE de 16 de junio de 2003 C-105/03. *Caso*

Pupino. Disponible en esta dirección: http://curia.europa.eu/juris/showPdf.jsf;jsessionid=262796D761E14F002BCDA9E88DDDCF99?docid=64218&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=10970304.

UNIÓN EUROPEA/COE. *Manual de legislación europea en materia de la protección de datos*. Disponible en esta dirección: https://op.europa.eu/es/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1.

A RELEVÂNCIA PENAL DAS *FAKE NEWS* NA CONFIGURAÇÃO DA SOCIEDADE ATUAL: O MÉTODO E OS EFEITOS DA PROPAGAÇÃO DE INFORMAÇÕES FALSAS

Giuseppe Cammilleri Falco[1]
Louise Fernanda de Oliveira Dias[2]
Fernando Andrade Fernandes[3]

RESUMO

A veiculação de informações falsas, hoje chamadas *fake news*, não é fato recente na história. Contudo, a utilização das novas tecnologias de informação, processamento e comunicação, em especial a internet,

1 Mestrando e bacharel (2018) em Direito pela Universidade Estadual Paulista "Júlio de Mesquita Filho" – Unesp, campos de Franca. Advogado e coordenador do Grupo de Estudos Avançados (GEA) de Escolas Penais do IBCCRIM de Ribeirão Preto/SP.

2 Mestranda e bacharela (2019) em Direito pela Universidade Estadual Paulista "Júlio de Mesquita Filho" – Unesp, campos de Franca. Advogada e conciliadora judicial.

3 Pós-doutor em Direito Penal pela Universidade de Salamanca (2011). Doutor em Direito pela Universidade de Coimbra (2000). Mestre em Direito pela Universidade Federal de Minas Gerais (1992). Bacharel em Direito pela Universidade Estadual Paulista "Júlio de Mesquita Filho". Professor assistente doutor da Universidade Estadual Paulista "Júlio de Mesquita Filho".

para propagação das mensagens promoveu uma mudança na percepção do problema, ao qual se atrelam três questões: a proteção de dados; a disseminação das notícias; o conteúdo da informação e seus limites, este atrelado ao direito de liberdade de expressão. Dessa forma, com o uso do método dedutivo, propõe-se precisar qual a conduta deve ser alvo de debate sobre a relevância ou irrelevância penal da veiculação de *fake news*, com a utilização de critérios de política criminal: a dignidade penal e a necessidade de tutela penal.

Palavras-chave: Crime. *Fake news*. Informações falsas. Internet.

ABSTRACT

The transmission of false information, fake news, is not a recent fact in human history. However, the use of new information, processing and communication Technologies, especially the internet, for its spread, promoted a chance in perception of the problem, to which three issues are linked: data protection; the dissemination of news and its content and limits, linked to the right to freedom of expression. Thus, using the deductive method, it is proposed to analyze which action it may be object of the debate about the criminal relevance of the fake news, using criminal policy criteria: criminal dignity and the necessity of the criminal intervention.

Keywords: Crime. Fake news. False information. Internet.

1. INTRODUÇÃO

A veiculação de informações falsas, *fake news*, não é fato recente na história, cuja ocorrência já era registrada em séculos anteriores ao nosso. Contudo, a utilização das novas tecnologias de informação,

processamento e comunicação, em especial a internet, para a propagação de informações formuladas com base em conteúdo desprovido de veracidade, promoveu mudança na percepção do problema, a qual teve em 2018 seu marco histórico.

Diante disso, o objetivo deste trabalho é analisar a relevância penal da conduta de propagação de *fake news*, por meio dos critérios de dignidade penal e a necessidade de intervenção penal, considerando-se os reflexos e influências nele incidentes pela atual configuração da sociedade. Em especial, pretende-se examinar a precisão da conduta, hoje chamada de *fake news* de modo a delimitar o alcance do hoje inflado debate sobre o tema. Essa perspectiva permeará todo o trabalho.

Assim, com a utilização do método dedutivo, parte-se de uma investigação sobre a configuração da sociedade atual; passa-se pela análise histórica da propagação de *fake news* e pela discussão sobre a vinculação do problema com a proteção de dados, a disseminação das notícias, o conteúdo das mensagens e seus limites, este atrelado ao direito de liberdade de expressão; e culmina-se na análise específica da relevância ou da irrelevância penal das condutas de divulgação de informações falsas.

2. A CONFIGURAÇÃO DA SOCIEDADE ATUAL E AS NOVAS TECNOLOGIAS DE INFORMAÇÃO, PROCESSAMENTO E CONFIGURAÇÃO

É de Jakobs (2003, p. 7) a célebre frase: "o Direito Penal constitui um cartão de visitas altamente expressivo" da sociedade. Com esses dizeres, o autor evidencia que o sistema jurídico e, mais especificamente, o sistema jurídico-penal[4] é um "sistema social parcial". Em outras

4 O sistema jurídico-penal é entendido de forma semelhante ao modelo de ciência global do direito penal, introduzido por Franz von Liszt, que compreendia a existência

palavras, o sistema jurídico-penal é parte da sociedade e tem com ela uma relação de dependência recíproca, de tal forma que, ao observar o direito penal, é possível tecer considerações sobre a sociedade na qual ele está inserido. Na mesma medida, ao observar uma sociedade, é possível estabelecer conclusões sobre o direito penal adotado[5].

Nesse sentido, a investigação sobre o problema das *fake news* está inserido em uma sociedade complexa, com forte influência das tecnologias de informação, processamento e comunicação[6], com especial ênfase para o computador[7] e a internet[8].

---

de três ciências conjuntas e autônomas: dogmática jurídico-penal, criminologia e política-criminal, de forma que a dogmática penal seria a "intransponível barreira da política criminal" (LISZT, *apud* ROXIN, 2000, p. 2). Contudo, como bem ressalta Roxin (2000, p. 23), a compreensão do sistema jurídico-penal como fechado "nos afasta da solução de nosso problema, eu já a tentei explicar: ele isola a dogmática, por um lado, das decisões valorativas político-criminais, e por outro, da realidade social, ao invés de abrir-lhes o caminho até elas". Dessa forma, "a partir dessa integração teleológica o abandono da ideia da Ciência Jurídica como um sistema fechado, assumindo, ao invés, uma característica aberta, implicando: enquanto 'sistema científico' (sistema de proposições doutrinárias), a natureza incompleta do conhecimento científico, em virtude da sua abertura a todas as outras Ciências; enquanto 'sistema objetivo' (sistema da ordem jurídica), estando sujeito à mutabilidade dos valores jurídicos fundamentais, em decorrência de ser o Direito um fenómeno situado no processo da história e, por isso, ser mutável" (FERNANDES, 2001, p. 17).

5 "Com efeito, somente um *sentido* de dupla via, de interferência recíproca, pode satisfatoriamente explicar as relações existentes entre modelo de Estado e modelo de direito penal. Ou seja, não é somente em um sentido de mão única, do direito penal para o modelo de Estado, ou vice-versa, que se forma a relação entre ambos, mas sim as implicações são recíprocas." (FERNANDES, 2003, p. 1154)

6 Alguns historiadores, entre eles Manoel Castells (2003; 2016), entendem que ocorreram três Revoluções Industriais no decorrer dos anos. A primeira teve início na Inglaterra, no final do século XVIII, e foi marcada pelo surgimento da máquina a vapor e pela substituição da manufatura por máquinas. A segunda despontou cerca de cem anos depois, nos Estados Unidos e na Alemanha, quando surgiram a

Quanto a esses aspectos, Castells (2016, p. 124) aponta cinco características que compõem o paradigma da tecnologia da informação. Somados, representam o que o autor chama de "base material da sociedade da informação".

Em primeiro lugar, está a informação como matéria-prima em si mesma. Diferentemente das tecnologias criadas no passado, as quais visavam, por exemplo, agilizar o transporte ou incrementar os processos de produção, a revolução atual cria tecnologias próprias para conduzir a informação.

Em segundo lugar, desponta a "penetralidade dos efeitos das novas tecnologias" (CASTELLS, 2016, p. 24). Uma vez que a informação é parte fundamental de todo agir humano e as novas tecnologias têm, como matéria-prima, a própria informação, elas são capazes de adentrar em todos os domínios da atividade humana, no lazer, no trabalho, na intimidade e, até mesmo, na prática de delitos.

Em terceiro lugar, surge a possibilidade de aplicação da "lógica de redes em qualquer sistema ou conjunto de relações, usando essas novas tecnologias da informação" (CASTELLS, 2016, p. 124). A rede, entendida como "nós interconectados" (CASTELLS, 2003, p. 7) é uma estrutura que rompe antigas configurações hierarquizadas e burocratizadas, dirigidas por um centro de comando. Ela é flexível e adaptável,

---

eletricidade e as tecnologias de comunicação. A terceira ocorreu no final do século XX, com as tecnologias em microeletrônica, computação (*software* e *hardware*), telecomunicações/radiodifusão e optoeletrônica.

7 Para os fins deste trabalho, o conceito de computador é o mais amplo possível, abrangendo todos os equipamentos computadorizados, como aparelhos celulares, televisões, relógios etc.

8 O conceito de internet abrange *hardware* e todo tipo de aparato capaz de conectar computadores e informações, seus atores e *personas* utilizados por eles e todas as nuances capazes de formar um verdadeiro meio ambiente digital, o ciberespaço.

podendo espalhar-se facilmente. Por isso, a internet – meio de comunicação que envolve computadores interconectados – é a base tecnológica de uma sociedade que se organiza em rede.

Esse contexto favorece o estabelecimento da quarta característica paradigmática da técnica da informação, a flexibilização; ou seja, a capacidade de adaptação e reconfiguração em um ambiente altamente mutável, como o da modernidade líquida[9]. Por esse mesmo motivo, entretanto, ocorre uma dificuldade na coordenação de funções, na concentração de recursos em metas especificadas e na realização de determinadas tarefas – conforme o tamanho e a complexidade da rede.

A última característica está relacionada à interdependência entre as tecnologias. As tecnologias de comunicação "agora são apenas uma forma de processamento de informação; as tecnologias de transmissão e conexão estão, simultaneamente, cada vez mais diversificadas e integradas na mesma rede operada por computadores" (CASTELLS, 2016, p. 125).

Diante disso, é necessário enfatizar a criação, no ambiente virtual, das chamadas redes sociais. Trata-se de uma estrutura construída com a finalidade de conectar pessoas, por um ou vários tipos de relações – pessoais, laborais e até criminosas –, como, por exemplo, o *Instagram*, o *Facebook*, o *WhatsApp*, o *Telegram* e o *Twitter*, que são, também, relevantes mecanismos de propagação de informação e reforçam a dimensão pública do ambiente virtual.

Essas redes, por utilizarem a internet em sua base, são responsáveis por carregar a informação de um ponto a outro do globo em instantes,

---

9 "O advento do telefone celular serve bem como 'golpe de misericórdia' simbólico na dependência em relação ao espaço: o próprio acesso a um ponto telefônico não é mais necessário para que uma ordem seja dada e cumprida. Não importa mais onde está quem dá a ordem – a diferença entre o 'próximo' e o 'distante', ou entre o espaço selvagem e o civilizado e ordenado, está a ponto de desaparecer." (BAUMAN, 2001, p. 18)

reduzindo as distâncias e massificando a informação. Diferentemente do que ocorre com outros meios de comunicação, como a televisão e o rádio, na internet receptores e emissores se fundem em um mesmo indivíduo.

Nesse sentido, é importante mencionar que o Brasil é o quarto lugar no *ranking* mundial de usuários de internet, segundo o relatório publicado em 2017 pela *United Nations Conference on Trade and Development* (Conferência das Nações Unidas sobre Comércio e Desenvolvimento – Unctad, na sigla em inglês). Portanto, uma quantidade expressiva de brasileiros produz e recebe informações na rede mundial de computadores.

Dada a importância da informação nos dias atuais, no cenário mundial e nacional, bem como da relevância das técnicas de informação, processamento e comunicação, um ponto que se torna patente é o da veiculação de informações falsas, comumente tratada por *fake news*.

3. *FAKE NEWS*, PROBLEMA NOVO OU NOVA FIGURA PARA UM VELHO PROBLEMA?

As chamadas *fake news* podem ser definidas, rapidamente, por sua tradução livre: notícias falsas. Essa definição, entretanto, englobaria diversos sentidos, como, por exemplo, divulgação de dados inverídicos em invólucros ou recipientes (art. 275 do Código Penal), o que não é propriamente o escopo do presente trabalho. Dessa forma, um recorte metodológico se faz necessário. O termo "*fake news"* será usado de forma mais específica, para indicar somente a produção de falsas informações (de cunho jornalístico ou não) acerca de determinados fatos.

Contudo, a pergunta que precisa ser formulada agora é: são as *fake news* uma novidade na sociedade? Se não, qual o motivo de tamanho interesse nesse debate?

O problema da veiculação de informações inverídicas (notícias falsas) não é novo. Exemplo disso foi o fato ocorrido ainda no século XIX, no qual o capitão francês Dreyfus foi acusado publicamente de entregar

documentos secretos do Estado Francês ao Império Alemão. O capitão, após grande alvoroço, provou sua inocência, levando Emilé Zola e Rui Barbosa a dissertarem[10] sobre a necessidade de se debater acerca do problema de notícias falsas.

Não se trata, portanto, de novidade. Todavia, alguns insistem nesse ponto e destacam que o ineditismo está, de fato, na capacidade de se influenciar politicamente a sociedade. Tal argumento não se sustenta, uma vez que, já na década de 1950, o então deputado Carlos Lacerda, opositor do governo, foi a público para acusar o então presidente Getúlio Vargas de ter ordenado seu assassinato, o que nunca foi comprovado. A notícia repercutiu e contribuiu para a grave crise política que culminou no suicídio de Vargas[11]. Tudo isso para dizer que, também na década de cinquenta, as notícias falsas tinham efeitos políticos. Logo, não há nesse ponto também novidade.

O que diferencia as notícias falsas divulgadas no decorrer da história e as atuais *fake news* é, precisamente, o método. A recente metodologia explora dois pontos, que intensificam o conflito entre a liberdade de informação e a vida privada.[12]

---

10 Rui Barbosa faz referência aos relatos da imprensa à época do julgamento, que indicavam a comprovação da culpa do capitão, mas que, depois, com a absolvição de Dreyfus, viu-se que não existiam. Ilustra-se: "Segundo as notícias na imprensa europeia, dentro e fora da França, todo o edifício da acusação assentava em um documento subtraído a uma legação estrangeira. Divulgá-lo seria arriscar, a um tempo, a segurança do país e a honorabilidade da acusação." (ZOLA; BARBOSA, 2008, p. 73)

11 "As investigações policiais sobre o crime e a que Aeronáutica realizou por sua própria conta começaram a revelar os lados sombrios do governo Vargas, embora fosse impossível comprometer pessoalmente o presidente com o que ele próprio chamou de mar de lama. (...) O movimento pela renúncia tomou grandes proporções. (...). Quando o cerco apertou ainda mais, Vargas respondeu com o último e trágico ato. Na manhã de 24 de agosto, suicidou-se em seus aposentos do Palácio do Catete, mas tinha também um profundo significado político." (FAUSTO, 2011, p. 231)

Em primeiro lugar, o modo de produção de informação está hipertrofiado, uma vez que qualquer celular tem potencial técnico para gerar e difundir dados. Além disso, a transmissão das mensagens adquiriu uma velocidade como nunca antes vista. O que preocupa nesse contexto é a capacidade de individualização da dispersão das notícias. Diante da possibilidade de captação de dados inseridos nas redes, as *fake news* puderam ser elaboradas e propagadas "sob medida", muito diferente das informações veiculadas em periódicos impressos, cuja matéria é apresentada igualmente para todos os leitores.

Dessa forma, ante a ciência de que o evento *fake news,* em sua tradução rasa, não é um problema novo, deve-se pontuar que o fenômeno, em seu modelo atual, é, ao menos para o grande público, a manifestação de um conflito mais complexo. De um lado, há a segurança de dados como expressão do direito à vida privada; de outro, a liberdade de informação para a veiculação de discursos de ódio por meio de notícias falsas.

Em síntese, a novidade que vem causando alvoroço a respeito do tema é, precisamente, a nova metodologia de captação e divulgação de informação. No direito, e sobretudo no que toca ao direito penal, ora entendido como produto da sociedade, essa mudança da estrutura de comunicabilidade gerou a necessidade de, ao menos, serem revisitados os institutos que envolvem a liberdade de informação e a vida privada.[13]

---

12 "Pode haver algum exagero nas previsões que fazem os cientistas acerca do futuro da sociedade atual, denominada *sociedade da informação.* Mas é fato que a capacidade de transmissão de dados, com fidedignidade e velocidade jamais vistas, bem como a facilidade de interação entre esses meios de comunicação criam as chamadas '*autoestradas da informação*' e estas constituem uma nova realidade, com a qual o direito deve lidar." (RODRÍGUEZ, 2008, p. 1)

13 *"Esto resulta de la constatación, obvia, pero no siempre valorada como se debe, de que el Derecho, y en especial el Derecho Penal, solo se concibe en relación a la sociedad. Si esto es una vieja verdad desde el aforismo latino del ubi societas*

3.1 O ANO DE 2018 E O DESCOBRIMENTO DO POTENCIAL DAS *FAKE NEWS*

O fato de, no aspecto mais amplo, direitos e informações – seja na forma de divulgação, seja na de transmissão, seja, ainda, na de produção – estarem em conflito não é novidade. Como dito, muitos são os exemplos de divulgação pública da vida privada. Vale dizer, nesse sentido, que o conflito remonta à criação dos direitos fundamentais, em especial o da liberdade de expressão.[14] Até mesmo no direito penal a divergência se apresenta. Crimes de injúria, calúnia e difamação

---

ibi jus, y el su correlato ubi jus ibi societas, la que debe ser profundizada es la idea que no solo el Derecho está asociado a la sociedad, sino que está asociado a una determinada sociedad. Es decir, el Derecho, y el Derecho Penal, se vinculan a un determinado contexto social, según las características presentes en un concreto punto temporal y espacial. En esta línea, si hay una expectativa de que el Derecho Penal, en alguna medida, pueda influenciar la configuración de una determinada sociedad, no menos correcto es que el contexto social influye en la configuración del Derecho Penal, teniendo en cuenta que son las normas penales el principal portal de conexión entre el mundo social y el mundo jurídico-penal." (FERNANDES, 2018)

14 A título de referência histórica: "Os direitos fundamentais, ao menos no âmbito de seu reconhecimento nas primeiras Constituições escritas, são o produto peculiar (ressalvado certo conteúdo social característico do constitucionalismo francês), do pensamento liberal-burguês do século XVII, de marcado cunho individualista, surgindo e afirmando-se como direitos do indivíduo frente ao estado, mais especificamente como direitos de defesa, demarcando uma zona de não intervenção do Estado e uma esfera de autonomia individual em face de seu poder (...). Assumem particular relevo nesse rol desses direitos, especialmente pela sua notória inspiração jusnaturalista, o direito à vida, à liberdade, à propriedade e à igualdade perante a lei. São, posteriormente, completados por um leque de liberdades, incluindo as assim denominadas liberdades de expressão coletiva (liberdades de expressão, imprensa, manifestação, reunião, associação, etc.) e pelos direitos de participação política, tais como o direito de voto e a capacidade eleitoral passiva, revelando, de tal sorte a íntima correlação entre os direitos fundamentais e a democracia." (SARLET, 2009, p. 46-47)

(arts. 138, 139 e 140 do CP), tanto no âmbito das relações pessoais quanto no de caráter econômico, como nos tipos de *insider trading* (art. 27-D da Lei n. 6.385/1976) ou informação falsa de produto (art. 66 do Código de Defesa do Consumidor), buscam regular condutas voltadas ao conteúdo e à transmissão de informações, de modo a prevenir consequências danosas.

Especificamente no que tange ao direito à vida privada, a mudança no panorama do conflito ocorreu em razão das *fake news,* que representam a ponta de um emaranhado de fios elétricos desencapados a envolver realidade informacional e seu conflito com o Direito.

Nesse sentido, o caso *Cambridge Analytica* mostrou ao mundo a importância dos dados virtuais e, mais do que isso, sua aplicação. Segundo noticiado,[15] a empresa conseguiu captar, organizar e analisar dados de aproximadamente 50 milhões de usuários de plataformas de redes sociais. Com eles, mapeou gostos pessoais, preferências políticas, padrões socioeconômicos, entre outras características. E não se limitou a isso; disseminou conteúdo capaz de influenciar as decisões cotidianas dos usuários. Em posse dos dados, a empresa foi capaz de traçar uma estratégia de produção e disseminação de informação individualizada, fazendo com que cada usuário recebesse um conteúdo específico e direcionado aos seus interesses.

A *Cambridge Analytica*, segundo noticiado, atuou na campanha de Donald Trump para a presidência dos Estados Unidos da América, bem como na campanha do *Brexit,* que consultou a população sobre a saída do Reino Unido da União Europeia. Para isso, produziu conteúdos – ainda não estamos no debate se falsos ou não – "personalizados" com o intuito de influenciar a decisão política dos leitores. Por exemplo, tinha-se a informação sobre quais usuários eram eleitores fiéis de

15 Cf. BBC News (Brasil), 2018.

Trump e quais eram – decididamente – eleitores de Hillary Clinton e quais – em dúvida – poderiam ser influenciados pelo envio de conteúdo. A esses que estavam em dúvida, eram disparados conteúdos, via de regra, engrandecendo Trump e, por vezes, denegrindo a concorrente Hillary Clinton[16].

O caso adquiriu tamanha proporção que foi parar no Senado estadunidense, onde o então CEO do *Facebook*, Mark Zuckerberg, reconheceu o vazamento de dados dos usuários e informou estar dispendendo grande esforço para evitar um novo episódio (SIMÕES, 2018).

No Brasil, certamente motivado pelo impacto mundial do exemplo americano, o Congresso promulgou, em 2018, a Lei Geral de Proteção de Dados (LGPD) – Lei n. 13.709/2018 –, que dispõe

> sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.[17]

Em seu art. 1º, versa a proteção aos direitos fundamentais da liberdade e de privacidade, demonstrando a importância de se regular o conflito entre a liberdade de informação e a vida privada.

Além da questão da proteção de dados dos usuários, a qual, certamente, tange ao direito à privacidade, a manipulação da informação fez

---

16 No julgamento da ADPF n. 572, em 18-6-2020, o ministro Gilmar Mendes, do STF, fez questão de pontuar a influência desse evento nas eleições presidenciais americanas.

17 "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural." (BRASIL, 2018)

com que as *fake news* fomentassem a discussão a respeito dos conteúdos veiculados. Com o objetivo de direcionar a opinião pública, houve uma produção massiva de conteúdos inverídicos. No Brasil, por exemplo, com vistas a desmoralizar a campanha política presidencial do Partido dos Trabalhadores por meio de acusações de corrupção, veiculou-se na internet a foto de uma grande fazenda, avaliada em 50 milhões de reais, cuja propriedade era atribuída ao filho do ex-presidente Luiz Inácio Lula da Silva. Entretanto, segundo apuração da *Revista Piauí* (MORAES, 2019), a imagem era da fachada do *campus* da USP de Piracicaba/SP (centro de pesquisas na área agronômica), a qual – por óbvio – não pertence ao filho de Lula.

O que impressiona neste fenômeno chamado *fake news* é, além de seus efeitos, o método usado, que pode ser dividido em três aspectos: 1º) proteção de dados; 2º) disseminação de notícias e 3º) limites do conteúdo produzido. Apesar de não se tratar de prática inédita, mas amplificada pelo contexto informacional pós-moderno, faz-se necessário projetar as questões ora debatidas para o campo jurídico, no qual o conflito entre liberdade de informação e direito à vida privada se intensificou.

4. OS APORTES JURÍDICOS DA NOVA METODOLOGIA DAS *FAKE NEWS*

4.1 A PROTEÇÃO DE DADOS E O DIREITO À VIDA PRIVADA

Delimitar o conceito de vida privada não é tarefa simples, sobretudo na pós-modernidade, em que, para usar da analogia de Zygmunt Bauman[18], a sociedade instalou microfones nos confessionários. Isto é, a pós-modernidade é de tal maneira marcada pela mitigação do limite

18 Conforme o programa "Estratégias para a vida", disponível no *YouTube*.

da vida privada que até os mais íntimos dos segredos, divididos somente com uma entidade divina, viraram objeto de interesse público. Logo, os assuntos mais relevantes estão, de fato, na esfera privada dos indivíduos. Não por outro motivo, as *fake news* abordam muitas vezes temas dessa seara.

Sobre tal superfície porosa, derrama-se a informação, fácil e rapidamente.[19] Remetendo-se ao exemplo do sociólogo polonês, pode-se afirmar que hoje os pecados não são confessados apenas por meio de autofalantes, há, ainda, as redes sociais.

O que talvez não tenha sido considerado até 2018 é o fato de que não somente o conteúdo da confissão é do interesse de alguns grupos mas também o caminho feito até a igreja. O que acontece com o chamado tratamento de dados[20] no estágio da coleta é, precisamente, o rastreamento desse caminho, vigiado quanto a todo e qualquer rastro deixado *on-line*. Em outras palavras, a conexão a uma rede de internet automaticamente aciona uma espécie de rastreador de passos físicos e virtuais. Aliás, nessa perspectiva, o que são os *smartphones* senão unidades individuais de coleta, transmissão e produção de dados?[21]

---

19 "Essa erosão do anonimato é produto dos difundidos serviços da mídia social, de câmeras em celulares baratos, sites grátis de armazenamento de fotos e vídeos e, talvez o mais importante, de uma mudança na visão das pessoas sobre o que deve ser público e o que deve ser privado." (BAUMAN, 2013, p. 29)

20 "Art. 5º Para os fins desta Lei, considera-se: (...) X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração." (BRASIL, 2018)

21 Victor Gabriel, em 2008, quando o *iPhone* (símbolo da revolução tecnológica informacional) ainda estava na 3ª geração (hoje chega-se à 11ª), já apontava a capacidade de armazenamento e combinação de dados das novas tecnologias: "A tecnologia hoje permite fazer armazenamento e combinação de dados como nunca antes, o que

Esse cenário, quando projetado no campo jurídico, vai de encontro aos tradicionais entendimentos de vida privada. Primeiramente, não comporta o conceito de intimidade apresentada no direito liberal, quanto ao reconhecimento do direito à vida privada, que a entendia como direito de estar só (COSTA JR., 1995), ou seja, tratava-se de uma faculdade do indivíduo de reduzir sua convivência a si mesmo. Isso se mostra, na realidade pós-moderna, impossível do ponto de vista material, em razão da complexidade social e, sobretudo, do desinteresse individual.

A necessidade de ver a vida privada não somente como liberdade mas também como garantia remonta à queda dos Estados totalitários europeus, quando as informações estatais (hoje tidas como públicas) eram secretas e as particulares eram arrancadas a fórceps pelos governos. Dessa forma, a vida privada aproxima-se da dignidade da pessoa humana, para tornar-se meio de exercício da personalidade. Não por outro motivo, o art. 5º, X, da Constituição Federal[22] assegura-lhe a inviolabilidade.

Sendo assim, a vida privada passa a ter de ser respeitada pelo Estado e agentes privados, independentemente do meio usado para isso[23]. Tanto

---

acarreta efetivamente um risco, reconhecido já por vários diplomas normativos." (RODRÍGUEZ, 2008, p. 21)

22 "Art. 5º (...) X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;" (BRASIL, 1988)

23 "Com o crescimento das tecnologias da informação, a possibilidade de ofensa à liberdade do cidadão já não se dá pela restrição de sua movimentação ou pelo contato do seu corpo. Uma série de intromissões indevidas em sua personalidade pode ser feita sem que se recorra ao elemento físico. É nesse momento que o direito à intimidade amplia-se e alcança sua fusão com as demais liberdades públicas, como direito à honra, à liberdade de expressão, de pensamento, de escolha religiosa etc. Nessa terceira fase da evolução da intimidade, encontra-se a intimidade-garantia." (RODRÍGUEZ, 2008)

é assim que o citado dispositivo constitucional, em seu inciso XI[24], determina a inviolabilidade das correspondências, mitigada apenas para fins de investigação criminal. Em outras palavras, o espaço privado das cartas está limitado aos intérpretes e, eventualmente, às partes de um processo penal.

Dessa maneira, estabelecida a vida privada como garantia jurídica para o desenvolvimento da personalidade e, assim, manutenção da dignidade da pessoa humana, a pergunta que surge é: os dados digitais são alcançados pela garantia jurídica constitucional da vida privada?

Sobre isso, a LGPD, ao afirmar, no art. 2º, I, IV e VII[25], que a proteção de dados tem por fundamento o respeito à privacidade, bem como a inviolabilidade da intimidade e o livre desenvolvimento da personalidade, não deixa dúvidas de que os dados digitais são alcançados pela garantia constitucional de preservação da vida privada.

No entanto, a mesma lei, no art. 7º, I[26], faculta ao titular dos dados a oportunidade de dispô-los e é, precisamente, nesse ponto que a realidade pós-moderna invade o plano jurídico, por vezes o invalidando. A divulgação dos próprios dados, ou seja, a publicidade, é pré-requisito para a participação na sociedade pós-moderna, principalmente, no que toca ao mundo virtual.

---

24 "Art. 5º (...) XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;" (BRASIL, 1988)

25 "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I – o respeito à privacidade; (...) IV – a inviolabilidade da intimidade, da honra e da imagem; (...) VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais." (BRASIL, 2018)

26 "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I – mediante o fornecimento de consentimento pelo titular;" (BRASIL, 2018)

Logo, da mesma forma que colocamos microfones nos confessionários, assinalamos aquele pequeno quadrado que representa a concordância com os termos de política de privacidade de uma rede social. E aceitamos isso não só por se tratar de pré-requisito para o cadastro em um *site* mas por ser a chave da participação na sociedade pós-moderna.

4.2 O ALCANCE DO DIREITO À LIBERDADE DE INFORMAÇÃO

O direito à liberdade de informação surgiu a partir do reconhecimento do direito à liberdade de imprensa. Por isso, nesse primeiro momento, tem-se uma estrutura axiológica ligada ao direito liberal burguês. No entanto, diante da atual relevância da informação, que se transformou em ativo econômico, bem como ante a atual facilidade de transmissão e criação de informações, o direito à liberdade de imprensa da estrutura liberal burguesa não é mais suficiente para regular as demandas da nova configuração social.

Nesse sentido, é preciso diferenciar liberdade de informação e direito à informação. Este é um direito individual, vinculado à privacidade e ao acesso a informações públicas[27]. Já aquela consiste em direito coletivo de produzir e receber informações.[28]

---

27 A título de melhor explicação, esse direito pode ser garantido pela ação de *habeas data,* cujas hipóteses de concessão estão descritas no art. 5º, LXII, *a* e *b*, da Constituição Federal.

28 "Nesse sentido, a *liberdade de informação* compreende a procura, o acesso, o recebimento e a difusão de informações ou ideias, por qualquer meio, e sem dependência de censura, respondendo cada qual pelos abusos que cometer. O acesso de todos à informação é um direito individual consignado na Constituição, que também resguarda o sigilo da fonte, quando necessário ao exercício profissional (art. 5º, XIV). Aqui se ressalva o direito do jornalista e do comunicador social de

Assim, deve-se estabelecer que o direito à liberdade de informação se manifesta em três circunstâncias: 1) liberdade de informar, ou seja, de produzir informações e disseminar ideias, no âmbito jornalístico ou não; 2) liberdade de acesso a informações, entendendo-se que hoje é necessário um mínimo de informações para o exercício consciente de liberdade pública[29] e 3) a liberdade de ser informado, a qual chega próximo ao direito à vida privada, sendo essa a faculdade da pessoa de selecionar as informações que deseja receber[30].

Posto isso, deve-se perceber que as *fake news* colocam em xeque essas liberdades, uma vez que aquelas resultam da hipertrofia das ferramentas informacionais. Daí questiona-se sobre serem as *fake news* manifestações de abuso da liberdade de informação.

Em um primeiro olhar, elas desafiam o aspecto da liberdade de informação em sua primeira dimensão, ou seja, o direito de produção de notícias, em especial, no que se refere ao conteúdo das mensagens veiculadas. Via de regra, estas não costumam se aprofundar quanto à veracidade do fato narrado, além de apresentarem uma abordagem rasa. Sendo assim, a identificação de uma *fake news* se dá, justamente, pela percepção da ausência de conteúdo denso e de investigação no sentido jornalístico.

---

não declinar a fonte onde obteve a informação divulgada. Em tal situação, eles ou o meio de comunicação utilizado respondem pelos abusos e prejuízos ao bom nome, à reputação e à imagem do ofendido (art. 5º, X)." (SILVA, 2013, p. 243)

29 "(...) sempre crescente da coletividade para que tantos os indivíduos como a comunidade estejam informados para o exercício consciente das liberdades públicas." (SILVA, 2013, p. 245)

30 "A liberdade de informação compreende tanto o direito de informar, que se confunde com a liberdade de manifestação do pensamento, como o de ser informado, que corresponde ao direito coletivo de receber a informação para que o receptor melhor identifique o seu pensamento." (CALDAS, 1997, p. 58)

No mais, elas vêm sendo responsáveis pela retomada de um discurso desagregador[31], que tem polarizado o debate político, e, mais do que isso, causado dissenso sobre a percepção da realidade.

Quanto a esse aspecto, o que surpreende é a legitimidade que tais notícias adquiriram nos últimos tempos. Embora não se possa atribuir total imparcialidade aos veículos de imprensa (e não é essa a obrigação), é notório que o senso comum vem atribuindo maior legitimidade às notícias veiculadas por aplicativos e redes sociais que as reportagens publicadas nos tradicionais veículos de imprensa. Isso se dá pela capacidade de alcance e velocidade de produção destes conteúdos rasos e sem maiores investigações, que superam o rigor da imprensa profissional. Enquanto qualquer um de nós, por meio do telefone celular, pode editar uma imagem, produzir um texto de duas frases e logo veicular nas redes sociais, o jornalismo tradicional mantém uma estrutura de edição, revisão e autorização que vai desde o repórter até o editor-chefe.

Uma outra questão que nos surpreende é a mitigação da liberdade de seleção das informações, ou seja, a liberdade de ser informado. Como revelado no caso *Cambridge Analytica,* as empresas detêm a capacidade de formular perfis e direcionar as mensagens enviadas. Diante disso, preocupa não o envio de propagandas políticas – que sempre houve –, mas a transmissão individualizada, sob o fundamento da captação de dados – *a priori* –, sem que o usuário tenha plena consciência dos efeitos dessa prática.

Ocorre que o indivíduo, ao acessar a plataforma de uma rede social, insere seus dados e autoriza a empresa administradora a dispor deles.

---

31 Ressalva-se que melhor expressão seria "discurso de ódio"; no entanto, para sintetizar, limita-se à expressão "discurso desagregador", pois o uso da terminologia "ódio" necessitaria de aporte teórico que não constitui objeto deste excerto. É, então, por fidelidade metodológica que se faz essa opção, bem como a ressalva.

Essa, por sua vez, obtém lucros e dividendos por meio de contratos de propaganda; por isso, passa a definir perfis e direcionar as mensagens. O mesmo acontece com todas as empresas que, como as redes sociais, usam de *big data*[32] e algoritmos para o tratamento de dados e disseminação de informações. Desse modo, o inscrito deixa de selecionar as mensagens que lhe são transmitidas e passa a receber aquelas elaboradas de acordo com seu perfil.

Essa prática pode ser inofensiva do ponto de vista do mercado de consumo; pois, baseada nas preferências de cada usuário, sugere a X a compra de um tênis esportivo e a Y a compra de itens de decoração. No entanto, adquire especial relevo nas campanhas políticas e de opinião, sobretudo em vista dos efeitos que são capazes de produzir. Dado que, conforme já dito, constatou-se a influência dessa prática nas decisões coletivas, ou seja, as coletividades vêm sendo influenciadas para uma determinada direção, por meio de contato individualizado de informações sobre fatos políticos.

A questão em debate, portanto, não se resume à veracidade das informações, mas, precisamente, ao método de transmissão e seus efeitos. Do ponto de vista jurídico-penal, essa é a conduta que deve ser objeto de análise. Do contrário, uma restrição de liberdade que ultrapasse esse alcance, estará, certamente, tangenciando a garantia constitucional de liberdade de informação em sua forma mais tradicional.

32 A expressão traduz, em resumo, a prática de análise e interpretação de grandes volumes e variedades de dados virtuais.

5. A DIMENSÃO JURÍDICO-PENAL DO PROBLEMA DAS *FAKE NEWS*: A ANÁLISE DE SUA RELEVÂNCIA

A tendência moderna, no tocante ao sistema jurídico-penal, é de uma maior racionalidade na intervenção penal. Isso se reflete na ênfase dada aos métodos usados para a realização do Direito na atualidade, no sentido de uma renormatização que está se acentuando.

Como consequência, as categorias e os conceitos da dogmática jurídico-penal passaram a ser cunhados e determinados por proposições político-criminais, de maneira que juntas – política criminal e dogmática jurídico-penal – formam uma unidade funcional. Logo, apenas um sistema penal que tenha fundamentação em valores político-criminais torna possível a ligação entre as normas e a realidade social:

> À sua luz se compreende perfeitamente que o jurídico e a sua dogmática não são – não podem, nem devem ser – algo de diferente e de separado do sistema social, mas, pelo contrário, se apresentam como verdadeiros *subsistemas* do sistema social. Como bem se compreende que a política criminal não seja – não possa, nem deva ser – uma simples *ciência auxiliar* do direito penal e da sua dogmática, uma ciência que só atuaria dentro dos limites que lhe são assinados pelas normas jurídicas provadas no Parlamento. (DIAS, 1999, p. 41)

Diante desse contexto, o problema da relevância das *fake news* será analisado com base em dois critérios político-criminais muito utilizados atualmente e que promovem resultados aceitáveis: a *dignidade penal* e a *carência de tutela penal*.

5.1 DA DIGNIDADE PENAL DOS DIREITOS ENVOLVIDOS

A dignidade penal, para Costa Andrade (1992, p. 184), é "como a expressão de um juízo qualificado de intolerabilidade social, assente na valoração ético-social de uma conduta, na perspectiva da sua criminalização e na punibilidade".

No plano "trans-sistemático", a dignidade penal assegura o fundamento constitucional de que apenas bens jurídicos de evidente relevância devem gozar dessa proteção e, nessa medida, a dignidade penal abarca o princípio da proporcionalidade.

Já no aspecto valorativo, Costa Andrade (1994, p. 184) ensina que "o juízo de dignidade penal privilegia dois referentes materiais: a dignidade de tutela do bem jurídico e a potencial e gravosa danosidade social da conduta, enquanto lesão ou perigo para os bens jurídicos".

Por fim, no âmbito jurídico-sistemático, a dignidade penal "mediatiza e actualiza" (ANDRADE, 1994, p. 184) o postulado de que o ilícito penal é singular e distinto de outras formas de ilícito.

Ora, a informação é um direito humano, constitucionalmente proclamado (art. 5º, XIV, da CF/1988), cuja inviolabilidade é garantida, na medida em que a Constituição também garante o direito à liberdade de imprensa e o direito de *Habeas Data*. Essa circunstância já seria justificadora da dignidade penal da informação, ao menos em termos formais.

Em termos materiais, é possível questionamentos acerca da danosidade social de algumas manifestações baseadas em informações falsas quando se trata de caso concreto, de pequena magnitude, tal como um comentário proferido entre amigos, desprovido de veracidade, que não implique a ocorrência de um ilícito penal (por exemplo, de um crime contra a honra).

Contudo, a propagação de notícias falsas com o uso da internet, seja por intermédio de redes sociais virtuais, seja por portais de notícias, principalmente quando atrelada ao uso de algoritmos, reveste-se de maior significância. Tal conduta está diretamente vinculada à complexi-

dade dessas novas tecnologias, sobretudo pelo potencial de manipulação da opinião pública e penetralidade em todos os aspectos da vida.

O método usado para propagação de *fake news*, que ora se pontua como diferencial de um crime contra a honra – tangencia direitos, como a privacidade e a liberdade de informação, os quais podem ser merecedores de tutela penal, como já o são em outros crimes. Ademais, sabendo que o direito penal é um instrumento de regulamentação de condutas e liberdades – exemplo disso é liberdade para o incremento de patrimônio, mas não por meio do furto –, observa-se que a relação entre o uso das novas técnicas informacionais e os direitos fundamentais pode ser ponto de regulação penal. Nesse caso, como em todos os delitos, há choque entre liberdades, quais sejam, o direito à vida privada, à liberdade de disposição de dados e à de informação, sobretudo no tocante à produção de conteúdo.

Por conseguinte, resta demonstrada a dignidade penal do direito à informação no plano trans-sistemático, uma vez que se trata de direito fundamental; no plano valorativo, na medida em que a veiculação de uma informação falsa hoje, com o uso da internet, pode causar fortes danos à sociedade; e, por fim, no plano jurídico-sistemático, no qual se distingue a divulgação de informações falsas de pequenas magnitudes daquelas veiculadas na internet.

5.2 DA POSSIBILIDADE DE TUTELA PENAL

Sobre a necessidade de tutela penal, Fernandes (2003, p. 69) entende que é a expressão de princípios que regem o direito penal, como a subsidiariedade, a *ultima ratio* (fragmentariedade) e a proporcionalidade:

> Trata-se de um referente político criminal, de cunho particularmente *funcional*, que implica em um duplo juízo: o da *necessidade*, dizendo

> respeito à inexistência de outros meios – jurídicos ou não – capazes de oferecer a tutela adequada e suficiente (*subsidiariedade*); o da *idoneidade*, relativo à aptidão e eficácia da tutela penal para a proteção do bem (*a adequação*); o da *proporcionalidade*, implicando em uma verificação das vantagens e desvantagens político-criminais de intervenção penal, com vistas a se poder afirmar que a tutela não gera mais custos que benefícios.

Em relação à tutela penal da informação, vemos que não há, no nosso ordenamento jurídico, nenhum tipo penal que preveja o "crime de *fake news*", embora haja projetos de lei em trâmite no Congresso nesse sentido.

A informação em si mesma não é protegida em termos penais, de forma que, para haver alguma violação penal, é preciso que a informação esteja atrelada a um tipo penal vinculado a normas relativas a outros bens jurídicos, como a honra, por exemplo.

Contudo, esses tipos penais, que não tratam a informação como valor em si mesma, não são suficientes para compreender as particularidades da propagação de uma informação falsa por intermédio das novas tecnologias de informação, processamento e comunicação, bem como dos efeitos decorrentes disso (violação da vida privada, manipulação da opinião pública, discurso desagregador).

Dessa forma, no tocante à propagação de *fake news* por intermédio das novas tecnologias de informação, processamento e comunicação, quando direcionadas ao grande público, com ou sem o uso de algoritmo voltado para definir um perfil e projetar mensagem específica a ele, mas agravada por esse uso, faz com que se eleve o debate ao plano da proteção pela via penal e sua eficácia.

Esse tipo de ofensa, dado seu potencial lesivo, faz com que haja proporcionalidade em se recorrer à tutela penal, mais gravosa. Nesse sentido, ainda que se possa discutir sobre os diversos problemas relacionados ao cárcere, cumpre esclarecer que não necessariamente há de

se vincular um tipo penal que tenha como centro norma proibitiva de disseminação de informação falsa, com a pena privativa de liberdade.

E, mais, como bem ressalta Jakobs (2003), a essência do direito penal não é a pena, mas a norma, sendo ela a responsável por assegurar, no plano da comunicação, a identidade de uma determinada sociedade. À pena é atribuída uma identidade normativa, como meio de manter a identidade do social.[33]

Assim, por um lado, é possível que a submissão das condutas relacionadas às *fake news* seja objeto de ressalvas quanto à necessidade de intervenção penal, em um sentido tradicional, implicando a violação das respectivas normas em consequências, por vezes, ineficazes, de um ponto de vista político-criminal, e injustificadas, de uma perspectiva das liberdades pessoais.

Todavia, por outro lado, há que se considerar o reconhecimento que vem merecendo os efeitos, acertadamente questionáveis em termos simbólicos, no que se refere às sanções penais tradicionais, mas efetivos quanto à validação das normas. Com isso, abre-se a hipótese da pertinência da criminalização das condutas associadas às *fake news*, no sentido recortado no texto, com previsão de sanções alternativas, mas revestidas do desvalor penal.

São para situações como as mencionadas que o equilíbrio entre dignidade penal e necessidade de pena não se dá em um ponto equidistante dos extremos, requerendo um juízo de ponderação mais agudo quanto à função de comunicação da norma de natureza penal.

---

33 "Apenas sobre a base de uma compreensão comunicativa do fato entendido como afirmação que contradiz a norma e da pena entendida como resposta que confirma a norma se pode encontrar uma relação iniludível entre ambas e, nesse sentido, uma relação racional, e tudo isso sob condições das quais aqui teremos de falar." (JAKOBS, 2003, p. 3)

6. CONCLUSÃO

O sistema jurídico-penal, enquanto "cartão de visitas" da sociedade, tem sido fortemente influenciado pela configuração desta, em especial, marcado pelo uso e importância cotidiana das novas tecnologias da informação. A elas é atribuída uma série de características intrínsecas, com ênfase para a penetralidade, o alcance massivo, a mitigação da distância física, a rapidez de propagação da informação e a concentração da produção de recepção de conteúdo a um perfil específico.

Essa influência se manifesta também no problema das *fake news*, que, embora sejam há muito conhecidas, a partir de 2018 passaram a ser foco de uma nova percepção sobre o problema que, por sua vez, está atrelada a uma mudança no método de propagação das informações falsas, devido à utilização das novas técnicas de informação, processamento e comunicação. Inclusive, com a análise de perfis de usuários e a destinação de informação exclusiva e moldada para cada um.

Frente a esse novo método, os efeitos também foram potencializados, de forma que a disseminação de informação falsa pode estar atrelada à violação da vida privada, devido ao uso de dados de usuário; à retomada de um discurso desagregador; e à influência exercida sobre a coletividade, movida em uma determinada direção, por meio de contato individualizado com informações sobre fatos políticos.

Dessa maneira, uma vez que o direito de acesso à informação é um direito fundamental e que a propagação de informações falsas se reveste de forte danosidade social, está justificada a sua dignidade penal. No mesmo sentido, diante da inexistência de um tipo penal que tenha como centro uma norma proibitiva de disseminação de informações falsas e que o direito penal é adequado para essa regulação, principalmente se considerado o método de transmissão de mensagens com o uso das novas tecnologias, está justificada a necessidade de intervenção penal.

É esse, em síntese, o ponto central do trabalho, mais do que desenvolver um juízo político-criminal sobre a criminalização das chamadas *fake news*, deve-se esclarecer qual a conduta será objeto do debate. Como se viu, existem condutas já criminalizadas, enquanto outras sequer mereceram tutela penal. Não por outro motivo, focamos em argumentar que a diferença histórica hoje promovida pelas *fake news* é propriamente o método.

Sendo assim, defende-se que a conduta a ser analisada é, precisamente, a dissipação direcionada e individualizada de notícias ou informações falsas por meio da captação e do tratamento de dados sem autorização do usuário. É em relação a esse modelo de conduta de *fake news* que deve recair o juízo político-criminal, a partir dos critérios do merecimento e da dignidade de pena.

Resulta bastante consistente daí a afirmação a respeito da dignidade penal, dada a relevância dos interesses em causa e a dimensão dos danos sociais provocados. Submetido o modelo de conduta ao critério da necessidade de pena, ainda que, em regra, o recurso às normas penais deva sempre ser preterido por outras formas de intervenção, há de ser considerada a importância do sentido que comunicam estas normas em termos preventivos, admitindo-se-lhes o recurso, mesmo que sem a necessidade do recurso às tradicionais e mais gravosas formas de sanção penal para a sua estabilização.

REFERÊNCIAS

ANDRADE, Manuel da Costa. A "dignidade penal" e a "carência de tutela penal" como referências de uma doutrina teleológico-racional do crime. *Revista Portuguesa de Ciência Criminal*, Lisboa, ano 2, fasc. 2, p. 173-205, abr./jun. 1992. p. 184.

BAUMAN, Zygmunt. *Modernidade líquida*. Tradução de Plínio Dentzien. Rio de Janeiro: Zahar, 2001.

BAUMAN, Zygmunt. *Vigilância líquida*: diálogos com David Lyon. Rio de Janeiro: Zahar, 2013.

BBC NEWS (Brasil). Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. *BBC News Brasil*, 20 mar. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751#:~:text=A%20rede%20social%20diz%20que,alega%C3%A7%C3%B5es%20%22falsas%20e%20difamat%C3%B3rias%22. Acesso em: 8 out. 2020.

BRASIL. [Constituição (1988)]. *Constituição Federativa do Brasil de 1988.* Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 9 out. 2020.

BRASIL. *Lei n. 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709compilado.htm. Acesso em: 8 out. 2020.

CALDAS, Pedro Frederico. *Vida privada, liberdade de imprensa e dano moral*. São Paulo: Saraiva, 1997. p. 58.

CASTELLS, Manuel. *A galáxia da internet:* reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. *A sociedade em rede*. Tradução de Roneide Venancio Majer. 8. ed. rev. e ampl., São Paulo: Paz e Terra, 2016. v. 1.

COSTA JR., Paulo José. *O direito de estar só, tutela penal da intimidade*. São Paulo: Revista dos Tribunais, 1995.

CPFL. *Estratégias para a vida | Zygmunt Bauman*. Produção: Café

Filosófico. 2017. Disponível em: https://www.youtube.com/watch?-v=IyhOBYoBnsU&ab_channel=Caf%C3%A9Filos%C3%B3ficoCPFL. Acesso em: 7 out. 2020.

DIAS, Jorge de Figueiredo. *Questões fundamentais do direito penal revisitadas*. São Paulo: Editora dos Tribunais, 1999.

FAUSTO, Boris. *História concisa do Brasil*. 2. ed. São Paulo: Edusp, 2011.

FERNANDES, F. A. Corrupción y medios de comunicación. *In*: RODRIGUEZ GARCIA, Nicolás *et al*. *Justicia penal pública y medios de comunicación*. Valencia, Espanha: Tirant lo Blanch, 2018. cap. 18.

FERNANDES, F. A. *O processo penal como instrumento de política criminal*. Coimbra: Almedina, 2001.

FERNANDES, F. A. Sobre uma opção jurídico-política e jurídico-metodológica de compreensão das ciências jurídico-criminais. *In*: SEBASTIÃO, Luzia Bebiana de Almeida *et al*. (Orgs.). *LiberDiscipulorum para Jorge de Figueiredo Dias.* 1. ed. Coimbra: Coimbra Editora, 2003, p. 1153-1183.

JAKOBS, Günther. *Sociedade, norma e pessoa:* teoria de um direito penal funcional. Tradução de Maurício Antônio Ribeiro Lopes. Barueri/SP: Manole, 2003. Estudos de Direito Penal, v. 6.

MORAES, Maurício. #Verificamos: "Fazenda de R$ 50 milhões do filho de Lula" é, na verdade, *campus* universitário em Piracicaba. *Revista Piauí*, Rio de Janeiro, 2019. Disponível em: https://piaui.folha.uol.com.br/lupa/2019/01/17/verificamos-fazenda-filho-lula-campus/. Acesso em: 8 out. 2020.

RODRÍGUEZ, Victor Gabriel. *Tutela penal da intimidade*: perspectiva da atuação penal na sociedade da informação. São Paulo: Atlas, 2008.

ROXIN, Claus. *Política criminal e sistema jurídico-penal*. Tradução de Luís Greco. Rio de Janeiro: Renovar, 2000.

SARLET, Ingo Wolfgang. *A eficácia dos direitos fundamentais*: uma teoria dos direitos fundamentais na perspectiva constitucional. 10. ed. Brasília: Livraria do Advogado, 2009. p. 46-47.

SILVA, José Afonso da. *Curso de direito constitucional*. 36. ed. rev. São Paulo: Malheiros, 2013.

SIMÕES, Helton Gomes. Em depoimento de 5 horas ao Senado americano, Mark Zuckerberg admite erros do Facebook: Presidente do Facebook respondeu questões sobre regulação, uso de dados de usuários e como empresa reagiu ao escândalo da Cambridge Analytica. *G1.com*, 10 abr. 2018. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/mark-zuckerberg-depoe-ao-senado-sobre-uso-de-dados-pelo-facebook.ghtml. Acesso em: 19 out. 2020.

UNCTAD – United Nations Conference on Trade and Development. *Information Economy Report*. Nova Iorque e Genebra: Nações Unidas, 2017. Disponível em: https://unctad.org/system/files/official-document/ier2017_en.pdf. Acesso em: 13 out. 2020.

ZOLA, Emilé; BARBOSA, Rui. *Eu acuso!* O processo do capitão Dreyfus. Tradução e organização de Ricardo Lísias. São Paulo: Hedra, 2008.

CONTROLE SOCIAL, TRATAMENTO DE DADOS SENSÍVEIS E SAÚDE PÚBLICA: PERSPECTIVAS À LUZ DA BIOÉTICA E DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Laura Maria Brandão Estancione[1]
João Rodrigo Stinghen[2]

RESUMO

A Lei Geral de Proteção de Dados Pessoais (LGPD) tem grande relevância, seja para adequar o Brasil aos padrões exigidos internacionalmente, seja para respeitar os direitos dos titulares. Sobretudo, proporciona a tutela dos dados sensíveis, tendo em vista a natureza mais intimista e personalíssima destes. Diante disso, o presente trabalho busca apresentar subsídios ao intérprete do art. 5º, II; do art. 6º, IX; e do art. 11 da LGPD, por meio da análise das intersecções com a bioética e o regulamento europeu de proteção de dados, no que possam enriquecer o debate sobre o tema. A discussão é especialmente relevante quando

1 Mestranda em Direito pela PUC-PR, com ênfase em bioética. Graduada em Direito pela UEL. Advogada penalista.

2 Pós-graduando em Direito Digital e Proteção de Dados pela Ebradi. Membro da Associação Nacional de Profissionais de Privacidade de Dados (ANPPD). Fundador do Instituto de *Compliance* Notarial e Registral (ICNR). Advogado.

esses direitos são relativizados por pautas coletivas, como a proteção da saúde pública em razão da pandemia de covid-19.

Palavras-chave: LGPD. GDPR. Dados sensíveis. Saúde pública. Covid-19.

ABSTRACT

The Brazilian General Data Protection Law (LGPD) is relevant to make Brazil conform to internationally required patterns, as well as to respect users' rights. Most importantly, one must protect sensitive data, given its intimate and personal nature. The present work aims to give subsidies to the interpreter of art. 5, II, art. 6, IX and art. 11 of the LGPD, searching for intersections with bioethics and with the European Union's General Data Protection Regulation (GDPR), with regards to what these instruments can help enrich discussion about the theme. The debate is especially relevant when these rights are relativized due to collective demands, such as the protection of public health in the context of covid-19's pandemic.

Keywords: LGPD. GDPR. Sensitive data. Public health. Covid-19.

1. INTRODUÇÃO

A insegurança prevalecente no ano de 2020, gerada pela pandemia de covid-19 e pelo vaivém do jogo político no cenário político-social brasileiro, resultou em sucessivos adiamentos da entrada em vigor da Lei Geral de Proteção de Dados Pessoais (LGPD). Esse diploma se apresentou no contexto nacional como norma de caráter imprescindível à adequação do Brasil aos padrões exigidos internacionalmente à garantia do respeito aos direitos dos titulares.

A LGPD teve sua edição voltada, sobretudo, à tutela de *dados sensíveis*, cuja natureza mais intimista e personalíssima exige maiores cuidados. Esse é, portanto, o escopo do presente trabalho, o qual abordará o tema à luz de conceitos e formas da área da privacidade de dados pessoais da lei brasileira e europeia, analisando intersecções com a bioética que possam enriquecer o debate a respeito da matéria.

A discussão é importante não pelo incentivo ao diletantismo acadêmico, mas pela contribuição ao estabelecimento de uma base doutrinária na qual o intérprete da LGPD – magistrado, agente de tratamento de dados ou membro da Autoridade Nacional de Proteção de Dados Pessoais – possa buscar opiniões fundadas, tecidas a partir do arcabouço conceitual e científico.

É evidente que as decisões e interpretações a partir do Regulamento Geral sobre Proteção de Dados – ou *General Data Protection Regulation* (GDPR) – são a fonte mais imediata de pesquisa. Porém, a busca do "melhor direito" não pode se limitar a ele.

Logo, assim como os critérios consolidados para as boas práticas de governança de dados são buscados em padrões da *Internacional Standard Organization* (ISO) e nos conteúdos da *International Technology Information Library* (ITIL), esse trabalho tem como objetivo fornecer, a partir dos conceitos da bioética, subsídios para o intérprete dos arts. 5º, II; 6º, IX; e 11 da LGPD.

2. OS DADOS SENSÍVEIS NA LGPD E NO GDPR

A comunidade global encontra-se numa nova fase, pós-moderna, iniciada pela chamada quarta revolução industrial, marcada pela era tecnológica numa simbiose com a vida humana.

Uma das frentes revolucionadas é a da informação, por seu imediatismo e alcance global, bem como por sua característica de tornar

menos nítido o limite entre o público e o privado. Exemplo disso é o aparelho telefônico móvel, que se tornou espécie de prótese, uma vez ser capaz de analisar o quadro de saúde (horas e qualidade do sono, passos dados e distância caminhada), os lugares mais frequentados por seu proprietário, as preferências pessoais etc. Quanto a esses aspectos, o que se revela mais preocupante é a capacidade de as operadoras de telefonia controlarem a tecnologia de geolocalização.

Em decorrência da covid-19, a entrada em vigor da LGPD teve de sofrer recorrentes adiamentos. Sua validade estava prevista para ter início a partir de 16 de agosto de 2020 – dois anos após sua publicação. Todavia, o advento da pandemia gerada pelo novo coronavírus permitiu o surgimento de uma série de iniciativas legais com a intenção de postergar a vigência.

Desde 2018, o GDPR foi o grande marco da conscientização mundial quanto à necessidade da proteção de dados na era da sociedade da informação, considerada a quarta revolução industrial. O paulatino crescimento do interesse pelo tema fez com que esse diploma legal adquirisse relevância mesmo nos países em que não aplicado. As razões para isso são diversas.

Uma delas reside no fato de o GDPR oferecer um *standard* valorativo e principiológico de proteção de dados suficientemente amplo e profundo (a LGPD não passa de um resumo do GDPR). Além disso, inúmeras empresas multinacionais pautaram sua atuação com base nele. Um terceiro motivo se fundamenta na histórica posição da Europa como centro de referência na matéria, a determinar seu pioneirismo na tutela dos direitos relacionados à privacidade de dados. Embora o tema da privacidade como direito autônomo tenha surgido no século XIX, nos EUA, ele passou a ser regulamentado na Europa, sendo previsto já no art. 12 da Declaração Universal dos Direitos Humanos de 1948.

A LGPD é uma das inúmeras normas criadas sob a influência do GDPR. Entretanto, no Brasil, a privacidade não é assunto recente, tendo sido a matéria tratada em diversos dispositivos da legislação brasileira. A privacidade é – por interpretação extensiva do termo "intimidade" – direito

fundamental previsto na Constituição desde 1988 (art. 5º, X), bem como direito da personalidade previsto no Código Civil desde 2002 (art. 21) – sem contar outros direitos de titulares de dados positivados em leis esparsas (como o CDC, a Lei de Acesso à Informação e o Marco Civil da Internet).

Com amparo nesse ambiente normativo, a LGPD, mesmo sem viger, já está gerando efeitos, inclusive como fundamento *obter dictum* para julgamentos de repercussão geral. A título de exemplo, no julgamento da Medida Cautelar na Ação Direta de Inconstitucionalidade n. 6.387, o Supremo Tribunal Federal (STF) suspendeu a eficácia da Medida Provisória (MP) n. 954/2020[3], que determinava a remessa massiva de dados pessoais de consumidores ao Instituto Brasileiro de Geografia e Estatística (IBGE) por empresas de telefonia. Como não havia suficientes esclarecimentos quanto à finalidade e segurança do tratamento desses dados, o STF entendeu que a MP violava a privacidade e a autodeterminação informativa dos titulares, ambos direitos já previstos no ordenamento brasileiro e positivados na LGPD.

2.1 DADOS SENSÍVEIS NO GDPR

Como se disse, a LGPD é um grande resumo do regulamento europeu de proteção de dados. Logo, uma interpretação da lei brasileira que se pretenda séria e profunda não pode se furtar à análise do diploma que tanto influencia as legislações e os padrões do mundo todo.

3 Em síntese, a MP n. 954/2020 dispõe que, no contexto da pandemia de covid-19, as empresas de telecomunicações deveriam compartilhar com o IBGE uma série de dados pessoais de seus consumidores (nomes, números de telefone e endereços), para fins de "produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares".

O GDPR (UENO, 2020) constitui-se de 99 artigos, divididos em 11 capítulos que contemplam conceitos e princípios relativos à proteção de dados, direitos dos titulares, responsabilizações por danos, agentes de tratamento, entre vários outros temas. No que ora interessa, convém mencionar os conceitos do art. 4º, notadamente o de *dados pessoais* (informação relativa a uma pessoa singular identificada ou identificável) e o de *dados sensíveis* (raça, etnia, opinião política, convicção religiosa ou filosófica, filiação sindical, genética e biometria).

O regulamento prevê em seu art. 9º a existência de um gênero denominado "categorias especiais de dados pessoais". Diferentemente da lei brasileira, ele traça como regra geral a proibição do tratamento desses dados:

> Artigo 9º Tratamento de categorias especiais de dados pessoais 1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa. (UENO, 2020)

Em seguida, o item 2 do art. 9º define as hipóteses em que seu tratamento é permitido. Logo, a opção legislativa de criar uma regra geral proibitiva com exceções tem como objetivo criar tipos cerrados, com rígidos esquadros autorizativos para o tratamento de dados pessoais especiais.

Mesmo assim, existem dez hipóteses autorizativas, que abarcam variadas situações. Ou seja, o objetivo do GDPR não é impedir o tratamento desses dados especiais, mas apenas restringi-lo, tendo em vista seu maior potencial danoso aos direitos dos titulares. Veja-se abaixo as hipóteses cujo estudo mais pode interessar ao escopo do presente trabalho:

b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do *exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social*, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;

c) Se o tratamento for necessário para proteger os *interesses vitais do titular dos dados ou de outra pessoa singular*, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;

(...)

g) Se o tratamento for necessário por motivos de *interesse público importante,* com base no direito da União ou de um Estado-membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;

h) Se o tratamento for necessário para efeitos de *medicina preventiva ou do trabalho*, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n. 3;

i) Se o tratamento for necessário por *motivos de interesse público no domínio da saúde pública*, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou

> dos Estados-membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional. (UENO, 2020)

Já no item 4 do art. 2º, é facultada aos Estados-membros a imposição de outras limitações ao tratamento de alguns dados especiais, como os biométricos ou relativos à saúde (UENO, 2020). Quanto a esse aspecto, convém mencionar na íntegra o art. 10, que versa o tratamento de dados pessoais relacionados às condenações penais e infrações:

> Artigo 10. (...) O tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas com base no artigo 6º, n. 1, só é efetuado sob o controlo de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado-membro que prevejam *garantias adequadas para os direitos e liberdades dos titulares dos dados*. (UENO, 2020)

Note-se que o dispositivo faz uma ressalva interessante, no sentido de que o tratamento de dados com *medidas de segurança* deve pautar-se pelas garantias adequadas aos direitos e às liberdades dos titulares. É justamente o que deve ocorrer, por exemplo, no tocante ao tratamento de dados pessoais – sobretudo sensíveis –, por ocasião de medidas de combate ao coronavírus, por exemplo.

2.2 CONCEITO E ESPÉCIES DE DADOS SENSÍVEIS NA LGPD

Os dados pessoais precisam ser protegidos por serem expressão da dignidade humana. Daí a LGPD se fundamentar no respeito à privacidade, na autodeterminação informativa, na inviolabilidade da intimidade, da honra e da imagem, nos direitos humanos, no livre desenvolvimento

da personalidade, dignidade e cidadania (art. 2º), e, sobretudo, na não discriminação (art. 6º, IX).

Os dados sensíveis são os que mais propriamente representam o âmago da intimidade humana, daí a proteção maior que a lei confere a seu tratamento. Antes, porém, de abordá-los, é preciso compreender alguns conceitos correlatos. A partir da LGPD, é possível deduzir três categorias de dados: (i) os anonimizados; (ii) os pessoais comuns; (iii) e os pessoais sensíveis. Os primeiros são relativos a titulares que não possam ser identificados (art. 5º, III), motivo pelo qual não geram direitos. Já os segundos pertencem a uma categoria residual: todos aqueles que não são sensíveis[4].

Finalmente, os terceiros consistem em informações que mais profundamente se relacionam com aspectos personalíssimos do titular. Daí a necessidade de uma proteção mais rígida, pois impactos sobre eles têm maior potencial lesivo aos titulares. Além disso,

> (...) o princípio da não discriminação ganha contornos especiais quando se está a investigar a tutela dos dados pessoais sensíveis, pois, devido à sua natureza, tais dados revelam um acirramento dos riscos de estratificação pessoal e estigmatização de pessoas a partir de perfis traçados pelo processamento de dados coletados. (FALEIROS JR., 2019)

O art. 11 da LGPD prevê um **rol específico de hipóteses autorizativas** para legitimação de tratamento, de interpretação taxativa, dado

4 Note-se que ampla gama de informações impessoais foge ao escopo da LGPD. Essas não se enquadram sequer no conceito de "dados anonimizados", pois nunca foram um dia pessoais. Isso, porém, não significa que não precisem de proteção, pois podem ser resguardadas por legislações específicas. Exemplos importantes são os dados referentes a pessoas jurídicas: não são protegidos pela LGPD, mas pelas leis de direitos autorais e patentes.

o uso da palavra "somente" no *caput* do dispositivo. Se o tratamento ocorrer com mais de um tipo de dados, a presença de elementos sensíveis atrai a incidência da proteção especial, na forma do art. 11, § 1º.

Embora semelhantes às hipóteses gerais do art. 7º, as previsões do art. 11 apresentam variações de redação que apontam sempre para a restrição ao tratamento de *dados sensíveis*, considerados mais valiosos (FALEIROS JR., 2019). Isso é claramente perceptível pelo cotejo entre os permissivos equivalentes de ambos os dispositivos.

A título de ilustração, tem-se que o art. 7º, I, prevê o tratamento "mediante o fornecimento de consentimento pelo titular"; já a base legal correspondente, do art. 11, I, prevê o tratamento "quando o titular ou seu responsável legal consentir, **de forma específica e destacada, para finalidades específicas**". Não é difícil perceber, pelas expressões em destaque, que o legislador procurou ressaltar a maior necessidade de proteção para os dados pessoais.

Ainda dentro dessa categoria, é possível traçar distinções. Para tanto, veja-se como a LGPD conceitua os dados sensíveis:

> Art. 5º (...) II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Da leitura do dispositivo, é possível deduzir três tipos de dados sensíveis, referentes à: (i) crença pessoal (religiosidade, ideologia, sindicalização); (ii) condição psicológica (saúde mental, sexualidade); e (iii) condição biológica (raça, etnia, biometria, genética, saúde física). Essa última categoria é o foco do presente trabalho.

3. SAÚDE PÚBLICA, TRATAMENTO DE DADOS SENSÍVEIS E BIOÉTICA

Uma sociedade que busca o bem comum deve estar ciente de que o coletivo é constituído de inúmeros e diversos particulares. Como a menor parcela desse conjunto, o indivíduo deve ser protegido de maneira especial, sobretudo em sua intimidade.

Evidentemente, tempos singulares demandam medidas diferenciadas. O combate ao novo coronavírus, por exemplo, exige certa relativização de direitos individuais em prol do bem comum, materializado pela saúde pública.

Mesmo assim, trata-se de um equacionamento. Embora seja consenso que, levando em conta o alto grau de potencial infeccioso da doença, seja preciso mitigar direitos, o contexto pandêmico nunca pode ser apanágio para aniquilamento do indivíduo e de suas liberdades.

Por isso, a proteção dos dados pessoais para questões clínicas e para pesquisas se faz elementar, sobretudo quanto aos dados biológicos, biométricos e de saúde. Suas peculiaridades biológicas e psicológicas, bem como suas crenças e valores não podem perder o foro íntimo.

A bioética é a ciência interdisciplinar que estuda a vida e suas formas de tutela, tanto no âmbito individual como no coletivo. Em termos de privacidade, protege a pessoa em sua integralidade e não permite que os interesses e o bem-estar individual sejam subalternos ao interesse exclusivo da ciência e da sociedade, conforme postula a Declaração Universal sobre Bioética e Direitos Humanos, em seu art. 3º, *b*.

3.1 PRIVACIDADE DE DADOS SENSÍVEIS COMO DIREITO HUMANO

Para compreender a bioética, uma das fontes mais relevantes é a Declaração Universal sobre Bioética e Direitos Humanos, segundo a qual: "Os benefícios resultantes de qualquer pesquisa científica e suas

aplicações devem ser compartilhados com a sociedade como um todo e, no âmbito da comunidade internacional, em especial com países em desenvolvimento" (art. 15, *a*, *caput*).

E acrescenta: "Os Estados devem promover a disseminação internacional da informação científica e estimular a livre circulação e o compartilhamento do conhecimento científico e tecnológico." (art. 24, *a*). Logo, obrigam-se a compartilhar informações e conhecimentos com a sociedade e a comunidade internacional, bem como estimular a circulação de dados cientificamente comprovados.

A competitividade para o desenvolvimento de vacina no caso da covid-19 é salutar em termos de celeridade. Não obstante, o avanço científico deve dar-se em pleno respeito à dignidade humana, aos direitos fundamentais e às liberdades individuais. Em decorrência disso, a declaração em comento assegura a privacidade dos indivíduos e a confidencialidade de seus dados (art. 9º). Para tanto, deve ser esclarecido o objetivo do uso das informações e, a depender do propósito, solicitado um termo de consentimento, denominado Termo de Consentimento Livre e Esclarecido (TCLE).

Há quem defenda não haver necessidade de escolha entre os direitos da privacidade e o da saúde (OPICE BLUM, 2020, p. 5). Evidentemente, pelo critério da proporcionalidade, mesmo nas chamadas "circunstâncias extraordinárias", um não anula o outro. A balança da justiça ora cede para um lado, ora para o outro, mas ambos coexistem em plena harmonia.

A concessão do uso de dados privados é uma decisão de foro íntimo e particular e, por isso, livre e esclarecida, para se aprimorar a própria saúde, no âmbito pessoal, e, também, com base na solidariedade, no coletivo.

3.2 PRIVACIDADE DE DADOS SENSÍVEIS E BIOÉTICA

Os dados pessoais sensíveis são, em conjunto, aquilo que individualiza a pessoa em meio à sociedade. É notável saber que, mesmo numa consideração do bem comum, que elimina o protagonismo do indivíduo, este vem a ser a menor célula a compor um grupo.

A filosofia e a sociologia se preocupam em conceituar o termo "indivíduo" por meio de inúmeras figuras linguísticas. A esse respeito, o grupo de comédia britânico Monty Python propõe, no filme *A Vida de Brian*, uma cena peculiar. O herói tenta convencer seu grupo de seguidores de que cada um deles é singular e, por isso, todos tinham de ser diferentes. A essa incitação o grupo respondia, em uníssono, que eram indivíduos e diferentes, exceto por uma voz inoportuna que a todos incomodava: "Eu não sou..." (BAUMAN, 2007, p. 25).

Não obstante o paradoxo filosófico da individualidade, o termo é de eminente relevância no campo biológico. Há traços personalíssimos que distinguem as pessoas e, por tornarem acessível o campo privado, devem ser protegidos. Trata-se, como mencionado alhures, das crenças religiosa e política, da sexualidade, da etnia etc.

Na condição pessoal biológica, os dados pessoais se afunilam para distinguirem um ser ímpar em meio a semelhantes. No tocante à etnia, terá determinada nacionalidade, naturalidade e ascendência. Quanto à biometria, existirão diferentes desenhos papilares e características faciais. Relativamente à genética, o DNA individual se constituirá numa peculiar e irrepetível sequência. No que se refere à saúde física, haverá uma relação única médico-paciente e não mera padronização da doença. Neste caso, dar-se-á maior ênfase quando tratada especificamente da proteção de dados na pandemia da covid-19.

> Numa sociedade de indivíduos, cada um *deve* ser um indivíduo. A esse respeito, pelo menos, os membros dessa sociedade são tudo

> menos indivíduos diferentes e únicos. São, pelo contrário, estritamente *semelhantes* a todos os outros pelo fato de terem de seguir a mesma estratégia de vida e usar símbolos comuns – comumente reconhecíveis e legíveis – para convencerem os outros de que assim estão fazendo. (BAUMAN, 2007, p. 26)

A proposta de Bauman refere-se à subjetividade. Ocorre que o fato se verifica igualmente na esfera biológica: dentro de uma sociedade de semelhantes (ou iguais perante a lei), há necessidade de individualização. A similaridade se justifica sob os critérios biológico, social, cultural, político, familiar etc. O *homo sapiens* pertence a determinado lugar geográfico, onde habita um povo, que conjuntamente se organiza e administra. Não obstante, a regra da justa medida impõe a diferenciação: "a regra da igualdade não consiste senão em aquinhoar desigualmente aos desiguais, na medida em que se desigualam" (BARBOSA, 2009, p. 35).

Para o exercício de direitos civis e igualmente para a persecução criminal, é indispensável a diferenciação. A credibilidade da administração pública e privada está em garantir a segurança nas transações bancárias, a eficiência em identificar a autoria delitiva, o sigilo e a universalidade da participação eleitoral ativa etc. Nesse sentido, são explorados mecanismos como os desenhos papilares.

> Os diferentes desenhos das papilas contribuem para a importância das características, que são: Unicidade – não existem dois indivíduos diferentes com impressões idênticas; Imutabilidade – a característica da impressão se mantém igual desde o nascimento até a decomposição após a morte; Praticabilidade – os desenhos papilares podem ser obtidos com grande facilidade e rapidez; Classificabilidade – os desenhos papilares, apesar de sua infinita variedade nas minúcias, atendem a um limitado número de tipos fundamentais, tornando possível classificá-los. (BELANDA; CAVALCANTI, 2006, p. 6)

Os desenhos das papilas, no entanto, são insuficientes. Primeiro, por já existirem tecnologias desenvolvidas com maior confiabilidade; segundo, porque a imutabilidade é relativa, uma vez que há desgaste com o passar dos anos e com determinadas práticas profissionais.

Outro critério consiste no material genético, protegido pela Lei de Biossegurança (Lei n. 11.105/2005) e pela Constituição Federal. A primeira cria um Sistema de Informações em Biossegurança (SIB) e estabelece responsabilidades civis e penais para a construção, o cultivo, a manipulação, o transporte, a transferência, a importação, a exportação, o armazenamento, a pesquisa, a comercialização, o consumo, a liberação no meio ambiente e o descarte de organismos geneticamente modificados (OGM) e seus derivados. Preocupa-se, outrossim, com o avanço científico da biotecnologia e a proteção da vida e da saúde humanas.

3.3 PRIVACIDADE DE DADOS SENSÍVEIS E SAÚDE PÚBLICA

No âmbito da proteção de dados, encontra-se o direito à privacidade. Contudo, tais informações podem ser elementares ao combate contra diversas enfermidades, de modo particular no contexto atual de pandemia causada por um vírus até então desconhecido pela ciência.

Os estudos se dão em âmbito clínico (diagnóstico e tratamento) e laboratoriais (desenvolvimento de vacinas, medicamentos etc.). A eficácia do estudo está em função das informações e dos conhecimentos obtidos a partir de dados reais e pessoais.

> Pouco conhecido para as pessoas que não fazem parte deste meio, os estudos clínicos são considerados como um dos mais importantes mecanismos no combate e prevenção de doenças, consistindo na realização de testes envolvendo seres humanos, que visam experimentar

> a eficácia, eficiência e segurança de novos medicamentos, vacinas e demais procedimentos da área da saúde. (OPICE BLUM, 2020, p. 10-11)

Diante da necessidade de contribuição individual para o combate ao novo coronavírus, doença altamente infecciosa que ultrapassa a mera coletividade por adquirir uma dimensão global, faz-se necessário resguardar o direito à privacidade, com a proteção de dados pessoais biológicos.

Nesse sentido, garante-se que o exame clínico se dê em local privado, sem exposição do corpo do paciente. Este pode consentir ou recusar o tratamento, bem como o atendimento por via digital, além de ter o direito ao conhecimento de medidas alternativas e menos intrusivas. A ele é assegurada a participação nos processos deliberativos e a proteção das informações pessoais, arquivadas de modo confidencial e sigiloso, com processamento e compartilhamento restringidos a fins específicos, sem obrigatoriedade de identificação pessoal.

Noutro aspecto de proteção da privacidade, está o uso de tecnologias hábeis a rastrear e mesmo identificar pessoas em busca de informações quanto à adesão às políticas de isolamento social:

> No que diz respeito à utilização de ferramentas de Inteligência Artificial (IA) ou *Big Data* (tais como geolocalização, reconhecimento facial, aplicativos que permitem rastrear pessoas infectadas por Covid-19), os órgãos citados esclarecem que o processamento de dados pessoais em larga escala somente poderá ser realizado se, fundamentado em evidências científicas, os possíveis benefícios à saúde pública dessa vigilância epidêmica digital substituírem os benefícios de outras soluções alternativas menos intrusivas. Além disso, recomendam a adoção de medidas legais adicionais, a fim de prevenir o uso inadequado dos dados dos pacientes com Covid-19 e o surgimento de consequências negativas, incluindo-se formas acentuadas de discriminação dessas pessoas. (UNB, 2020, p. 13)

A mitigação da proteção de dados pessoais tem de ser justificada por um bem de ordem mais elevada no caso concreto, como a saúde pública em um contexto de doença altamente infecciosa. Em hipótese alguma, pode o Estado, alegando essa finalidade, exceder-se e abusar no seu poder, o qual deve vir sempre acompanhado do dever de tutela para com seu cidadão.

Ainda, aquele que participa de pesquisas voluntariamente tem igual direito à proteção de seus dados pessoais. Convém mencionar que a adesão a esse procedimento deve ser consentida, podendo, inclusive, ser retirada sem qualquer ônus, mesmo após a assinatura do TCLE. Do mesmo modo, os dados pessoais precisam ser protegidos sempre que possível. Além disso, todas as informações a respeito do manuseio e compartilhamento de dados biológicos têm de ser esclarecidas ao participante. Este deve, enfim, ter acesso a eventuais benefícios decorrentes da pesquisa para a qual contribuiu (UNB, 2020, p. 32-34).

É necessário o zelo atento do Direito para que o Estado e as organizações internacionais não incorram em falta nem abuso na proteção do indivíduo e da coletividade a que ele pertence.

4. CONCLUSÃO

Tudo que adentra a esfera privada do indivíduo, especialmente aquilo que o distingue dos demais – o *individualiza* –, deve ser tutelado, sobretudo, neste cenário de pós-modernidade. Daí extrai-se a demasiada importância da LGPD, pois o respeito à individualidade se inicia no leito de um hospital e estende-se, com a mesma intensidade pandêmica, por todos os continentes.

A tecnologia e a biotecnologia trouxeram muitos benefícios que podem e devem ser usados como ferramentas para oferecer eficácia a todos os tipos de questões sociais, políticas, econômicas e, atualmente,

pandêmicas. Seu uso pode tornar mais célere e aprimorado o processo de combate ao novo coronavírus, em especial por permitir o compartilhamento de informações em escala global. No entanto, é elementar que a tecnociência seja usada em prol do bem comum e não venha a aniquilar o indivíduo.

REFERÊNCIAS

BARBOSA, Ruy. *Oração aos moços*. Bauru, São Paulo: Edipro, 2009.

BAUMAN, Zygmunt. *Vida líquida*. Rio de Janeiro: Jorge Zahar, 2007.

BELANDA, Douglas; CAVALCANTI, Ana Elizabeth L. W. Biometria como mecanismo de formação e prova contratual: um olhar para as transações eletrônicas bancárias na sociedade da informação. *Revista dos Tribunais*, v. 1016, jun. 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. São Paulo: Renovar, 2006.

FALEIROS JR., José L. A tutela jurídica dos dados pessoais sensíveis à luz da Lei Geral de Proteção de Dados. *In*: LONGHI, João V. R.; FALEIROS JR., José L. (Coords.) *Estudos essenciais de direito digital*. Uberlândia: LAECC, 2020. *E-book*.

JARA, Arquimedes Alez. *Privacidade dos dados genéticos humanos armazenados em biobancos de pesquisas*: uma análise da proteção jurídica no Brasil à luz dos Direitos Humanos. 2019. Dissertação (Mestrado) Faculdade de Direito e Relações Internacionais, Universidade Federal da Grande Dourados, Dourados, MS, 2019. Disponível em: https://bit.ly/3deuV5m. Acesso em: 21 jun. 2020.

LADEIA, Yuri Rodrigues. Internet das coisas – IOT – e privacidade de dados: desafios técnicos, jurídicos e operacionais para o *compliance*. *Migalhas*, 2019. Disponível em: https://bit.ly/2XUcTAN. Acesso em: 21 out. 2019.

MACHADO, Ronny M.; FUJITA, Jorge S. Os impactos da sociedade da informação no direito à privacidade da pessoa natural e da pessoa jurídica. *Thesis Juris*, São Paulo, v. 7, n. 2, 2018. Disponível em: https://bit.ly/3dWoJzV. Acesso em: 21 out. 2019.

MALDONADO, Viviane (Coord.). *LGPD*: manual de implementação. São Paulo: Revista dos Tribunais, 2019.

NEGRI, Sergio M. C.; KORKMAZ, Maria Regina D. C. R. A normatividade dos dados sensíveis na Lei Geral de Proteção de Dados: ampliação conceitual e proteção da pessoa humana. *Revista de direito, governança e novas tecnologias.* Disponível em: https://bit.ly/310eNC1. Acesso em: 21 jun. 2020.

ONU. *Declaração Universal dos Direitos Humanos*. Adotada e proclamada pela Resolução n. 217 A (III) da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Assinada pelo Brasil na mesma data. Disponível em: https://bit.ly/2FAPLRv. Acesso em: 16 set. 2020.

ONU. *Declaração Universal sobre Bioética e Direitos Humanos*. Adotada por aclamação em 19 de outubro de 2005 pela 33. Sessão da Conferência Geral da Unesco em Paris. Disponível em: https://bit.ly/2Rrj4bA. Acesso em: 15 set. 2020.

OPICE BLUM. *Proteção de dados na saúde*. São Paulo, abr. 2020. Disponível em: https://28563dcd-7409-4c91-96aa-c236d9f0a871.usrfiles.com/ugd/28563d_4dbd214a0d174d37a4fcd554975b031a.pdf. Acesso em: 9 dez. 2020.

RODOTÁ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. São Paulo: Renovar, 2008.

SALDANHA, Jânia Maria Lopez; BRUM, Márcio Morais; MELLO, Rafaela da Cruz. As novas tecnologias da informação e comunicação entre a promessa de liberdade e o risco de controle total: estudo da jurisprudência do sistema interamericano de direitos humanos. *Anuário Mexicano de Derecho Internacional*, México, v. 16, 2016. Disponível em: https://www.sciencedirect.com/science/article/pii/S1870465417300144. Acesso em: 21 out. 2019.

SANTANA, Célia M. M. de; ABDALLA-FILHO, Elias. Banco nacional de perfis genéticos criminal: uma discussão bioética. *Revista Brasileira de Bioética*, v. 8, n. 1-4, 2012. Disponível em: https://bit.ly/380bcWd. Acesso em: 21 jun. 2020.

SANTOS, Aline F. dos *et al*. Dados sensíveis na era da informação: análise dos programas de desconto de medicamentos no Brasil. *In*: BARROS, Guilherme S. B. (Org.). *Coleção Jovem Jurista*. Rio de Janeiro: Escola de Direito FGV Direito Rio, 2012, p. 267-314. Disponível em: https://bit.ly/2YYw3oq. Acesso em: 21 jun. 2020.

SARLET, Gabrielle B. S.; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. *Civilistica.com*, v. 8, n. 1, 2019. Disponível em: https://bit.ly/3ekvITv. Acesso em: 21 jun. 2020.

SOARES, Matias Gonsales. A Quarta Revolução Industrial e seus possíveis efeitos no direito, economia e política. *Migalhas*, 2018. Disponível em: https://bit.ly/37tfIvV. Acesso em: 21 out. 2019.

UENO. *GDPR em português*. Disponível em: https://bit.ly/2ToJsVp. Acesso em: 4 mar. 2020.

UNB. OPAS. *Direitos humanos dos pacientes e covid-19*. Brasília, 2020.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. *Ciência da Informação.* Brasília, v. 29, n. 2, 2000. Disponível em: https://bit.ly/37qV1AH. Acesso em: 21 out. 2019.

O DIREITO AO ESQUECIMENTO E A PROTEÇÃO DE DADOS: DADOS DE CONSULTA NAS AÇÕES DE IMPROBIDADE ADMINISTRATIVA

Robson Martins[1]
Mário Lúcio Garcez Calil[2]
Erika Silvana Saquetti Martins[3]

RESUMO

O presente trabalho visa estudar a incidência do direito fundamental ao esquecimento, relativamente a acordos de não persecução cível em ações de improbidade, no contexto de proteção de dados. Para concretizar esse objetivo, serão utilizados o método dedutivo e os procedimentos bibliográfico e documental. O estudo se justifica pela necessidade de se concretizarem todos os direitos fundamentais, mesmo aqueles que não se encontram expressos na Constituição de 1988, sobretudo os atinen-

1 Doutorando em Direito pela Faculdade de Direito de Bauru (CEUB-ITE). Procurador da República no Paraná.
2 Pós-doutorando (Bolsista PDJ-CNPQ) pela Fundação de Ensino Eurípides Soares da Rocha. Professor Associado V da Universidade Estadual de Mato Grosso do Sul.
3 Mestranda na área de Estado, Poder e Jurisdição pela Uninter. Advogada em Curitiba.

tes à personalidade e dignidade. Concluiu-se que, embora necessária a disponibilização de informações acerca do passado de agentes públicos, a manutenção de um banco de dados constituído de acordos de não persecução cível cumpridos inutiliza o direito fundamental ao esquecimento.

Palavras-chave: Direito fundamental ao esquecimento. Acordo de não persecução cível. Consulta CNJ. Ações de improbidade administrativa.

ABSTRACT

This study aims to study the incidence of the fundamental right to forget the civil non-persecution agreement in actions of improbity, in the context of data protection. The deductive method and bibliographic and documentary procedures will be used. The study is justified in view of the need to realize all fundamental rights, even those that are not expressed in the 1988 Constitution, especially those related to personality and dignity. It was concluded that, in spite of the need to provide information about the past of public agents, the maintenance of a database that provides fulfilled civil non-persecution agreements disables the fundamental right to be forgotten.

Keywords: Fundamental right to forgetfulness. Civil non-pursuit agreement. Consultation CNJ. Administrative improbity actions.

1. INTRODUÇÃO

O objetivo deste artigo é estudar a incidência do direito fundamental ao esquecimento, relativamente a acordos de não persecução cível em ações de improbidade, no contexto da proteção de dados. Para embasar a discussão, adotamos o método dedutivo e os procedimentos bibliográfico e documental.

A pesquisa será dividida em três partes. Na primeira, analisaremos o direito ao esquecimento e sua relação com a proteção de dados, enquanto direito da personalidade. Para tanto, serão comparadas as perspectivas brasileira e europeia, além de examinado o Enunciado n. 531 da IV Jornada de Direito Civil do Conselho da Justiça Federal (CJF).

Na segunda parte, enfocaremos o direito ao esquecimento no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD), a partir do chamado *princípio da autodeterminação informativa* e do entendimento do Superior Tribunal de Justiça (STJ) relacionado à temática em voga.

Por fim, abordaremos o direito ao esquecimento no contexto do acordo de não persecução cível quanto às ações de improbidade administrativa, em contraposição ao teor da Resolução Conjunta n. 6, de 21 de maio de 2020, do Conselho Nacional de Justiça (CNJ).

Justifica-se o estudo ora apresentado ante a necessidade de se concretizarem os direitos fundamentais, mesmo os não expressos na Constituição Federal de 1988, sobretudo no que concerne àqueles diretamente atinentes à personalidade e à dignidade.

Apesar da necessidade de informar os potenciais eleitores sobre o passado de agentes públicos, a manutenção de um banco de dados que disponibilize acordos de não persecução cível efetivamente cumpridos fere o direito fundamental ao esquecimento.

2. O DIREITO AO ESQUECIMENTO E A PROTEÇÃO DE DADOS

No presente tópico, analisaremos o denominado direito ao esquecimento e sua relação com a proteção de dados, enquanto direito da personalidade. Para isso, serão examinadas a perspectiva brasileira e a europeia, assim como o Enunciado n. 531 da IV Jornada de Direito Civil do Conselho da Justiça Federal.

2.1 O DIREITO AO ESQUECIMENTO COMO DIREITO DA PERSONALIDADE

Os direitos fundamentais, especialmente aqueles relacionados à personalidade e dignidade, encontram-se em permanente evolução, fato que determina a criação constante de garantias, surgidas em decorrência das novas necessidades humanas identificadas com o passar do tempo.

Segundo Bobbio (2004, p. 5), a multiplicação de direitos ocorre devido à (i) crescente quantidade de bens jurídicos tuteláveis na sociedade complexa; (ii) extensão da titularidade de alguns deles a sujeitos diversos do homem; e (iii) mudança de perspectiva em relação ao próprio homem, agora visto não como ente genérico ou abstrato, mas como ser repleto de especificidades. Todos esses processos são interdependentes, uma vez que a multiplicação dos direitos do homem explicita a necessidade de se observar um contexto social determinado.

Desse modo, é possível considerar que o direito ao esquecimento surgiu como garantia contra o Estado, de modo a preservar a dignidade das pessoas expostas em decorrência dos mais diversos motivos, pelo poder público, pela imprensa e, mais atualmente, pelas redes sociais cibernéticas. Nesse viés, não se restringe aos conflitos entre os direitos da personalidade e a liberdade de expressão ou de imprensa, pois seu surgimento se relaciona a casos nos quais alguém tenta impedir a exploração de fatos constrangedores ocorridos há certo tempo e que deveriam ser esquecidos (MOREIRA; ALVES, 2015, p. 95).

O direito ao esquecimento foi expandido para a proteção do consumidor, o sigilo dos dados eletrônicos e a garantia de "um novo começo para aquelas pessoas que resolvem mudar o seu plano existencial, alterando ou adequando a sua identidade pessoal como é o caso do transexual" (MOREIRA; ALVES, 2015, p. 95). Faz referência direta, portanto, à personalidade individual e ao seu resguardo quanto à superação jurídica e social de situações pretéritas não mais existentes ou de imputações jurídicas que deixaram de surtir seus efeitos ao longo do tempo.

2.2 O DIREITO EUROPEU

A comunidade europeia foi um dos primeiros organismos internacionais a formular, de maneira efetiva, um verdadeiro direito ao esquecimento, bem como a delimitar procedimentos voltados a sua concretização no mundo dos fatos, especificamente no contexto da internet.

Com uma abordagem inovadora, a Europa, por meio de suas diretivas e leis de proteção de dados, entende que, se as pessoas têm direito à privacidade, esta deve estender-se às informações sobre elas. Assim, as leis europeias visam assegurar também a integridade de informações sobre os indivíduos. Desse modo, se uma agência de pontuação de crédito tiver informações incorretas, é possível exigir legalmente a correção. No Reino Unido, em particular, sob a Lei de Reabilitação de Infratores, determinou-se a desnecessidade, após certo tempo, de serem mencionadas as condenações criminais já cumpridas. Apesar disso, a possibilidade de se resgatarem informações antigas ainda é um problema, pois ainda causa prejuízo àqueles que estão à procura de emprego. Na França, para situações desse tipo, há *le droit d'oubli*, ou "o direito de ser esquecido" (ARTHUR, 2014).

Diante desse contexto, a União Europeia (UE) compreende que o direito ao esquecimento é, especialmente, uma garantia do indivíduo contra o Estado, por intermédio do qual o cidadão passa a ter sua reputação protegida, mesmo após uma condenação criminal, desde que essa tenha sido cumprida. Sob essa perspectiva, a Diretiva Europeia n. 95/46/CE estabeleceu a proteção dos dados tanto no setor público quanto no privado. A norma defende que a salvaguarda dos dados deve ser parte das políticas públicas, referindo-se às informações pessoais vinculadas à pessoa singular identificada ou identificável (MENDES, 2014, p. 56).

Tal direito, contudo, sofre limitações quanto à existência de condições de efetivação (MENDES, 2014, p. 56), sobretudo no que se relaciona aos diversos e potentes instrumentos de busca presentes na internet,

a exemplo do próprio *Google Search*. Por isso, a desindexação de *links* na rede foi a forma escolhida pela Comunidade Europeia para garantir a autodeterminação informativa. Desse modo, procura agir sobre os resultados de pesquisa apresentados por motores de busca, apagando o elo entre a informação e o terceiro interessado (ACIOLI, 2017, p. 358).

Destarte, o Direito comunitário europeu entende que, para a concretização do direito ao esquecimento na internet, é possível determinar a desvinculação do nome da pessoa titular dessa garantia. Tal medida visa dificultar a procura pela relação do nome do indivíduo com o fato que se deseja fazer cair no ostracismo.

2.3 O ENUNCIADO N. 531 DO CJF

Para além de sua evidente dimensão constitucional, os direitos da personalidade são uma preocupação central do direito civil pátrio, tendo em vista sua proximidade direta com a vida dos indivíduos. Essa é a razão pela qual vários deles se encontram regulamentados pelo Código Civil.

Nesse sentido, na VI Jornada de Direito Civil do CJF, foi elaborado o Enunciado n. 531, vinculado ao art. 11 do Código Civil, cujo conteúdo afirma que "a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento".

Além disso, elaborado sob a justificativa de que, em decorrência dos danos gerados pelas tecnologias de informação, o direito ao esquecimento é parte importante do direito à ressocialização, o diploma assegura a possibilidade de se discutir o uso de dados quando esses estiverem relacionados a fatos passados, desatualizados. Em que pese a amplitude do enunciado, uma vez que se remete à dignidade humana, nota-se que sua motivação fez direta referência à proteção de dados intercambiáveis por meio da internet, sobre ela fazendo incidir o direito ao esquecimento.

Ainda, o Enunciado n. 531 concluiu ser incabível uma condenação eterna ao cidadão que tenha cumprido pena. Essa impossibilidade se deve, sobretudo, à própria Constituição Federal, que veda sanções de caráter perpétuo, de modo que os registros condenatórios não podem permanecer além do tempo da punição (EHRHARDT JR.; NUNES; PORTO, 2017, p. 65), sob risco de ultrapassar o mandamento legal sobre o qual se baseou.

Desse modo, o direito ao esquecimento é plenamente aplicável após o esgotamento dos objetivos de uma condenação. Mostra-se lógico determinar-se, em seguida, a desnecessidade de se manter o nome do apenado eternamente vinculado a uma decisão judicial pretérita, despersonalizando-o e, consequentemente, relativizando sua dignidade.

3. O DIREITO AO ESQUECIMENTO E A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Neste item examinaremos o direito ao esquecimento no contexto da LGPD, a partir do denominado princípio da autodeterminação informativa, bem como o entendimento do STJ acerca da referida temática.

3.1 O DIREITO FUNDAMENTAL À AUTODETERMINAÇÃO INFORMATIVA NA LGPD

No Brasil, o direito ao esquecimento é diretamente retirado da necessária proteção à dignidade da pessoa humana, encontrando-se dimensionado na própria personalidade do indivíduo como ser humano. Situação similar ocorre na Alemanha.

Em 1977, o Parlamento alemão aprovou a lei federal de proteção de dados (*Bundesdatenschutzgesetz*), estabelecendo o *direito fundamental à autodeterminação informativa* (*Grundrecht auf informationelle Selbstbestimmung*), o qual possibilitou que o indivíduo se insurgisse em face de

representações inverídicas, não autorizadas, degradantes ou deturpadas a seu respeito.[4] Além disso, garante a proteção contra observações secretas e indesejadas acerca de sua personalidade, por exemplo, em relação aos direitos à imagem, à palavra escrita e falada, à escuta clandestina e ao monitoramento por vídeo em locais públicos. Consagra, também, ao indivíduo o poder de decidir acerca de sua utilização (MENKE, 2015, p. 207).

A autodeterminação informativa complementa a proteção constitucional da liberdade comportamental e da privacidade. Não se encontra limitada, no entanto, às chamadas *informações sensíveis*; abarca, também, o contato com dados pessoais. Somado a isso, compreende as possibilidades de tratamento e associação que influenciem a privacidade e a liberdade do indivíduo, protegendo informações consideradas individual ou conjuntamente, contra o contato de terceiros (MENKE, 2015, p. 207).

Esse princípio valoriza a posição do indivíduo em decorrência da escolha sobre a divulgação de seus dados, mas não permite o domínio absoluto. Em 2008, contudo, o Tribunal Constitucional Federal alemão modernizou o conceito de autodeterminação informativa para assegurar a confidencialidade e integridade no contexto dos sistemas técnico-informacionais, destacando "a migração das relações sociais e a condução da vida do indivíduo para o ambiente técnico-informacional" (MENKE, 2015, p. 208).

A LGPD – Lei n. 13.709 –, sancionada em 2018 pelo Congresso Nacional brasileiro, acabou por consagrar algo similar ao *direito fundamental à autodeterminação informativa*, tendo em vista que alguns de seus preceitos remetem diretamente à proteção à personalidade e à dignidade dos indivíduos.

---

4 O ápice do reconhecimento dessa salvaguarda ocorreu na decisão do Tribunal Constitucional Federal sobre o censo demográfico realizado no país, em 1983 (*Volkszählungsurteil*) (MENKE, 2015, p. 207).

Nesse sentido, dispõe no art. 2º:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I – o respeito à privacidade;
>
> (...)
>
> IV – a inviolabilidade da intimidade, da honra e da imagem;
>
> (...)
>
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Outrossim, a proteção de dados compreende aspectos essenciais do direito fundamental ao esquecimento, de maneira que este deve ser aplicado, também, ao ambiente virtual, sobretudo para proibir o acesso a informações relacionadas a fatos pretéritos cuja utilidade já se esvaiu.

3.2 O ENTENDIMENTO DO STJ

O reconhecimento, no Brasil, do direito fundamental ao esquecimento não é recente. O STJ há muito entende pela sua incidência, especialmente no que se relaciona às condenações cujas penas já foram integralmente cumpridas ou até mesmo em pesquisas efetivadas na internet de fatos deletérios à vida do cidadão.

Em 2013, o Tribunal consagrou o direito ao esquecimento relativamente a notícias veiculadas na televisão referentes a pessoas que cumpriram sua condenação ou foram absolvidas. Entendeu-se à época que a dignidade humana atua como limitadora do direito à informação (BRASIL, STJ, 2013, n.p.). Quanto a esse aspecto, o ministro Luis Felipe Salomão, no exame do Recurso Especial (REsp) n. 1.334.097/RJ, consignou que o reconhecimento do direito ao esquecimento, nesses casos, sinaliza a

evolução cultural da sociedade, a concretizar um ordenamento jurídico que opta pela esperança em vez da memória. Nesse sentido, relaciona-se diretamente à garantia fundamental representada pela proibição de imposição de penas perpétuas, determinando, assim, que os efeitos de uma pena não podem incidir eternamente sobre a existência do condenado.

Essa óptica, também apresentada em outros julgados da Corte, acabou por apontar a necessidade de se definirem *marcos temporais* acerca da *vida útil da informação criminal* e de se restringir a publicidade daquela *ainda em trâmite*. Surge daí o primeiro obstáculo quanto aos bancos de dados jurisprudenciais. Esses necessitam de atualização contínua para a exclusão de decisões do repositório ou, ainda, de outra estratégia que garanta o anonimato das partes (MARTINS NETO; PINHEIRO, 2014, p. 825-826), de modo a impedir a penalização perpétua, mesmo que por via oblíqua.

Em 2016, o STJ entendeu que o direito ao esquecimento equivale ao "de não ser lembrado contra sua vontade, especificamente no tocante a fatos desabonadores, de natureza criminal, nos quais se envolveu, mas que, posteriormente, fora inocentado" (BRASIL, 2016, n.p.). No caso, o Tribunal ainda não se havia pronunciado acerca do procedimento voltado à efetivação das decisões garantidoras do direito fundamental ao esquecimento, especialmente quanto às informações contidas e difundidas em ambiente virtual.

Já em 2018, entendeu pela existência de uma "via conciliadora do livre acesso à informação e do legítimo interesse individual, porque não serão excluídos da busca referências ao nome da recorrida", nem serão ocultados resultados advindos de uma busca referente a seu nome. Ressaltou, entretanto, a necessidade de se evitar que "uma busca direcionada a informações sobre a sua pessoa, por meio da inclusão de seu nome como critério exclusivo de busca, tenha por resultado a indicação do fato desabonador noticiado há uma década, impedindo a superação daquele momento" (BRASIL, STJ, 2018, n.p.).

Tal decisão, assim, se encontra em desacordo com o entendimento da União Europeia acerca do tema. Além disso, ocorreu antes da entrada em vigor da LGPD, de maneira que a jurisprudência do STJ deve adaptar-se às referidas premissas.

4. O DIREITO AO ESQUECIMENTO E O ACORDO DE NÃO PERSECUÇÃO CÍVEL

O objetivo do presente tópico é tratar do direito ao esquecimento no contexto do acordo de não persecução cível em relação às ações de improbidade administrativa, em contraposição à Resolução Conjunta n. 6, de 21 de maio de 2020, do CNJ.

4.1 O ACORDO DE NÃO PERSECUÇÃO CÍVEL

No que concerne à *administração pública consensual* e às formas pacíficas de solução de conflitos, vários projetos de lei surgiram em ambas as Casas do Legislativo federal, determinados a permitir a transação em ações de improbidade administrativa, mediante certos requisitos de indispensável cumprimento.

O Projeto de Lei n. 10.887/2018 da Câmara dos Deputados propôs que a celebração de acordo deveria considerar a personalidade do agente, a natureza, a circunstância, a gravidade e a repercussão social do ato de improbidade, de acordo com o que consta do art. 17-A, § 2º.

O Senado, por sua vez, por meio do Projeto de Lei n. 3.359/2019, prevê a redução proporcional à espécie do ato de improbidade administrativa praticado – enriquecimento ilícito, dano ao erário ou violação aos princípios –, bem como outras circunstâncias fáticas, no art. 17-A, § 1º, II.

Após a Lei n. 13.964/2019 (denominada "pacote anticrime"), o art. 17, § 1º, da Lei de Improbidade Administrativa passou a afirmar

que: "as ações de que trata este artigo admitem a celebração de acordo de não persecução cível, nos termos desta Lei". Seu § 10-A possibilita requerer ao juiz a interrupção do prazo para contestação, por período "não superior a 90 (noventa) dias".

Mais do que isso, a expressão "havendo a possibilidade de solução consensual", sem referência ao "acordo de não persecução cível", "poderia indiciar que outras ferramentas de obtenção de consenso poderiam ser cabíveis" (PINHO, 2020, p. 154-155).

Trata-se, portanto, de instrumento voltado a permitir que o acusado da prática de ato de improbidade deixe de ser acionado, mediante acordo homologado judicialmente, dirigido à eliminação do referido evento pretérito. Com isso, favorece que ele dê prosseguimento a sua vida.

4.2 A RESOLUÇÃO CONJUNTA N. 6, DE 21 DE MAIO DE 2020, DO CNJ

As condenações por atos de improbidade devem ser disponibilizadas para consulta, especialmente em decorrência do direito fundamental à segurança jurídica, bem como da necessidade de se assegurar aos potenciais eleitores o conhecimento acerca da conduta ímproba de um candidato ou mesmo de um servidor público.

Nesse sentido, a Resolução Conjunta n. 6/2020 do CNJ (BRASIL, 2020, n.p.) instituiu uma "sistemática unificada para o envio, no âmbito do Poder Judiciário, de informações referentes a condenações por improbidade administrativa e a outras situações que impactem no gozo dos direitos políticos". Estas serão objeto de compartilhamento entre o CNJ e o Tribunal Superior Eleitoral, relacionadas, inclusive, a "acordos de não persecução cível relativos à improbidade administrativa" e "cumprimentos de sanções e termos de acordo de improbidade administrativa".

Desse modo, além das condenações por improbidade administrativa, a referida resolução define que o banco de dados compreenda

os acordos de não persecução cível. Ocorre que essa determinação é capaz de esvaziar os objetivos do citado instituto, deixando-o à mercê de interpretações dúbias.

No Brasil, não é possível que um controlador de dados mantenha o acesso às informações pessoais que lhe foram entregues, depois de esgotadas suas finalidades, sem garantir o anonimato e a vedação de acesso por terceiros, salvo nos casos de obrigações legais *stricto sensu*, uma vez que, após o trânsito em julgado, o processo já perde sua finalidade (OCKE; SANTOS, 2020, p. 79). O mesmo entendimento é válido para o acordo de não persecução cível que, caso cumprido integralmente, deve resultar no encerramento de qualquer punibilidade relacionada à conduta ímproba.

Por conseguinte, apesar da necessidade de tornar acessível informações sobre o passado de agentes públicos, especialmente a seus potenciais eleitores, a manutenção de um banco de dados que disponibilize acordos de não persecução cível cumpridos fere de morte o direito fundamental ao esquecimento. Nesse prisma, verifica-se que há necessidade clara de reformulação das consultas públicas a atos de improbidade, tanto referentes a ações com trânsito em julgado quanto a casos de efetivação do acordo de não persecução cível. Busca-se, assim, garantir a dignidade da pessoa humana aos cidadãos que foram objeto de ação de improbidade administrativa. Ademais, mesmo em condenações por atos de improbidade, a consulta pública precisa ter prazo predeterminado para ficar disponível, de modo a se evitar uma pena perpétua.

5. CONCLUSÃO

Os direitos fundamentais relacionados à personalidade e à dignidade se encontram em permanente evolução, determinando a criação de garantias decorrentes de novas necessidades. Nesse contexto, o direito

ao esquecimento surgiu como garantia contra o Estado a preservar a dignidade da pessoa humana, remetendo-se à personalidade individual e ao seu resguardo quanto à superação de situações pretéritas.

Em relação a esse preceito, a comunidade europeia foi um dos primeiros organismos internacionais a formulá-lo e a delimitar procedimentos para sua concretização no contexto da internet. A UE compreende que o direito ao esquecimento é uma segurança do indivíduo contra o Estado, relacionado à proteção de sua privacidade e, especificamente, de sua reputação, incidindo, notadamente, quanto às pesquisas feitas na internet. Nesse contexto, determina-se a desvinculação do nome da pessoa em relação aos motores de busca, precipuamente na rede mundial de computadores.

Além de sua dimensão constitucional, os direitos da personalidade são uma preocupação central do direito civil. Nesse sentido, é reconhecido pelo Enunciado n. 531 do CJF, o qual faz expressa menção à internet e à proteção de dados eletrônicos, especificamente no que se relaciona às condenações que já perderam seus efeitos, tornando desnecessária a vinculação do nome do indivíduo a uma decisão que perdeu sua razão de ser. Demonstra-se, assim, a relação com um *direito fundamental à autodeterminação informativa*, amplamente reconhecido pelo Tribunal Constitucional Federal da Alemanha e, mais recentemente, pela LGPD.

No Brasil, apesar de o reconhecimento desse direito fundamental não ser recente, o STJ não tem decidido pela necessária desvinculação do nome do indivíduo do fato a ser esquecido, encontrando-se em desacordo com o entendimento da UE sobre a temática. Vale realçar, quanto a isso, que tais pronunciamentos ocorreram antes da entrada em vigor da LGPD.

O acordo de não persecução cível é instrumento destinado a possibilitar que o acusado da prática de ato de improbidade não seja efetivamente acionado perante o Poder Judiciário, mediante termo homologado judicialmente. Visa, assim, a eliminar o evento pretérito e a permitir que o indivíduo prossiga com sua existência.

As condenações efetivas e transitadas em julgado por atos de improbidade devem ser disponibilizadas ao público em geral, informando aos potenciais eleitores o conhecimento sobre a conduta do candidato e do servidor público. Ocorre que a Resolução Conjunta n. 6, de 21 de maio de 2020, do CNJ determina que os acordos de não persecução devem constar de um banco de dados próprio.

Essa determinação, entretanto, além de esvaziar os objetivos do referido instituto, cujo cumprimento integral deve levar ao encerramento da punibilidade relacionada à conduta ímproba, fere de morte um relevante aspecto do direito fundamental ao esquecimento.

Outrossim, há necessidade de que, mesmo em condenações por atos de improbidade administrativa, a consulta pública do CNJ fique disponível por um prazo certo, ou seja, pelo tempo máximo da condenação, de modo a se evitar a instituição de pena perpétua e se garantir à pessoa a dignidade para refazer sua vida.

REFERÊNCIAS

ACIOLI, Bruno de Lima; EHRHARDT JR., Marcos Augusto de Albuquerque. Uma agenda para o direito ao esquecimento no Brasil. *Revista Brasileira de Políticas Públicas*, Brasília, v. 7, n. 3, 2017, p. 383-410.

ARTHUR, Charles. Explaining the "right to be forgotten" – the newest cultural shibboleth. *The Guardian*, 14 maio 2014. Disponível em: https://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth. Acesso em: 16 out. 2020.

BOBBIO, Norberto. *A era dos direitos.* Rio de Janeiro: Elsevier, 2004.

BRASIL. Câmara dos Deputados. *Projeto de Lei n. 10.887.* 2018. Disponível em: www.camara.leg.br. Acesso em: 10 out. 2020.

BRASIL. Conselho da Justiça Federal. IV Jornada de Direito Civil. *Enunciado 531*. 2013. Disponível em: www.cjf.jus.br. Acesso em: 10 out. 2020.

BRASIL. *Lei n. 13.709*. 2018. Disponível em: www.planalto.gov.br. Acesso em: 10 out. 2020.

BRASIL. Senado Federal. *Projeto de Lei n. 3.359*. 2019. Disponível em: www12.senado.leg.br. Acesso em: 24 jul. 2020.

BRASIL. Superior Tribunal de Justiça. *AgInt no REsp 1.593.873-SP*. Rel. min. Nancy Andrighi. Julgado em 10 nov. 2016. Disponível em: www.stj.jus.br. Acesso em: 10 out. 2020.

BRASIL. Superior Tribunal de Justiça, *REsp n. 1.334.097-RJ.* Rel. min. Luís Felipe Salomão. Julgado em 28 maio 2013. Disponível em: www.stj.jus.br. Acesso em: 10 out. 2020.

BRASIL. Superior Tribunal de Justiça. *REsp n. 1.660.168.* Rel. min. Nancy Andrighi. Julgado em 5 maio 2018. Disponível em: www.stj.jus.br. Acesso em: 10 out. 2020.

EHRHARDT JR., Marcos Augusto de Albuquerque; NUNES, Danyelle Rodrigues de Melo; PORTO, Uly de Carvalho Rocha. Direito ao esquecimento segundo o STJ e sua incompatibilidade com o sistema constitucional brasileiro. *Revista de Informação Legislativa*, a. 54, n. 213, jan.-mar. 2017, p. 63-80.

MARTINS NETO, João dos Passos; PINHEIRO, Denise. Liberdade de informar e direito à memória: uma crítica à ideia do direito ao esquecimento. *Estudos Jurídicos*, v. 19, n. 3, 2014, p. 808-838.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENKE, Fabiano. A proteção de dados e o novo direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (Coords.). *Direito, inovação e tecnologia.* São Paulo: Saraiva, 2015. v. 1, p. 205-230.

MOREIRA, Rodrigo Pereira; ALVES, Rubens Valtecides. Direito ao esquecimento e o livre desenvolvimento da personalidade da pessoa transexual. *Revista de Direito Privado*, v. 64, out.-dez. 2015, p. 81-102.

OCKE, Caio Pryl; SANTOS, Larissa da Silva. É hora de quebrar a escavadeira? O "direito ao esquecimento" de dados pessoais em processos judiciais com a finalidade esgotada. *Revista do CEPEJ*, Salvador, v. 22, jan.-jul. 2020, p. 71-86.

PINHO, Humberto Dalla Bernardina de. O consenso em matéria de improbidade administrativa: limites e controvérsias em torno do acordo de não persecução cível introduzido na Lei n. 8.429/1992 pela Lei n. 13.964/2019. *Revista Interdisciplinar de Direito Curso de Direito do Centro Universitário de Valença* (UniFAA), v. 18, n. 1, jan.-jun. 2020, p. 145-162.

RECONHECIMENTO FACIAL E SEGURANÇA PÚBLICA: COMO GARANTIR A PROTEÇÃO DE DADOS PESSOAIS E EVITAR OS RISCOS DA TECNOLOGIA

Eduarda Costa Almeida[1]

RESUMO

No presente artigo, analisa-se o uso de câmeras de vigilância com a tecnologia de reconhecimento facial (RF) automatizado e em tempo real para tratamento de dados no âmbito da segurança pública, visando à condução de investigações criminais e à instrução processual penal. As ferramentas de RF cada vez mais são usadas para auxiliar as atividades policiais, por isso é fundamental analisar os casos concretos de aplicação dessa tecnologia, os parâmetros mínimos que asseguram sua legitimidade e os principais riscos aos quais a população estará submetida caso essas garantias não sejam observadas. A exploração inadequada do RF apresenta alta propensão de violar direitos fundamentais, como a privacidade e o desenvolvimento autônomo da personalidade. Diante disso, buscou-se identificar o funcionamento da técnica e mapear os princípios a serem

1 Pesquisadora do Laboratório de Políticas Públicas e Internet (Lapin). Estudante de Direito da Universidade de Brasília.

respeitados no âmbito da segurança pública de forma a mitigar possíveis danos aos cidadãos. Atualmente, a Diretiva n. 2016/680 da União Europeia e os princípios evidenciados nela, como os da finalidade, necessidade e transparência, são direcionamentos relevantes à análise da regulamentação dessa prática no Brasil. À teoria deve-se acrescentar a experiência de outros países, os riscos e danos já causados pelo uso indevido de RF.

Palavras-chave: Segurança pública. Reconhecimento facial em tempo real. Proteção de dados. Riscos. Viés no algoritmo.

ABSTRACT

This article analyzed the use of surveillance cameras with automated facial recognition (FR) technology in real time for data processing within the scope of public security, aiming at conducting criminal investigations and prosecuting criminal proceedings. FR tools are increasingly being used to assist police activities, so it is essential to analyze the specific cases of use of this technology, the minimum parameters for a legitimate use of the technology and the main risks to society if these guarantees are not observed. Misuse of the FR has a high propensity to violate fundamental rights, such as privacy and autonomous personality development. This study sought to understand the functioning of the FR and to map the principles that must be observed so that the use of FR in public security in order to mitigate possible damage to citizens. Currently, Directive 2016/680 of the European Union and the principles evidenced in it, such as that of purpose, necessity and transparency, are relevant directions for analyzing how the regulation of data use in the scope of public security could occur in Brazil. Finally, the main risks of the misuse of facial recognition and the damage already caused to individuals around the world are emphasized so that Brazilian legislation is aware of the mistakes already made.

Keywords: Public security. Real-time facial recognition. Data protection. Risks. Bias in the algorithm.

1. INTRODUÇÃO

Vivemos na sociedade da informação, na qual as pessoas estão imersas em um ambiente de uso contínuo de diferentes tecnologias, em constante desenvolvimento. O acesso a espaços e serviços digitais acaba por gerar grande acúmulo de dados pessoais, ou "rastros", no mundo virtual. Grande parte dessas informações tem sido utilizada por empresas e governos para diversas finalidades, a exemplo do *marketing* direcionado, das identidades digitais[2] e da segurança pública.

Diante desse novo contexto, surgiu a necessidade de uma norma que tutelasse o direito de privacidade e proteção de dados dos cidadãos. Por isso, em 2018, o Congresso Nacional brasileiro sancionou a Lei Geral de Proteção de Dados (LGPD), que dispõe sobre o tratamento de informações com responsabilidade e em observância aos princípios da proteção de dados em diversos contextos.

No entanto, a LGPD não se aplica inteiramente a casos de tratamento de dados pessoais para fins exclusivamente de segurança pública (art. 4º, III, *a*). Ela prevê que a legislação específica a ser criada deverá observar os princípios gerais de proteção de dados, os direitos do titular e o devido processo legal. Ainda, terá de prever medidas proporcionais e necessárias ao atendimento do interesse público (art. 4º, § 1º). Dessa

2 No Brasil, a Lei n. 13.444/2017 criou o programa Identificação Civil Nacional, que visa à criação de meios para emissão do Documento Nacional de Identidade (DNI) digital a todos os brasileiros. Essa identidade substitui outras formas de identificação.

forma, por mais que a tecnologia avance, é primordial a regulação específica sobre o uso de inovações aplicadas ao contexto de segurança pública a fim de se evitar o grande potencial de abusividade.

Assim, o governo brasileiro tem-se movimentado para pensar em estratégias de regulamentação do uso da tecnologia de Reconhecimento Facial (RF). A Câmara dos Deputados, em abril de 2019, realizou audiência pública na Comissão de Ciência e Tecnologia, Comunicação e Informática, com participação de diversos setores da sociedade, para discutir a aplicação de RF na manutenção da segurança pública (BRASIL, 2019). As posições defendidas foram controversas. Destaca-se, dentre elas, a preocupação de organizações da sociedade civil com a privacidade e a acurácia do sistema. Além disso, em novembro de 2019, a mesma Casa Legislativa instituiu uma comissão de juristas para elaborar anteprojeto de legislação específica para o tratamento de dados pessoais no âmbito da segurança pública (JÚNIOR, 2019).

Diante do exposto, nota-se que o Estado também é entidade tratadora de informações pessoais, isto é, controladora de dados. Ainda, ele busca utilizar informações dos cidadãos para promover a segurança pública em vista do cenário de elevada violência no Brasil[3] e da relevância do tema para a sociedade. Porém, esbarra na peculiaridade do tratamento de dados pessoais na prevenção, investigação, detecção e repressão de infrações penais ou execução de sanções penais.

O uso de instrumentos tecnológicos para auxiliar a segurança pública tem aplicações concretas já praticadas pelas autoridades estatais, como

3 O Ipea, órgão que registra dados sobre a violência no Brasil, aponta que, em 2017, houve 65.602 homicídios. Ainda, 75,5% das vítimas foram indivíduos negros. A taxa de homicídios por 100 mil negros foi de 43,1, ao passo que a de não negros foi de 16,0. Para mais informações, acesse: https://www.ipea.gov.br/atlasviolencia/download/19/atlas-da-violencia-2019.

escutas telefônicas, câmeras de vigilância CCTV[4] e estudo estatístico visando à atuação policial mais eficiente em áreas e horários específicos. Além dessas ferramentas, está em debate o uso da tecnologia de RF e sua validade como instrumento de complementação da atividade policial. Apesar das controvérsias, o recurso já está em prática.

Exemplo disso ocorreu no carnaval do Rio de Janeiro, em 2019. A tecnologia de reconhecimento de objetos possibilitou a recuperação de um veículo roubado. No mesmo evento, o uso de câmeras deu causa à detenção de quatro pessoas com mandado de prisão em aberto (SILVA, 2019). Em Salvador, também no carnaval daquele ano, um homem procurado pela polícia foi preso depois de identificado pelo sistema de RF (LAVADO, 2020).

Outro caso foi o da Companhia do Metropolitano de São Paulo, que publicou, em 2019, edital de licitação para implementar um sistema de câmeras com RF em algumas linhas de metrô da cidade (METRÔ, 2019).

No exterior, a polícia metropolitana de Londres (MET), por sua vez, utilizou, durante meses, RF no *King's Cross Central*, um dos locais mais visitados em Londres, sem informar aos transeuntes que seus dados estavam sendo coletados (SABBAGH, 2019). Essa atuação levantou questionamentos que serão aprofundados a seguir.

Em São Francisco, nos Estados Unidos, o órgão governamental competente, *The Board of Supervisors*, baniu a tecnologia de RF por oito votos contra um, visto o alto potencial de uso abusivo e a consequência de uma vigilância opressiva e massiva (CONGER; FAUSSET;

4 CCTV, cujo significado é *Closed Circuit Television*, é um sistema de câmeras no qual os sinais não são distribuídos publicamente, mas monitorados, principalmente para fins de vigilância e segurança. O CCTV depende do posicionamento estratégico das câmeras e da observação nos monitores. Como aquelas se comunicam com estes e/ou com gravadores de vídeo por meio de linhas privadas de cabos ou comunicação sem fio, elas recebem a designação "circuito fechado" (ROUSE, 2012).

KOVALESKI, 2019). Ainda, a IBM, uma das maiores empresas de tecnologia do mundo, anunciou que deixará de investir em RF, já que esse instrumento está sendo usado, majoritariamente, para controle social e opressão pelas forças policiais (IBM, 2020).

Dessa forma, em vista da expressiva possibilidade de violação de direitos fundamentais, vários questionamentos vêm sendo suscitados sobre a adequação da RF aos espaços democráticos. Sendo possível a implementação de RF no âmbito da segurança pública, impõe-se o debate sobre as maneiras de se regular a exploração da tecnologia de forma a garantir sua utilidade e de modo que sua implementação esteja direcionada à proteção dos dados pessoais daqueles que cometeram crimes ou não.

Neste artigo, analisou-se o tratamento de imagem de câmeras com tecnologia de RF em tempo real para fins de identificação de pessoas envolvidas em investigações criminais e instruções processuais penais.[5] Metodologicamente, por meio de regulação e bibliografias específicas, este estudo visou descrever o funcionamento técnico do RF e mapear os princípios essenciais incidentes na aplicação desse recurso na segurança pública. Assim, limitou-se à análise dos princípios da finalidade, transparência e necessidade, já que são basilares para a Diretiva n. 2016/680 da União Europeia (UE) e impactam concretamente a forma de uso do RF na segurança pública. Serão desenvolvidos também os três riscos associados à não observância dessas medidas.

5 Estão fora do escopo deste artigo os casos de tratamento posterior a ato ilícito ou crime. Tais situações diferem do uso de RF para identificação de pessoas em tempo real.

2. SEGURANÇA PÚBLICA NO BRASIL

No Brasil, o tema da segurança pública está inserido em um cenário mais amplo, por isso é preciso reconhecer alguns aspectos peculiares das políticas públicas criminais e do sistema penitenciário do país. Schneider e Miranda (2020, p. 4) afirmam que o Estado brasileiro, "para executar o controle social, adota uma política de segurança pública segregacionista e preconceituosa". Por isso, pensar em formas eficientes para a manutenção da segurança pública perpassa o problema brasileiro em que um grupo social é reprimido com coerção física e policial, e outro é protegido.[6]

Ainda, é necessário refletir que temas relacionados à segurança pública, inegavelmente, remetem a questões sobre as políticas criminais adotadas pelo governo brasileiro e o sistema penal seletivo em vigor. Assim, "qualquer tecnologia pensada para melhorar a segurança pública, além de considerar aspectos técnicos de funcionalidade, precisa atentar também para as variáveis de raça que perpassarão a sua utilização" (SILVA; SILVA, 2019, p. 7). Logo, a aplicação da tecnologia de RF, vista como prioritária para muitas autoridades brasileiras, apresenta mais uma peculiaridade diante de um sistema criminal falho e segregacionista que passa a lidar com dados delicados dos cidadãos.

---

6 Baratta (2002, p. 197) afirma existirem, em regra, duas classes: dominante e subalterna. A primeira "está interessada na contenção do desvio em limites que não prejudiquem a funcionalidade do sistema econômico-social e os próprios interesses e, por consequência, na manutenção da própria hegemonia no processo seletivo de definição e perseguição da criminalidade". Já a segunda é selecionada pelos mecanismos de criminalização. Em suma, o sistema penal brasileiro é muito similar ao descrito pelo autor, pois "o sistema das imunidades e da criminalização seletiva incide em medida correspondente sobre o estado das relações de poder entre as classes, de modo a oferecer um salvo-conduto mais ou menos amplo para as práticas ilegais dos grupos dominantes, no ataque aos direitos das classes subalternas" (idem, p. 198).

3. ASPECTOS TÉCNICOS DO RECONHECIMENTO FACIAL

O reconhecimento facial (RF) é o resultado do uso de um algoritmo baseado em visão computacional (*computer vision*) e aprendizado de máquinas (*machine learning*), separado em dois momentos (GOOGLE CLOUD PLATFORM, 2018) que completam o processo: o reconhecimento do rosto humano, *stricto sensu*, e a identificação da pessoa (MOBIDEV, 2019). Por meio de uma ramificação do *machine learning*, o *deep learning*, a capacidade de processamento de imagens foi desenvolvida a ponto de possibilitar o RF automatizado em tempo real (BBC EARTH LAB, 2015).

O RF é um método de identificação de pessoas por meio de rostos capturados em vídeos, fotos ou imagens coletadas em tempo real. Majoritariamente, os sistemas capturam e tratam dados considerados relevantes e únicos, como a distância entre os olhos ou o formato do queixo. Assim, à medida que as pessoas se movimentam por espaços públicos que possuem câmeras de vigilância com RF, a tecnologia isola imagens faciais e extrai dados contidos nelas. Esses são tratados e convertidos em representações matemáticas conhecidas como *face template*, uma assinatura facial resultante do tratamento de uma imagem capturada em tempo real e comparada com outras disponíveis em uma base de dados (EFF, 2017) – uma lista de *templates* de pessoas que podem ser identificadas. No contexto da segurança pública, esse banco de dados é preenchido com assinaturas faciais de sujeitos de interesse.

O resultado do tratamento dos dados faciais é representado por uma porcentagem de características semelhantes entre duas assinaturas. A correspondência indica a probabilidade de a pessoa que passa por uma câmera de vigilância ser ou não uma daquelas inseridas no banco. Por isso, a resposta não é binária, isto é, não se limita a *sim, o rosto capturado corresponde ao* template *existente no banco de dado*s, ou *não,*

o template *do rosto capturado pela câmera não é similar a nenhuma das assinaturas faciais contidas no banco de dados* (BBW, 2018, p. 6).

Ainda, quando a tecnologia é imprecisa na identificação da pessoa e o resultado apresentado pelo RF é incorreto, ele se classifica em (i) falso negativo ou (ii) falso positivo. O primeiro ocorre quando o sistema de RF falha na correspondência entre um rosto e uma assinatura facial que, de fato, está contida em um banco de dados. Ou seja, o sistema retornará erroneamente zero resultados em resposta a uma consulta, sendo que existe um resultado válido. Já um falso positivo ocorre quando o sistema reconhece a compatibilidade entre o *template* de uma pessoa capturada em tempo real e um outro contido no banco de dados, mas a pessoa que passou pela câmera de vigilância não é quem o sistema diz que ela é (EFF, 2017).

É importante notar que a existência de falsos negativos e falsos positivos gera consequências significativas para aplicação na segurança pública. Por exemplo, a incidência de falsos positivos causa danos a pessoas não culpáveis, visto que a identificação errônea de um inocente como alguém que cometeu um crime pode motivar a prisão e, possivelmente, condenação de um inocente. Não obstante, em caso de incidência de falsos negativos, o prejuízo está na impunidade de um criminoso.

4. A NATUREZA DO DADO TRATADO E A NECESSIDADE DE REGULAMENTAÇÃO

A informação tratada pelo RF é um dado biométrico, o que significa que a tecnologia permite a identificação e a autenticação de pessoas baseadas em um conjunto de informações únicas e específicas para cada indivíduo (THALES, 2020). Nesse sentido, é personalíssimo e singular, tal qual a impressão digital, a íris e o DNA. De acordo com a LGPD, um dado biométrico, quando vinculado a uma pessoa natural, é sensível (art. 5º, II). Por isso, a legislação destaca o tratamento de dados pessoais sensíveis, já que, caso eles "sejam conhecidos e submetidos a

tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva e que apresentaria maiores riscos potenciais do que outros tipos de informação" (DONEDA, p. 143).

Não é uníssono o apoio ao uso de tecnologias de RF para a manutenção da segurança pública. Como evidenciado no exemplo de São Francisco, algumas autoridades e instituições entendem que os riscos e prejuízos são superiores aos benefícios.[7] Não obstante, havendo a possibilidade de se usar RF, devem ser tomadas algumas medidas de precaução e elaborado um marco regulatório quanto à aplicação dessa tecnologia.

Nessa perspectiva, o impacto do tratamento indevido de dados faciais de uma pessoa é significante, e os riscos de violação de direitos e liberdades individuais são elevados. Ainda, o mau uso das informações, quando as finalidades do processamento estão no âmbito da segurança pública, produz efeitos mais gravosos, já que o direito penal é *ultima ratio* e prerrogativa do Estado contra atitudes extremas dos cidadãos.[8] Desse modo, salvaguardas específicas para o processamento de dados

---

7 Destacam-se o *The Board of Supervisors* de São Francisco (EUA), a organização britânica *Big Brother Watch* e a Rede de Observatórios da Segurança. Ademais, algumas pesquisas usadas como referências bibliográficas apontam para os elevados riscos do uso indiscriminado do reconhecimento facial na área de segurança pública para a liberdade dos cidadãos.

8 A característica de *ultima ratio* está em conformidade com o princípio da intervenção mínima, uma vez que o direito penal possui aspecto de responsabilização subsidiário, existe apenas nos ambientes em que os outros meios de controle social (civil e administrativo) não são suficientes para penalizar o sujeito. Então, adotam-se medidas excepcionais. Dessa forma, a área penal "deve ser a *ultima ratio* do sistema normativo, isto é, deve atuar somente quando os demais ramos do Direito revelarem-se incapazes de dar a tutela devida a bens relevantes na vida do indivíduo e da própria sociedade." (BITENCOURT, 2019, p. 58). Por isso, o tratamento de dados no âmbito da segurança pública também deve ser visto como excepcional e bem regulamentado.

biométricos pelo Estado são fundamentais. Por isso, no contexto europeu, a Diretiva n. 2016/680 prevê as peculiaridades a serem observadas nesse caso (arts. 3º, 13, e 10º).

5. A DIRETIVA N. 2016/680 DA UNIÃO EUROPEIA (UE)

Em 2016, o parlamento europeu e o conselho da UE estabeleceram a Diretiva n. 2016/680 para regulamentar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais pelas autoridades para efeitos de segurança pública. No documento, explicitam os princípios orientadores, como o da segurança e integridade da informação, qualidade dos dados, finalidade, necessidade e transparência (art. 4º, 1). Os três últimos serão tratados de forma mais específica neste artigo por interferirem diretamente no modo de uso do RF no âmbito da segurança pública, por estarem elencados na LGPD e manterem relação direta com a garantia dos direitos fundamentais. Em suma, a Diretiva da UE busca assegurar o tratamento de informações pessoais para fins de segurança pública, de forma responsável, diante da proteção de dados.

5.1 PRINCÍPIO DA FINALIDADE

Um dos princípios norteadores da Diretiva é o da finalidade (art. 4º, 1, *b*)[9], o qual determina que a coleta de dados pessoais deve ser feita

9 O considerando 29 da Diretiva n. 2016/680 afirma que "os dados pessoais deverão ser recolhidos para finalidades determinadas, explícitas e legítimas abrangidas pelo âmbito de aplicação da presente diretiva e não deverão ser tratados para fins incompatíveis com os da prevenção, investigação, detecção ou repressão de

para atingir objetivos específicos, explícitos e legítimos diante do escopo da segurança pública. Em suma, busca-se a prevenção, investigação, detecção e repressão de infrações penais ou a execução de sanções penais, incluindo-se a salvaguarda e prevenção de ameaças à segurança pública (art. 1º, 1).

Sob essa perspectiva, as informações pessoais coletadas por câmeras de vigilância não poderão ser utilizadas para qualquer outro fim e vice-versa. Isso significa dizer que instrumentos usados para mapeamento de regiões populosas, análise do fluxo de tráfego ou rastreamento de ônibus não poderão processar informações voltadas à segurança pública, ainda mais em caso de dados sensíveis no contexto de RF autonomizado e em tempo real. No caminho inverso, também as informações coletadas para fins de segurança não poderão ser tratadas para outras finalidades.

Em um estudo sobre o impacto do RF no Reino Unido, o *Information Commissioner's Office* (ICO), órgão inglês para defesa dos direitos à informação, afirma que os dados pessoais processados para qualquer uma das finalidades de aplicação da lei, a exemplo do tratamento para segurança pública, devem ser mantidos por não mais do que o necessário para atingir o objetivo do processamento (ICO, 2019, p. 29). Consequentemente, torna-se imprescindível identificar o período pelo qual as forças policiais devem armazenar esses dados.

Sobre essa questão, o ICO analisou dois casos de uso de RF por organizações policiais diferentes, a *Metropolitan Police Service* (MPS)

---

infrações penais ou execução de sanções penais – nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública. Se os dados pessoais forem tratados, pelo mesmo ou por outro responsável pelo tratamento, para uma finalidade abrangida pelo âmbito de aplicação da presente diretiva que não aquela para a qual foram recolhidos, esse tratamento deverá ser permitido, na condição de que esse tratamento seja autorizado em conformidade com as disposições legais aplicáveis e necessário e proporcionado para a prossecução dessa outra finalidade".

e a *South Wales Police* (SWP). Ambas deletaram os registros resultantes do uso da tecnologia de RF após o processamento, exceto nos casos em que o sistema encontrou correspondência entre o rosto analisado instantaneamente e os *templates* contidos no banco de dados da polícia. No caso da SWP, foram excluídos todos os registros no final da implantação do RF, incluídas as imagens das pessoas reconhecidas e as dos falsos positivos, além dos dados da lista de observação. Já a MPS manteve registros por trinta dias, incluindo falsos positivos (ICO, 2019, p. 29). O cuidado em excluir dados não aproveitáveis evidencia que o interesse para a segurança pública em manter imagens ou *templates* de pessoas identificadas ou não como sujeitos de interesse é injustificável e desproporcional.

Por fim, nota-se que o uso de RF não é autorizado para o atendimento de toda e qualquer finalidade relativa à segurança pública. Por exemplo, o objetivo de preservar a segurança não é alcançado quando o RF é explorado para determinar a dosimetria de pena a um indivíduo no sistema de justiça criminal (BUOLAMWINI; GEBRU, 2018, p. 1). Finalidades similares à segurança são atingidas apenas quando identificadas pessoas insertas na lista de interesse da polícia, uma vez que poderão enfrentar um processo judicial segundo o devido processo legal.

5.2 PRINCÍPIO DA NECESSIDADE

Para efetivação do princípio da necessidade, preza-se pela limitação do tratamento ao mínimo necessário à realização de suas finalidades (GOV.BR, 2020, p. 14). Para adequada utilização de dados biométricos na manutenção da segurança pública, é fundamental a observância do ciclo de vida do dado pessoal. Em regra, ele possui cinco fases: coleta, retenção, processamento, compartilhamento e eliminação (GOV. BR, 2020, p. 41). Todas essas etapas merecem cuidado específico.

Em conformidade com o ciclo e o princípio da necessidade, frisa-se a relevância da fase de eliminação dos dados.

Segundo o ICO (2019, p. 29), o processamento para fins de aplicação da lei deve estar sujeito a cronogramas de retenção, revisão periódica e exclusão quando não justificável a manutenção das informações.[10] A importância dessa última questão é reconhecida na Diretiva da UE, a qual estabelece, em seu art. 5º, a previsão de "prazos adequados para o apagamento dos dados pessoais ou para a avaliação periódica da necessidade de os conservar. Devem ser previstas regras processuais que garantam o cumprimento desses prazos".

Além disso, o Grupo de Trabalho do Artigo 29º para a proteção de dados (*Article* 29) – composto por europeus que, de forma independente, lidaram com as questões relacionadas à proteção de dados e privacidade antes da aplicação do GDPR – emitiu parecer sobre a Diretiva n. 2016/680. No documento, destaca que deve haver previsão de "critérios claros e transparentes para a avaliação da necessidade de conservar (...) dados pessoais, bem como de requisitos processuais (...), com vista a evitar eventuais abusos" (ARTICLE 29 WP, 2017, p. 4).

Como consequência, compreende-se que manter o *template* do rosto de

10 Ainda que o tratamento de dados pessoais com técnicas de RF para fins de prevenção de crimes não seja escopo deste artigo, nota-se que a questão de saber se certos dados cumpriram seus objetivos e não são mais necessários surge especialmente quando o armazenamento de dados é permitido para fim preventivo. É inerente a tal propósito que o armazenamento possa basear-se apenas em uma avaliação de risco relativa a um determinado titular de dados. Nesses casos, é complexo identificar o ponto em que os dados não são mais úteis, ao contrário da investigação criminal, que exige automaticamente uma decisão sobre a supressão das informações pessoais coletadas durante o processo. No entanto, o princípio da necessidade solicita uma revisão do prognóstico após um período adequado. A decisão de manter os dados para outro período deve ser bem fundamentada, e o raciocínio precisa ser documentado para permitir a revisão.

um transgressor da lei só é relevante para fins de reconhecimento facial até o momento em que cumprida a sanção penal. Após esse período, armazenar o *template* não é mais útil ou necessário, e o risco de compartilhamento ou uso indevido é alto. Em vista desse contexto, o *Article* 29 (2017, p. 6) propõe um sistema de exclusão automática das informações pessoais assim que expirado o limite de tempo de conservação e defende a avaliação periódica de modo a garantir o respeito ao princípio da necessidade.

5.3 PRINCÍPIO DA TRANSPARÊNCIA

O princípio da transparência, ou da publicidade, favorece o combate ao uso abusivo de informações e a prestação de contas (*accountability*) aos titulares quanto à construção de bancos de dados (MENDES, 2014, p. 71). A aplicação desse preceito no contexto de uso do RF para a segurança pública implica o estabelecimento de parâmetros à atuação policial. Diante disso, foram destacadas algumas questões relevantes à análise apresentada neste artigo: (i) qual banco de dados é explorado pela polícia; (ii) o que o responsável pelo tratamento deve informar e registrar; e (iii) qual a necessidade de desenvolvimento de um relatório de impacto pelo uso da tecnologia de RF.

Um dos pontos mais controversos é a definição do banco de dados a ser explorado e utilizado como referência na comparação de *templates* faciais. Questiona-se se o mais adequado dispõe de todos os procurados pela polícia ou apenas daqueles que cometeram crimes mais graves; ainda, se não condenados deveriam compor esse grupo. A extensão desse banco e sua constituição permitem inferências relevantes para os direitos de privacidade e proteção de dados. Primeiramente, se uma pessoa não tem o respectivo *template* inserido no banco de dados da polícia, não poderá ser reconhecida mesmo que passe na rua e tenha seus dados faciais tratados, visto que será impossível ao sistema fazer a correspondência.

Portanto, um dos pontos-chave para o bom funcionamento do RF é a composição da lista de sujeitos de interesse (banco de dados ou *watchlist*), formada pelo *template* biométrico dessas pessoas. No Reino Unido, todas os cidadãos detidos pela polícia passam a compor o banco de dados. A Seção 64A da Lei de Polícia e Evidência Penal de 1984 (PACE) garante à polícia o poder de tirar fotografias faciais de quem fica detido após a prisão – são as chamadas "imagens de custódia". Isso permite, ainda, o *upload* dos sistemas locais para o banco de dados nacional da polícia, o *Police National Database*.

No entanto, usar as imagens de custódia como banco de dados para o RF é uma decisão complexa, já que grande parte das pessoas presas não chega a ser acusada ou condenada. No caso do Reino Unido, a organização *Big Brother Watch* (BBW) afirma que as forças policiais locais não sabem determinar quantos rostos disponíveis na base de dados de imagens de custódia são de inocentes (BBW, 2018, p. 4). Por isso, a regulação brasileira para uso de tecnologias na segurança pública deve ficar atenta quanto a dois aspectos: (i) a definição de um procedimento para o cidadão se certificar de que seus dados não são mantidos ilegalmente pela polícia e, em caso afirmativo, possa solicitar a exclusão da imagem ou do *template*; e (ii) a elaboração de mecanismos que possibilitem a exclusão automática dos dados pessoais quando ausente acusação ou condenação por crime.

Segundo a ICO (2019, p. 17), as organizações policiais devem garantir que os dados constantes do banco de dados sejam limitados e utilizados apenas quando estritamente necessário. Assim, nota-se que as salvaguardas da proteção de dados e dos direitos humanos somente se cumprem quando as forças policiais formam cuidadosamente a lista de sujeitos de interesse. Esse procedimento reduz o número de *templates* e informações pessoais, assegurando a inclusão de novas imagens quando necessário para atender às finalidades do tratamento de dados.

No Brasil, a situação do sistema penal é peculiar, pois há poucas

informações sobre o funcionamento da burocracia penal. Por exemplo, até 2018, o número de encarcerados era estimado, e o juiz de direito era pouco informado sobre a custódia do preso (CNJ, 2018, p. 9). Além disso, a superlotação dos presídios é uma realidade em todo o país: em 2019, existiam 441.147 vagas ocupadas por 733.460 pessoas (CNMP, 2020). Ainda nesse sentido, "em 2016, o Supremo Tribunal Federal declarou o estado de coisas inconstitucional em que estava o sistema penitenciário e determinou providências administrativas" (CNJ, 2018, p. 9) e, no julgamento do Recurso Extraordinário n. 641.320/RS, foi indicada a criação de um cadastro nacional de presos pelo Conselho Nacional de Justiça (CNJ).[11]

Criou-se, então, o Banco Nacional de Monitoramento de Prisões, de modo que "toda pessoa que passar pelo sistema prisional será cadastrada (...) e ganhará um registro nacional, chamado RJI (Registro Judicial Individual)" (CNJ, 2018, p. 22). Esse cadastro compila dados pessoais do preso, como fotografia, cópia de documentos e outras informações gerais. No contexto de implementação de RF, o sistema se assemelha ao modelo do Reino Unido, uma vez que gera um *template* de todo indivíduo que passa por câmeras de vigilância e o compara com a imagem de pessoas que tiveram a prisão determinada.

Não obstante a necessidade de medidas que assegurem a proteção de dados aos cidadãos e a transparência no uso da tecnologia, essa não foi a realidade do uso de RF no carnaval de 2019, no Rio de Janeiro. Nesse exemplo, as imagens coletadas por 28 câmeras espalhadas em Copacabana foram compiladas e transmitidas para o Centro Integrado de Comando e Controle, onde eram comparadas com os dados faciais

11 No entanto, ainda se questiona sobre a necessidade e operabilidade de um banco de dados centralizado em âmbito nacional, visto que o sistema penitenciário brasileiro é significante e, por isso, trata informações pessoais de milhares de pessoas que estão em prisões por todo o país.

disponíveis na Polícia Civil (VETTORAZZO; PITOMBO, 2019). Ainda no caso de uso de RF no Rio, também foi compartilhado o banco de dados do Detran, órgão que detém informações fotográficas de todos os condutores de veículos do Estado, inclusive de inocentes, as quais poderiam ter sido utilizadas para RF, possibilitando que pessoas não procuradas pela polícia fossem reconhecidas.

Quanto ao que deve ser informado e registrado pelo responsável pelo tratamento de dados, a Diretiva n. 2016/680, em seu art. 13º, assegura que sejam informados ao titular alguns comunicados. O sujeito deve saber sobre a finalidade do tratamento de seus dados pessoais, além de ter o direito de solicitar a retificação de uma informação incorreta. Para que haja transparência no processo, cabe ao responsável informar o fundamento jurídico do tratamento e o prazo de conservação dos dados ou, no mínimo, os critérios para definição desse período e os possíveis destinatários (art. 13º, n. 2). Logo, busca-se nitidez na relação entre o titular e o responsável pelo tratamento.

O princípio da transparência é efetivado também por meio da elaboração de um relatório de impacto do uso da tecnologia no âmbito da segurança pública. A Diretiva europeia prevê essa avaliação, o *Data Protection Impact Assessment*. Ela indica que devem ser descritas as operações no tratamento dos dados pessoais e apresentados (i) os riscos aos direitos e às liberdades dos titulares dos dados; (ii) as medidas previstas para fazer face a eles; (iii) as garantias dos sujeitos previstas em lei; (iv) as medidas de segurança; e (v) os mecanismos para assegurar a proteção dos dados pessoais (art. 27º). Esse documento é fundamental para que se avalie o impacto que qualquer processamento de alto risco terá sobre indivíduos e, mais importante, se busquem meios de minimizar os problemas advindos. É também instrumento essencial para as forças policiais demonstrarem que o uso do RF está restrito ao estritamente necessário e os requisitos e princípios da proteção de dados estão sendo atendidos (ICO, 2019, p. 23).

Diante do exposto, nota-se que a diretiva europeia prevê uma nova arquitetura de direitos aos titulares, bem como de atividades a serem cumpridas pelas autoridades estatais por conta do uso de novas tecnologias para efeitos de segurança pública. Assim, recomenda-se que o processamento de dados sensíveis, no Brasil, de forma similar ao exemplo europeu, seja previsto e regulado em lei.

6. RISCOS NO USO DO RECONHECIMENTO FACIAL

A exploração do RF com vistas à garantia da segurança pública apresenta riscos para os direitos fundamentais do indivíduo, como liberdade, privacidade, inviolabilidade da vida íntima e outros. Eles apontam para a possibilidade de violação de valores muito caros à sociedade moderna, a exemplo do direito de ir e vir e da garantia de igualdade entre os cidadãos. Para algumas autoridades estatais, como as da cidade de São Francisco, os malefícios causados pela aplicação da tecnologia são maiores que os benefícios (CONGER; FAUSSET; KOVALESKI, 2019). Logo, é relevante pontuar as possíveis ameaças para que sejam implementados mecanismos efetivos de mitigação dos danos e de proteção de informações particulares, ainda mais quando os objetos de tratamento são dados biométricos. Dentre vários riscos analisados, ligados à não concretização dos princípios da finalidade e necessidade, destacam-se: (i) vigilância massiva; (ii) erros de acurácia; e (iii) existência de viés no algoritmo.

6.1 VIGILÂNCIA MASSIVA

Em uma sociedade da informação, as pessoas constantemente registram dados e atividades em redes sociais e plataformas de serviços como

Netflix, *Google Maps* e *WhatsApp*. Por isso, algumas empresas armazenam informações pessoais de milhares de usuários ao redor do mundo e cruzam dados para identificar padrões comportamentais e interesses individuais. Esse movimento também ocorre no setor público, como no processamento de dados dos cidadãos tendo em vista a manutenção da segurança pública, por exemplo.

Assim, sob o fundamento de garantir proteção da sociedade, "instituições (...) governamentais armazenam e analisam dados, organizando e gerenciando populações inteiras. Esta nova estruturação digital trouxe consigo a possibilidade de armazenar uma quantidade inimaginável de dados" (SCHNEIDER; MIRANDA, 2020, p. 6). Frise-se que as consequências desse procedimento são de alto risco e podem acarretar a vigilância de um número significativo de indivíduos e, até mesmo, a prisão de alguns deles. O uso indiscriminado do RF em câmeras no espaço público propicia a vigilância massiva do Estado, que pode ser informado quanto ao local visitado por um cidadão, ao tempo de permanência ali e às interações feitas com outros frequentadores.

Nesse sentido, Bigo (2006, p. 47) discorre sobre o contexto apresentado em seguida aos ataques de 11 de setembro, em que imperou a sensação de ameaça à segurança constante. O resultado foi o *ban-opticon*, termo cunhado pelo estudioso para se referir ao uso de instrumentos tecnológicos na definição de um alvo a ser vigiado. O conceito, amplamente aplicado, é uma nova versão do panóptico de Foucault. Assim, "fundando-se em (...) dados biométricos e técnicas digitais de reconhecimento facial, o banóptico é capaz de realizar o controle social por intermédio da identificação preventiva de indivíduos" (SCHNEIDER; MIRANDA, 2020, p. 6). Dessa forma, há uma preocupação quanto à eventual subtração das liberdades individuais.

O uso descontrolado de RF permite que as forças policiais identifiquem todos os que transitam em espaços públicos, até mesmo em marchas e eventos religiosos, reuniões políticas, protestos ou manifestações

populares. Além disso, esses dados podem facilmente ser cruzados com outros disponíveis na internet (PRIVACY INTERNATIONAL, 2019), a exemplo dos inseridos em redes sociais, registros de saúde, bancos de dados de proteção ao crédito etc. Em Hong Kong, manifestantes que participavam dos protestos de 2019 tiveram a preocupação de se munirem com canetas de *laser* para impedir o funcionamento das câmeras, visto que isso permitiria a identificação dos atuantes no evento político (TREVISAN, 2019).

Com a permanente vigilância e supervisão do Estado sob o pretexto de segurança, cria-se uma condição em que parte da liberdade das pessoas encontra-se ferida. Não há mais ampla autonomia para o desenvolvimento da personalidade e autodeterminação, visto que as pessoas estão sendo constantemente observadas. Além disso, os direitos de privacidade e inviolabilidade da intimidade, mesmo que exercidos em espaços públicos, são violados e, por isso, constrói-se um entendimento de que dados pessoais, como informações biométricas, por exemplo, não estão mais sob a posse do sujeito, mas sob o controle do Estado, que decide livremente a forma de tratá-las.

Além disso, a vigilância exercida pelo uso da RF é potencializada, ante a facilidade de se reconhecer uma pessoa independentemente de contato físico ou autorização prévia. Anteriormente, o indivíduo tinha conhecimento de estar sendo identificado e da finalidade do procedimento, como em pontos de fiscalização no trânsito ou na migração em um país; porém, o RF tornou possível vigiar alguém sem o seu conhecimento. Dessa forma, cada vez mais, as pessoas estão sujeitas ao tratamento de dados biométricos e à verificação de identidade sem sequer estarem cientes disso.

A falta de regulação e determinação de uma finalidade específica para exploração da tecnologia e o uso indevido de câmeras criam o estado de vigilância massiva. O ICO (2019, p. 3) evidencia o maior risco desse contexto: vigilância em larga escala com impacto sobre os

direitos humanos e de informação. O BBW (2018, p. 13) aponta que o uso indiscriminado de RF é uma ameaça à privacidade, porquanto as câmeras podem atuar como postos de controle para identificação biométrica. Esse tipo de aplicação da tecnologia não visa à manutenção da segurança pública, já que coleta informações não necessariamente úteis. Mesmo que ela se restringisse a pessoas que cometeram crimes, é fundamental observar as devidas formas de tratamento em respeito à proteção de dados. A liberdade de expressão e o direito de realizar atividades diárias sem perturbações de autoridades estatais, de ir aonde quiser e com quem quiser, além de participar de eventos e manifestações são mitigados quando ausente a regulação (BBW, 2018, p. 13).

Quanto à vigilância massiva, a China desenvolveu um sistema próprio de classificação dos cidadãos, o *Social Credit System* (SCS), que possibilita a integração de sistemas de crédito, punição, recompensa e identidade do indivíduo. Em suma, todos são rastreados por câmeras de vigilância e classificados em quatro áreas: atividades comerciais, comportamentos sociais, interesse administrativo e cumprimento das leis (MAURTVEDT, 2017, p. 16). Por meio dessas notas, sanções são aplicadas, como, por exemplo, proibição de aquisição de passagens em voos domésticos – mais de 9 milhões de chineses com notas baixas sofreram essa penalidade (MA, 2018). Especificamente sobre o RF, o país está desenvolvendo mecanismos que comparam, de forma automática e instantânea, rostos com mais de 1,3 bilhão de fotos de identificação, em segundos, para auxiliar o rastreamento dos cidadãos (JIAQUAN, 2018). Ainda, o *site* do SCS já encoraja os usuários a informarem seus dados faciais por meio de fotos, o que oferece mais um instrumento de incorporação de dados ao grande banco chinês (MATSAKIS, 2019).

A inexistência de um regulamento para proteger a privacidade dos cidadãos é uma das razões pelas quais a China dispõe da enorme quantidade de dados pessoais e da mais avançada tecnologia em inteligência artificial habilitada para vigilância (MAURTVEDT, 2017, p. 19). Nesse

sentido, o SCS reforça os princípios e fundamentos da vigilância, induzindo os chineses a um estado de vigília permanente, que garante a execução das funções do poder. No caso, o poder detido pelo Estado é derivado da capacidade não juridicamente regulada de tratar informações e extrair conhecimentos de dados sobre os sujeitos, e, ainda, da possibilidade de restringir o acesso a bens e serviços comuns (MAURTVEDT, 2017, p. 50).

6.2 ERROS DE ACURÁCIA

Outro problema no uso da tecnologia de RF é o baixo nível de acurácia do sistema, ou seja, o percentual de falha é bastante significativo, seja por identificar erroneamente uma pessoa, seja por não reconhecer o sujeito procurado a despeito de sua imagem constar do banco de dados. O resultado dessa falha é prejudicial à população, ainda mais quando se trata da segurança pública.

Um relatório do BBW (2018, p. 3) indica que, no Reino Unido, 95% das correspondências feitas por RF resultaram em indicação incorreta de pessoas inocentes. A incidência da baixa acurácia gera efeitos na atuação policial quanto ao princípio da finalidade e necessidade de armazenamento das informações. Ainda que todas as imagens sem correspondência venham a ser excluídas do sistema, o armazenamento das demais será suficiente para gerar riscos à proteção dos dados. A exemplo do Reino Unido, 95% das fotos mantidas pela polícia não estariam atendendo à finalidade da segurança pública, visto serem os índices de erro do sistema tão elevados.

Ainda no carnaval de 2019, no Rio de Janeiro, uma mulher foi confundida pelo sistema de RF com outra, acusada de ter cometido crimes. A senhora inocente foi conduzida à delegacia e só mais tarde liberada. O erro na formação do banco de dados da polícia ficou evi-

dente em relação a outro aspecto, a cidadã procurada já se encontrava presa desde 2015, mas ainda constava da lista de sujeitos de interesse da polícia (CORREIO, 2019).

Para evitar esse tipo de problema, argumenta-se que os profissionais, majoritariamente policiais, responsáveis pela verificação da correspondência entre a face e o *template*, devem ser capacitados para compreenderem o sistema de RF em uso e perceberem quando abordar a pessoa identificada. No entanto, existem, quanto a isso, no mínimo dois impasses. Na maioria das vezes, os *templates* não estão associados à fotografia da pessoa procurada, apenas à representação matemática da foto, e as forças policiais não são submetidas a treinamento especializado para tomarem melhores decisões (EFF, 2017). Diante dessa realidade, o ICO (2019, p. 31) frisa a necessidade de se revisarem as políticas de privacidade, as práticas de governança, os procedimentos e treinamentos da atuação policial e as avaliações de risco à proteção de dados pessoais, tendo em vista as novas tecnologias.

Sobre aspectos técnicos, algumas características da imagem podem atrapalhar o bom funcionamento do RF, tais como iluminação, enquadramento do rosto, expressão facial, qualidade de imagem e envelhecimento facial. Além disso, alguns estudos apontam que grupos demográficos específicos de etnia, gênero e idade são mais suscetíveis a sofrerem erros no processo de RF (BUOLAMWINI; GEBRU, 2018, p. 1).

6.3 VIÉS NO ALGORITMO

As entidades que lidam com RF sinalizam os aspectos discriminatórios na forma de concepção da tecnologia. O desempenho dos algoritmos de RF é prejudicado quando os dados selecionados para o treinamento da inteligência artificial não são representativos (KLARE *et al*., 2012, p. 1791). O ICO (2019, p. 33) pontua que o sistema pode

apresentar um determinado viés se as faces utilizadas no treinamento do algoritmo não tiverem representatividade equilibrada da população, ou seja, não observarem as variações de cor e etnia. Logo, a taxa de precisão e acurácia será diferente quando apresentado rosto para cuja detecção o sistema não foi treinado.

Estudo realizado com diferentes algoritmos de classificação de gênero, idade e etnia analisou se os algoritmos de RF exibem vieses demográficos quando aplicados em grupos específicos (KLARE *et al*., 2012, p. 1789). Notou-se variação para pior no desempenho do RF quando exposto a grupos demográficos representativos, isto é, com grande presença de pessoas variadas, como mulheres, negros e jovens. Após a avaliação dos diferentes algoritmos de classificação pelo rosto, confirmou-se que eles não apenas tinham desempenho significativamente pior em certos cortes demográficos como também consistentemente apresentavam pior performance nos mesmos grupos, sempre entre mulheres, negros e indivíduos mais jovens, de 18 a 31 anos (KLARE *et al*., 2012, p. 1789).

Portanto, treinar a inteligência artificial de RF com dados demograficamente bem distribuídos é fundamental para reduzir a vulnerabilidade de certos grupos (KLARE *et al*., 2012, p. 1800). Além disso, o desempenho do sistema em relação a grupos étnicos e etários específicos melhora quando há treinamento exclusivamente direcionado a eles (KLARE *et al*., 2012, p. 1800).

Da perspectiva do RF automatizado, o teste realizado pelo *National Institute of Standards and Technology* (NIST), agência governamental estadunidense sobre inovação e competitividade tecnológica (2019, p. 7), apontou que os algoritmos de RF têm variações na acurácia, a depender do grupo demográfico de um sujeito. Entre outras descobertas, o estudo demonstrou que falsos positivos são duas a cinco vezes mais frequentes na análise de mulheres, variando de acordo com o algoritmo, o país de origem e a idade (NIST, 2019, p. 7). Essa discrepância está presente

na maioria dos algoritmos e conjuntos de dados (*datasets*) testados pelo NIST. Ainda, a menor taxa de falso positivo ocorre com europeus (NIST, 2019, p. 7), que são majoritariamente brancos.

Uma pesquisa conduzida pelo *Massachusetts Institute of Technology* (MIT) apontou que algoritmos comercializados para a fase de reconhecimento de rostos erram em classificar mulheres negras até 34,7% das vezes; e homens brancos, no máximo, em 0,8% dos casos (BUOLAMWINI; GEBRU, 2018, p. 1). A performance de algoritmos de classificação de gênero foi melhor em indivíduos com cor de pele mais clara. Como exemplo, a taxa de erro de algoritmos da Microsoft foi de 0,7% para essas pessoas e 12,9% para as de pele escura; já algoritmos da IBM apresentaram taxas de erro superiores a 22% quanto a essas últimas (BUOLAMWINI; GEBRU, 2018, p. 10).

A principal justificativa para a atuação diferente do RF em relação à cor da pele está no processo de treinamento da inteligência artificial. É mais fácil o reconhecimento de alguém pertencente ao escopo usado no treino do sistema, já que se tornam familiares os atributos faciais. Porém, quando o grupo é constituído por uma etnia de forma desproporcional, o algoritmo otimiza a precisão para a maioria (GARVIE; BEDOYA; FRANKLE, 2016). Portanto, as pesquisas evidenciam menor acurácia quando o RF é usado para identificar uma diversidade maior de pessoas, especificamente mulheres negras, visto que elas apresentam atributos faciais distintos dos de homens brancos. Mediante essa peculiaridade, é fundamental o estabelecimento de relatórios rigorosos sobre as métricas de desempenho da tecnologia para que haja transparência no funcionamento do algoritmo e se estabeleçam debates sobre o uso ético do RF.

O tópico da discriminação, ante a existência de viés no algoritmo, ligada ao uso do RF é ainda mais sensível quando a tecnologia é usada para auxiliar a segurança pública de um país com diversas etnias e sistema penal racista. Um grupo demográfico pouco representado no conjunto de dados de referência do algoritmo de RF pode ser sujeito a

frequente identificação errônea. Assim, é primordial analisar as consequências do aumento da representação fenotípica e demográfica em conjuntos de dados faciais e na avaliação algorítmica.

7. CONCLUSÃO

A atuação policial e o uso de novas tecnologias no âmbito do direito penal só serão legítimos e constitucionais se regulamentados em conformidade com os direitos constitucionais do devido processo legal, da privacidade e da proteção de dados do titular. Com isso, garantem-se, por mais relevantes que a segurança pública e o interesse público sejam, os direitos individuais e impede-se a instauração da vigilância massiva. Nesse sentido, a tecnologia de RF pode ser vista como instrumento conveniente, no entanto é primordial pensar nos desafios advindos da sua utilização e na preservação de direitos fundamentais e de valores sociais relevantes, como a privacidade e o direito de ir e vir.

No contexto do RF, restou evidente que seu uso expõe as pessoas a riscos elevados e peculiares, na medida em que são identificadas mesmo sem aviso ou consentimento prévios. Esses riscos são ainda mais manifestos quando a tecnologia é utilizada para finalidades similares à segurança pública, já que essencialmente o direito penal é intrusivo, excepcional e desempenha a função de balizar e limitar o poder punitivo do Estado. Contudo, se não houver regulamento adequado e direcionado para a proteção de dados, existe o risco elevado de a regra ser a vigilância digital, o controle e a penalização dos cidadãos. Não obstante o RF já seja utilizado pelas forças policiais brasileiras, é fundamental promulgar uma legislação autorizativa da exploração dessa tecnologia capaz de coibir o uso abusivo.

Diante do exposto, qualquer forma de regulamentação escolhida deve prever salvaguardas especialmente sobre os princípios da finalidade,

necessidade e transparência. O primeiro tem os objetivos específicos de delinear as motivações legítimas do uso da tecnologia para aplicação na segurança e de minimizar a quantidade de dados coletados, armazenados e tratados pelo Estado. O segundo preceito garante a atualização das informações pessoais, o tratamento restrito ao minimamente necessário e a exclusão de quaisquer outros materiais. Já o terceiro assegura os direitos dos titulares, a atuação legal das forças policiais e a supervisão e controle do uso da tecnologia pela sociedade.

A observação dos regulamentos específicos e da proteção de dados pessoais também tem como finalidade mitigar possíveis danos. Um deles seria a violação dos direitos fundamentais previstos na Constituição brasileira, como a liberdade básica do indivíduo. Os três principais riscos apontados neste artigo foram a vigilância massiva, os erros de acurácia e o viés do algoritmo. A desregulação no uso de RF coloca os cidadãos em um contexto de vigília no qual todos são suspeitos. Isso vai de encontro às garantias fundamentais e ao direito à privacidade. Diante desses riscos, é fundamental garantir a frequência dos exames de acurácia da tecnologia por meio de testes padronizados e independentes, de modo a se analisar a taxa de erro diante de tendências étnicas e de gênero. Ainda, a falta de precisão e a existência de, em regra, bases de dados de treinamento enviesadas possui como consequência a discriminação de grupos que são mais prováveis de serem identificados erroneamente pelo RF.

Portanto, as consequências do uso do RF para a segurança são reconhecidas e devem ser mais bem analisadas para que se entenda a possibilidade ou não da aplicação dessa tecnologia no âmbito da segurança pública no Brasil, país que possui sistema penal falho e segregacionista. No entanto, os efeitos do RF só serão devidamente alcançados se o uso for proporcional e houver equilíbrio entre a privacidade dos indivíduos e a aplicação da lei. Não é desejável que se escolha um tema em detrimento de outro, como a segurança pública frente às liberdades humanas que possibilitam o desenvolvimento autônomo da personalidade, visto

que os malefícios dessa seleção atingem os valores de uma sociedade democrática e são de difícil compensação.

REFERÊNCIAS

ARTICLE 29. *Parecer sobre algumas questões importantes da Diretiva relativa à proteção de dados na aplicação da lei (Diretiva (UE) 2016/680).* 2017. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178. Acesso em: 5 maio 2020.

BARATTA, Alessandro. *Criminologia crítica e crítica do direito penal*: introdução à sociologia do direito penal. Tradução de Juarez Cirino dos Santos. 3. ed. Rio de Janeiro: Editora Revan, Instituto Carioca de Criminologia, 2002.

BBC EARTH LAB. *How does facial recognition work? | Brit Lab.* 2015. Disponível em: https://www.youtube.com/watch?v=1aHub80AHFk. Acesso em: 24 jul. 2020.

BIG BROTHER WATCH (BBW). *Face Off*: the lawless growth of facial recognition in UK policing. 2018. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em: 5 maio 2020.

BIGO, Didier. Security, exception, ban and surveillance. *In:* LYON, David. *Theorizing surveillance*: the panopticon and beyond. Wilan, 2006. p. 46-68.

BITENCOURT, Cezar Roberto. *Tratado de direito penal*: parte geral. 19. ed. São Paulo: Saraiva, 2019. v. 1.

BRASIL. Câmara dos Deputados. *Comissão de Ciência e Tecnologia, Comunicação e Informática, Audiência Pública Ordinária*. 2019. Dis-

ponível em: https://www.camara.leg.br/evento-legislativo/54893. Acesso em: 5 maio 2020.

BUOLAMWINI, Joy; GEBRU, Timmit. Gender Shades: Intersectional accuracy disparities in commercial gender classification. *Conference on Fairness, Accountability, and Transparency*, Proceedings of Machine Learning Research 81, p. 1-15, 2018.

CONGER, Kate; FAUSSET, Richard. KOVALESKI, Serge. *San Francisco Bans Facial Recognition Technology*. 2019. Disponível em: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html. Acesso em: 5 maio 2020.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). *Banco Nacional de Monitoramento de Prisões*. 2018. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2018/01/57412abdb54eba909b3e1819fc4c3ef4.pdf. Acesso em: 7 maio 2020.

CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO (CNMP). *Sistema prisional em números*. 2020. Disponível em: https://www.cnmp.mp.br/portal/relatoriosbi/sistema-prisional-em-numeros. Acesso em: 15 maio 2020.

CORREIO. *Inocente é confundida com criminosa por câmera de reconhecimento facial no Rio*. Disponível em: https://www.correio24horas.com.br/noticia/nid/inocente-e-confundida-com-criminosa-por-camera-de-reconhecimento-facial-no-rio/. Acesso em: 8 maio 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

ELECTRONIC FRONTIER FOUNDATION (EFF). *Face Recognition*. 2017. Disponível em: https://www.eff.org/pages/face-recognition. Acesso em: 5 maio 2020.

GARVIE, Clare; BEDOYA, Alvaro; FRANKLE, Jonathan. *Unregulated police face recognition in America*. 2016. Disponível em: https://www.perpetuallineup.org/findings/racial-bias#footnote223_i485k1t. Acesso em: 12 maio 2020.

GOOGLE CLOUD PLATFORM. *How Computer Vision Works*. 2018 Disponível em: https://www.youtube.com/watch?v=OcycT1Jwsns&t=32s. Acesso em: 24 jul. 2020.

GOV.BR. *Guia de boas práticas Lei Geral de Proteção de Dados (LGPD)*. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-lgpd.pdf. Acesso em: 6 maio 2020.

IBM. *IBM CEO's Letter to Congress on Racial Justice Reform*. 2020. Disponível em: https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/. Acesso em: 5 set. 2020.

INFORMATION COMMISSIONER'S OFFICE (ICO). *ICO investigation into how the police use facial recognition technology in public places*. 2019. Disponível em: https://ico.org.uk/media/about-the-ico/documents/2616185/live-frt-law-enforcement-report-20191031.pdf. Acesso em: 6 maio 2020.

JIAQUAN, Zhou. *Drones, facial recognition and a social credit system*: 10 ways China watches its citizens. 2018. Disponível em: https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china. Acesso em: 8 maio 2020.

JÚNIOR, Janary. *Maia cria comissão de juristas para propor lei sobre uso de dados pessoais em investigações*. 2019. Disponível em: https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/. Acesso em: 25 jul. 2020.

KLARE, Brendan *et al.* Face Recognition Performance: Role of De-

mographic Information. *IEEE Transactions on information forensics and security*, v. 7, n. 6, 2012, p. 1789-1801.

LAVADO, Thiago. *Aumento do uso de reconhecimento facial pelo poder público no Brasil levanta debate sobre limites da tecnologia*. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/02/21/aumento-do-uso-de-reconhecimento-facial-pelo-poder-publico-no-brasil-levanta-debate-sobre-limites-da-tecnologia.ghtml. Acesso em: 5 maio 2020.

MA, Alexandra. *China has started ranking citizens with a creepy "social credit" system*: here's what you can do wrong, and the embarrassing, demeaning ways they can punish you. 2018. Disponível em: https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4. Acesso em: 8 maio 2020.

MANN, Monique; SMITH, Marcus. Automated Facial Recognition Technology: recent developments and approaches to oversight. *UNSW Law Journal*, v. 40, 1, 2017, p. 121-145.

MATSAKIS, Louise. *How the West Got China's Social Credit System Wrong*. 2019. Disponível em: https://www.wired.com/story/china-social-credit-score-system/. Acesso em: 8 maio 2020.

MAURTVEDT, Martin. *The Chinese Social Credit System*: surveillance and social manipulation: a solution to "moral decay"? 2017. Tese (Doutorado) – Department of Culture Studies and Oriental Languages, University of Oslo, Norway.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, cap. 1.

METRÔ. *Metrô compra sistema de monitoramento eletrônico com*

reconhecimento facial. 2019. Disponível em: http://www.metro.sp.gov.br/noticias/28-06-2019-metro-compra-sistema-de-monitoramento-eletronico-com-reconhecimento-facial.fss. Acesso em: 5 maio 2020.

MOBIDEV. *Face Detection & Recognition Software based on Machine Learning*. 2019. Disponível em: https://www.youtube.com/watch?v=X7_ojlEXnWc. Acesso em: 24 jul. 2020.

PRIVACY INTERNATIONAL. *Protecting Civic Spaces*. 2019. Disponível em: https://privacyinternational.org/long-read/2852/protecting-civic-spaces. Acesso em: 8 maio 2020.

ROUSE, Margaret. *CCTV (closed circuit television)*. 2012. Disponível em: https://whatis.techtarget.com/definition/CCTV-closed-circuit-television. Acesso em: 15 maio 2020.

SABBAGH. Dan. *Facial Recognition Row*: police gave King's Cross owner images of seven people, 2019. Disponível em: https://www.theguardian.com/technology/2019/oct/04/facial-recognition-row-police-gave-kings-cross-owner-images-seven-people. Acesso em: 11 out. 2019.

SCHNEIDER, Camila Berim; MIRANDA, Pedro Fauth Manhães. Vigilância Digital como instrumento de promoção da segurança pública. *Publicatio* – Ciências Sociais Aplicadas. Ponta Grossa, 28, 2020, p. 1-14.

SILVA, Rosane Leal; SILVA, Fernanda dos Santos Rodrigues. Reconhecimento facial e segurança pública: os perigos do uso da tecnologia do sistema penal seletivo brasileiro. *5º Congresso Internacional de Direito e Contemporaneidade*: mídias e direitos da sociedade em rede. Santa Maria, 2019.

SILVA, Tomaz. *Câmeras de reconhecimento facial levam a prisões no carnaval do Rio*. 2019. Disponível em: https://agenciabrasil.ebc.com.

br/geral/noticia/2019-03/cameras-de-reconhecimento-facial-levam-4-prisoes-no-carnaval-do-rio. Acesso em: 5 maio 2020.

THALES. *Biometrics*: authentication & identification (definition, trends, use cases, laws and latest news) – 2020 review. 2020. Disponível em: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics. Acesso em: 5 maio 2020.

TREVISAN, Beatriz. *Manifestantes usam* laser *contra câmeras de reconhecimento facial.* 2019. Disponível em: https://olhardigital.com.br/noticia/manifestantes-usam-laser-contra-cameras-de-reconhecimento-facial/88677. Acesso em: 25 jul. 2020.

UNIÃO EUROPEIA. *Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=EN. Acesso em: 6 maio 2020.

VETTORAZZO, Lucas; PITOMBO, João Pedro. *Rio e Salvador terão sistema de reconhecimento facial no Carnaval*. 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/02/rio-e-salvador-terao-sistema-de-reconhecimento-facial-no-carnaval.shtml. Acesso em: 7 maio 2020.

ANÁLISE DA LEI N. 12.654/2012, QUE PREVÊ A IDENTIFICAÇÃO E A INVESTIGAÇÃO CRIMINAL GENÉTICA, À LUZ DOS DIREITOS FUNDAMENTAIS

Felipe Bendlin[1]

RESUMO

A coleta de material genético e a criação de bancos de dados com perfis genéticos são uma realidade e uma tendência mundial. Conforme dados da Interpol, 73 países-membros já aderiram à prática. No Brasil, a Lei n. 12.654/2012 inovou prevendo essa possibilidade. Desse diploma extraem-se diversas previsões: (i) possibilidade de incluir a coleta de material genético para fins de identificação criminal (art. 5º, parágrafo único, da Lei n. 12.037/2009); (ii) criação de uma rede nacional de banco de dados de perfis genéticos (art. 5º-A e art. 7º-B da Lei n. 12.037/2009, bem como art. 9º-A, § 1º, da Lei n. 7.210/1984); (iii) possibilidade do uso da coincidência de perfis genéticos como prova pericial (art. 5º-A, § 3º, da Lei n. 12.037/2009); (iv) identificação obrigatória do perfil genético do condenado por crime doloso de

1 Bacharel em Direito pelas Faculdades Integradas do Vale do Iguaçu (Uniguaçu). Pós-graduado em Defesa Civil pela Faculdade São Braz. Bombeiro militar do Paraná.

natureza grave contra a pessoa ou crime hediondo (art. 9º-A da Lei n. 7.210/1984); e, por fim, (v) possibilidade do uso dos perfis genéticos armazenados nos Bancos de Dados de Perfis Genéticos como prova (art. 9º-A, § 2º, da Lei n. 7.210/1984).

Este artigo visa discutir o uso de banco de dados com perfis genéticos para a persecução penal perante os direitos fundamentais. A provável e até esperada negativa do acusado a submeter-se ao procedimento de coleta de material genético, amparado pelos direitos fundamentais, é o problema que se apresenta aqui. Entre as considerações feitas, verificou-se a possibilidade de algum tipo de responsabilização penal pela desobediência à coleta, conforme praticado nos Estados Unidos, sem ferir o direito à não autoincriminação. Analisa-se, ainda, o cabimento da coleta, de forma compulsória e alternativa, de uma interpretação desfavorável ao acusado que se recusar ao procedimento, conforme já ocorre no direito civil, com os exames de DNA para comprovação de paternidade.

Palavras-chave: Identificação criminal genética. Banco de dados de perfis genéticos. Investigação criminal genética.

ABSTRACT

The genetic material collection and the creation of databases with genetic profiles are a reality and a global trend, according to the INTERPOL 73 member countries have already joined the practice. In Brazil, the Law 12.654/2012 innovated providing this possibility. From the Law 12.654/2012 are extracted several legal possibilities: (i) the possibility of including the collection of genetic material for criminal identification purposes (article 5, sole paragraph, of Law 12.037/2009.); (ii) creation of a national network genetic profiles database (article 5-A and article 7-B of Law 12.037/2009 and article 9-A, first paragraph, of Law 7.210/1984); (iii) the possibility of using the coincidence of

genetic profiles as expert evidence (article 5-A, third paragraph, of Law 12.037/2009); (iv) mandatory identification of the genetic profile from people convicted for a crime of a serious nature against the person or heinous crime (article 9-A of Law 7.210/1984); and, finally, (v) the possibility of using genetic profiles stored in genetic profiles database as evidence (article 9-A, § 2º, of Law 7.210/1984). This article aims to discuss the need to use a database with genetic profiles for criminal prosecution without its implementation being a violation of fundamental rights. The likely and even expected negative from the accused to undergo this procedure, supported by fundamental rights, provides the main problem of this work. Among the considerations made in this article, there was the possibility of some type of criminal liability for disobedience to collection, as practiced in the United States, without harming the right to non-self-incrimination. It is also analyzed the appropriateness of the collection in a compulsory and alternative way of an unfavorable interpretation to the accused who refused the procedure, as already occurs in Civil Law, with DNA tests to prove paternity.

Keywords: Genetic criminal identification. Genetic profiles database. Genetic Criminal investigation.

1. ASPECTOS HISTÓRICOS, ATUAIS E LEGAIS SOBRE O USO DE BANCOS DE DADOS DE PERFIS GENÉTICOS PARA FINS FORENSES

Para iniciar uma abordagem a respeito deste assunto tão delicado, deve-se analisar os elementos obtidos desde o surgimento das técnicas de DNA até os mais modernos *softwares* de análise e combinação de dados.

Com vistas a uma melhor compreensão, são apresentadas as experiências de países onde o tema já está maduro, analisando-se de forma comparada e histórica os prós e contras por lá encontrados. Por fim, confronta-se o resultado obtido com a legislação dessa matéria no Brasil.

1.1 O DNA PARA FINS FORENSES

Apesar de o DNA ter sido descoberto, por volta de 1890, pelo médico bioquímico suíço Johham Friedrich Miescher (SAUTHIER, 2015), o grande avanço do ponto de vista forense ocorreu apenas em 1984, quando o pesquisador britânico Alec Jeffreys aprimorou a técnica para que, com pequenas quantidades de amostras biológicas, geralmente encontradas em cenas de crimes, fosse possível uma tipagem completa (BONACCORSO, 2010).

A nova técnica, chamada DNA LCN (*Low Copy Number*) – em uma tradução livre: baixo número de cópias de DNA –, permitiu a análise de amostras de material biológico em pequenas quantidades, submetendo-as a um número aumentado de ciclos, com vistas a maximizar os produtos anteriormente descartados, como uma gota de saliva em um copo onde o criminoso tenha bebido (ARAUJO, 2008).

Atualmente, o processo de identificação através do DNA evoluiu de forma tão extraordinária que faria inveja a Sherlock Holmes e a seu fiel escudeiro, dr. Watson. Impulsionados pelos atentados de 11 de setembro de 2001, pesquisadores americanos aprimoraram as técnicas de análise chegando ao ponto de realizarem mais de quinhentos testes por dia para identificar os corpos dilacerados das vítimas.

Em 1986, na cidade de Leicestershire – Inglaterra, foi realizada a primeira investigação criminal com uso de amostra de DNA encontrada em uma cena de homicídio. Duas meninas de quinze anos, Lynda Mann e Dawn Ashworth, foram assassinadas nos anos de 1983 e 1986, respectivamente. Apesar do lapso temporal entre os eventos, ambos apresentavam as mesmas características e similitudes no tocante ao *modus operandi*, o que fez com que as autoridades da época acreditassem se tratar de um único criminoso. Inicialmente, um jovem de dezessete anos havia confessado a autoria apenas do segundo homicídio, mas, ao se compararem amostras do DNA do sêmen encontrado nos corpos, concluiu-se que o mesmo autor havia cometido os dois crimes, como

suspeitado a princípio. Surpreendentemente, o rapaz não cometera nenhum deles. Como ainda não existia um banco de dados com perfis genéticos cadastrados para realizar uma comparação, foram necessários mais de cinco mil exames durante cerca de oito meses até se chegar a um acusado, Colin Pitchfork, o qual apresentou compatibilidade e, logo após, confessou os dois assassinatos (SAUTHIER, 2015).

Note-se, então, que uma amostra de DNA encontrada numa cena de crime, mesmo com as melhores técnicas de análise, sem um suspeito ou um banco de dados para que possa haver confronto, é praticamente inútil. Nesse sentido, estudos forenses britânicos constataram que, em cerca de 50% dos crimes contra o patrimônio, há vestígios dos quais é possível retirar uma amostra de DNA para análise; porém, em menos de 1% desses delitos, há um suspeito para comparação (PERÍCIA FEDERAL, 2007). No Brasil, por exemplo, antes da edição da Lei n. 12.654/2012 e do Decreto-Lei n. 7.950/2013, em mais de 70% dos casos em que a perícia coletava material biológico como vestígio, o exame de DNA sequer era realizado por falta de suspeitos para o confronto e de um banco de dados de referência (JACQUES, 2013).

Com o intuito de solucionar o problema, criaram-se os primeiros bancos de dados de perfis genéticos na década de 1990, na Inglaterra e nos Estados Unidos, com perfis de referência (SAUTHIER, 2015). Desse modo, casos antes tidos como sem suspeitos passaram a ter um acusado, e até mesmo casos antigos (*cold cases* – casos policiais não resolvidos) puderam ser elucidados (BONACCORSO, 2010).

Desde então, a implantação de bancos de dados de perfis genéticos tem-se tornado uma tendência mundial. De acordo com dados da Interpol[2], 73 países já adotaram esse sistema (INTERPOL, 2015), dos

2 "*Interpol is the world's largest international police organization, with 190 member countries. Our role is to enable police around the world to work together to make*

quais podemos citar: Alemanha, Austrália, Áustria, Bélgica, Canadá, Chile, Colômbia, Croácia, Dinamarca, Eslováquia, Espanha, Estônia, Finlândia, França, Holanda, Hungria, Itália, Islândia, Letônia, Noruega, Nova Zelândia, Panamá, Polônia, Portugal, República Tcheca, Singapura, Suécia e Suíça. O Brasil passou a fazer parte dessa lista com a Lei n. 12.654/2012, a qual modificou as de n. 12.037, de 1º de outubro de 2009, e n. 7.210, de 11 de julho de 1984 – Lei de Execução Penal. O diploma estabeleceu a tipagem genética como forma de identificação e investigação criminal e criou o banco de perfis genéticos para fins forenses (SAUTHIER, 2015), *in verbis*:

> Art. 1º O art. 5º da Lei n. 12.037, de 1º de outubro de 2009, passa a vigorar acrescido do seguinte parágrafo único:
>
> Art. 5º (...)
>
> Parágrafo único. Na hipótese do inciso IV do art. 3º, a identificação criminal poderá incluir a coleta de material biológico para a obtenção do perfil genético. (NR)
>
> Art. 2º A Lei n. 12.037, de 1º de outubro de 2009, passa a vigorar acrescida dos seguintes artigos:
>
> Art. 5º-A Os dados relacionados à coleta do perfil genético deverão ser armazenados em banco de dados de perfis genéticos, gerenciado por unidade oficial de perícia criminal. (Lei n. 12.654, de 28 de maio de 2012)

---

the world a safer place. Our high-tech infrastructure of technical and operational support helps meet the growing challenges of fighting crime in the 21st century." Em tradução livre: "Interpol é a maior organização policial do mundo, com 190 países-membros, Nosso papel é permitir que as polícias ao longo globo trabalhem juntas para torná-lo um lugar mais seguro. Nossa infraestrutura de alta tecnologia de apoio técnico e operacional ajuda a enfrentar os desafios crescentes de combate à criminalidade do século 21." (INTERPOL, 2016)

Posteriormente, o diploma foi regulamentado pelo Decreto n. 7.950/2013, o qual definiu a modalidade de retirada do perfil genético no prazo prescricional do delito ou em data anterior definida por decisão judicial e autorizou o uso de banco de dados para busca de pessoas desaparecidas.

1.2 BANCO DE DADOS DE PERFIS GENÉTICOS

Cabe ressaltar que, para a investigação com banco de dados de perfis genéticos funcionar, deve haver na verdade dois arquivos, o primeiro com amostras biológicas coletadas nos locais de crimes – sêmen, por exemplo. Já o segundo deve conter os perfis de referência coletados de acordo com a legislação de cada país – no Brasil, apenas condenados por crimes hediondos são obrigados a fornecer os dados, enquanto na Inglaterra qualquer pessoa detida pela polícia pode ser tipada (NETTO, 2007).

Assim que um perfil de referência é retirado sob qualquer circunstância, é enviado para comparação com o banco de amostras biológicas de locais de crimes:

> Quando os bancos de dados apontam para uma relação entre um provável criminoso e alguns indícios, surge o que na língua inglesa costuma ser denominado de *cold hit* ou, em tradução livre, "identificação a frio". É o caso de quando há comparação de um indício com outros e se conclui que uma série de delitos foi cometida por uma mesma pessoa, porque, por exemplo, o DNA retirado do sêmen coincide em todos os casos. (BONACCORSO, 2010)

Naturalmente, quanto maior a quantidade de dados de referência, maior a chance de sucesso em uma tentativa (*cold hit* – identificação

a frio[3]) de identificação genética de um crime até então sem suspeito.

Há ainda um banco de dados de perfis genéticos para identificação de desaparecidos. Nesse caso, também há um arquivo de amostras fornecidas voluntariamente por familiares; e um outro de vestígios extraídos de ossadas ou restos humanos não identificados (BONACCORSO, 2010).

Para o uso dos dados coletados, é necessário um sistema (*software)* de armazenamento, análise e combinação. Atualmente os mais usados com esse fim são o *Combined DNA Index System* (Codis), dos Estados Unidos da América; o *National DNA Databank* (NDNAD), da Inglaterra; o *European Molecular Biology Laboratory — Bank* (EMBL – Bank), da Europa; e o *Interpol DNA Database* (SAUTHIER, 2015).

Nos Estados Unidos, um dos pioneiros nesse assunto, foi desenvolvido em 1994 um sistema-piloto através da Lei de Identificação de DNA, que autorizou o banco de dados em nível nacional – o *National DNA Index System* (NDIS) – e especificou que tipos de dados poderiam ser mantidos. Em 1998, foi implementado o atual e talvez principal sistema da atualidade, o Codis (FBI, 2016).

O Codis, sistema utilizado atualmente pelo *Federal Bureau Investigation* (FBI), possui atualmente mais de 6,4 milhões de perfis de DNA de infratores cadastrados. Atualmente todos os 50 estados têm recolhido amostras de DNA dos condenados para alimentar o Codis. Além disso, em 26 deles, são também coletadas amostras dos investigados (FBI, 2016).

Em 2009, o Brasil assinou um termo de compromisso para utilização do Codis. Em 2010, foi realizada a maior instalação desse *software* fora dos Estados Unidos. Foram integrados 1 laboratório federal e 15 estaduais – Amazonas, Amapá, Bahia, Ceará, Espírito Santo, Minas Gerais, Mato Grosso do Sul, Pará, Paraíba, Paraná, Rio de Janeiro, Rio Grande

3 Termo utilizado para identificar de um suspeito unicamente por meio do banco de dados de perfis genéticos. Ver Sauthier (2015).

do Sul, Santa Catarina, São Paulo e Mato Grosso (GODINHO, 2014); além dos bancos nacionais, para uso criminal ou cível (TORRE, 2011).

Contudo, apenas em 2013 foram instituídos oficialmente, por meio do Decreto n. 7.950/2013, o Banco Nacional de Perfis Genéticos e a Rede Integrada de Bancos de Perfis Genéticos (RIBPG), com objetivos de coleta e integração de perfis genéticos voltados à elucidação de crimes, *verbis*:

> Art. 1º Ficam instituídos, no âmbito do Ministério da Justiça, o Banco Nacional de Perfis Genéticos e a Rede Integrada de Bancos de Perfis Genéticos.
>
> § 1º O Banco Nacional de Perfis Genéticos tem como objetivo armazenar dados de perfis genéticos coletados para subsidiar ações destinadas à apuração de crimes.
>
> § 2º A Rede Integrada de Bancos de Perfis Genéticos tem como objetivo permitir o compartilhamento e a comparação de perfis genéticos constantes dos bancos de perfis genéticos da União, dos Estados e do Distrito Federal.

O decreto supracitado também autoriza expressamente o uso dos dados coletados para a busca de pessoas desaparecidas: "Art. 8º O Banco Nacional de Perfis Genéticos poderá ser utilizado para a identificação de pessoas desaparecidas."

1.3 LEGISLAÇÃO

Assim como o Brasil, outros países tiveram que adequar suas leis para o uso de bancos de dados de perfis genéticos.

Nos Estados Unidos, por exemplo, inicialmente por meio da Lei *DNA Analyses Backlog Emininations Act of 2000*, autorizou-se a coleta apenas

para condenados por crimes previstos num rol taxativo. Porém, quatro anos mais tarde, com a Lei *Justice for All Act of 2004*, permitiu-se a coleta dos perfis de indiciados.

Ademais, o fornecimento de material biológico nos Estados Unidos é obrigatório. O procedimento é pré-requisito para a obtenção de benefícios ou, em caso de recusa, para incidência em um tipo de contravenção penal (LAIDANE, 2014). Pretende-se, com isso, priorizar a eficiência da persecução penal em relação às garantias individuais, tendo em vista a elucidação dos crimes.

Nos Estados Unidos, a aceitação desse método de investigação, identificação e prova é tão grande que existe até uma organização sem fins lucrativos associada com a Universidade de Yeshiva, *Cardozo School of Law* chamado *Innocence Project*, ou Projeto Inocência em tradução livre. O *Innocence Project* foi fundado em 1992 por Barry C. Scheck e Peter J. Neufeld para ajudar prisioneiros que poderiam ser inocentados com o auxílio do exame de DNA. Até agora, mais de trezentos acusados foram inocentados, incluindo vinte que estavam aguardando execução no corredor da morte.

No Brasil, a Lei n. 12.654/2012 tem sua origem no projeto de Lei n. 2.458/2011, de autoria do senador Ciro Nogueira (PP/PI). Após tramitação no Congresso Nacional, foi aprovado, sancionado pela presidente e publicado no *Diário Oficial da União* no dia 29 de maio de 2012 como lei, entrando em vigor em todo o território nacional a partir de novembro de 2012.

O diploma altera dispositivos de dois outros: os de n. 12.037/2009, ou Lei da Identificação Criminal, que trata da identificação criminal do civilmente identificado, e 7.210/1984, ou Lei de Execução Penal.

Com o novo regramento, dois modelos de coleta de perfil genético passaram a ser possíveis, um facultativo e outro obrigatório. O primeiro, inserido no parágrafo único do art. 5º da Lei da Identificação Criminal, trata da possibilidade de, no curso da investigação de um

delito, quando essencial à investigação policial, o acusado ser obrigado, para fins de identificação criminal, a fornecer, além dos já conhecidos dados datiloscópicos e fotográficos, amostras genéticas a critério da autoridade policial e com prévia autorização judicial para obtenção do perfil genético:

> Art. 5º (...)
> Parágrafo único. Na hipótese do inciso IV do art. 3º, a identificação criminal poderá incluir a coleta de material biológico para a obtenção do perfil genético. (Lei n. 12.654, de 28 de maio de 2012)

O segundo modelo, obrigatório, acrescentado no art. 9-A da Lei de Execuções Penais, ocorre em duas hipóteses: a) para os condenados por crimes dolosos com violência de natureza grave contra a pessoa; e b) após a condenação pelos crimes previstos no art. 1º da Lei n. 8.072/1990 – Lei dos Crimes Hediondos:

> Art. 9º-A Os condenados por crime praticado, dolosamente, com violência de natureza grave contra pessoa, ou por qualquer dos crimes previstos no art. 1º da Lei n. 8.072, de 25 de julho de 1990, serão submetidos, obrigatoriamente, à identificação do perfil genético, mediante extração de DNA – ácido desoxirribonucleico, por técnica adequada e indolor. (Lei n. 12.654, de 28 de maio de 2012)

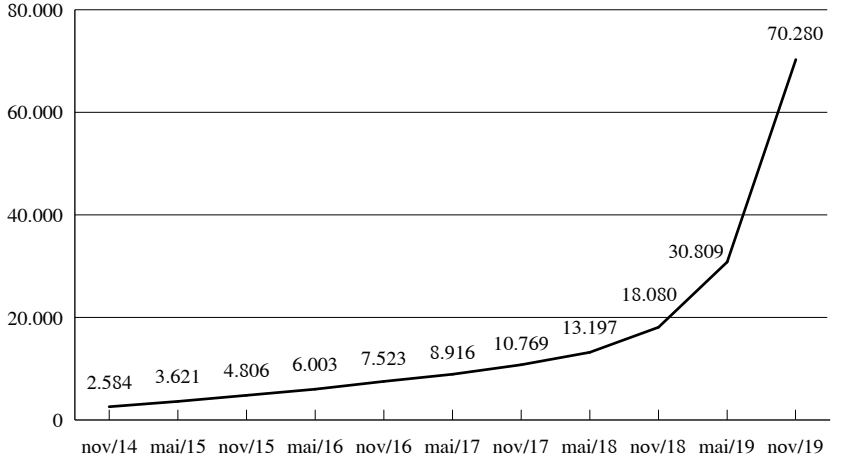
Em ambos os casos, o material genético deverá ser coletado de maneira adequada e indolor através da retirada de células da mucosa oral com uso de um *swab* (um tipo de cotonete estéril), conforme determina a Resolução n. 3, de março de 2014.

Contudo, somente a partir de 2018, com políticas públicas mais "eficientistas", tais como a Lei n. 13.964/2019, do então Ministro da Justiça e Segurança Pública, Sergio Moro, a Rede Integrada de Bancos

de Perfis Genéticos do Brasil começou a ser alimentada de maneira mais robusta.

Ao inserir-se na Lei de Execução Penal o § 8º ao art. 9º-A, tornou-se falta grave do condenado a não submissão a tipagem genética.

EVOLUÇÃO DAS AMOSTRAS TOTAIS NO BNPG



Fonte: XI Relatório da RIBPG (nov./2019).

Essas informações devem ser armazenadas em banco de dados de perfis genéticos gerenciado por unidade oficial de perícia criminal, pelo prazo para prescrição do delito ou data anterior definida por decisão em juízo. Todas poderão ser acessadas pelas autoridades policiais mediante autorização da Justiça (Decreto n. 7.950, de 12 de março de 2013).

Delineado esse panorama, constata-se que a investigação e identificação criminal genética são realidade e tendência mundiais e que, há alguns anos, chegou ao Brasil. Em decorrência disso, torna-se necessário um estudo aprofundado dos direitos fundamentais contidos na nossa Constituição Federal com vistas a solucionar a eterna tensão entre o eficientismo e o garantismo característicos do processo penal.

2. ANÁLISE DA LEI N. 12.654/2012 À LUZ DOS DIREITOS FUNDAMENTAIS

Extraem-se da Lei n. 12.654/2012 as seguintes disposições: (i) possibilidade de incluir a coleta de material genético para fins de identificação criminal (art. 5º, parágrafo único, da Lei n. 12.037/2009); (ii) criação de uma rede nacional de banco de dados de perfis genéticos (art. 5º-A e art. 7º-B da Lei n. 12.037/2009, bem como art. 9º-A, § 1º, da Lei n. 7.210/1984); (iii) possibilidade do uso da coincidência de perfis genéticos como prova pericial (art. 5º-A, § 3º, da Lei n. 12.037/2009); (iv) identificação obrigatória do perfil genético do condenado por crime doloso de natureza grave contra a pessoa ou crime hediondo (art. 9º-A da Lei n. 7.210/1984); e, por fim, (v) a possibilidade de uso dos perfis genéticos armazenados nos bancos de dados durante investigações criminais (art. 9º-A, § 2º, da Lei n. 7.210/1984).

2.1 IDENTIFICAÇÃO HUMANA

A identificação humana vem evoluindo ao longo da história, desde as amputações de orelhas, mãos e línguas previstas no Código de Hamurabi – 1700 a.C. –, passando por marcações a ferro e tatuagens, até os dias de hoje, com modernos e eficientes métodos datiloscópicos e de DNA (SAUTHIER, 2015).

Conforme ressalta Rosa (2015), o ato de identificar uma pessoa física é de tamanha importância que a ausência dela de forma inequívoca é causa de prisão cautelar nos termos do art. 313, parágrafo único, do Código de Processo Penal (CPP): "será admitida a prisão preventiva quando houver dúvida sobre a identidade civil da pessoa ou quando esta não fornecer elementos suficientes para esclarecê-la (...)".

A identificação de uma pessoa pode ser classificada em duas espécies, quais sejam: a *identidade civil*, obtida por meio de registros

oficiais, com nome, nacionalidade, filiação, profissão etc.; e a *identidade física,* que se refere ao corpo humano como um todo, sendo considerados tanto o fenótipo quanto o genótipo (SAUTHIER, 2015).

Na legislação brasileira, a *identidade civil* pode ser atestada conforme o art. 2º da Lei n. 12.037/2009, por meio de:

> I – carteira de identidade;
> II – carteira de trabalho;
> III – carteira profissional;
> IV – passaporte;
> V – carteira de identificação funcional;
> VI – outro documento público que permita a identificação do indiciado, além dos documentos militares.

Já a *física*, no processo penal, é conhecida como *identificação criminal*. Ela é considerada exceção desde a vigência da Constituição da República de 1988, que revogou o antigo entendimento do Supremo Tribunal Federal (STF), no enunciado n. 568 da Súmula, o qual não considerava constrangimento ilegal a identificação criminal do civilmente identificado. Em seu art. 5º, LVIII, a nova Constituição estabeleceu que este só poderá ser identificado criminalmente nos casos previstos de forma expressa em lei (SILVA, 2012).

Um bom método de identificação criminal, segundo Costa (2015), deve conter quatro fundamentos, dois de ordem biológica (*unicidade* e *imutabilidade*) e dois de ordem técnica (*classificabilidade* e *praticidade*). Ele explica:

> A *unicidade* é o conjunto de atributos que tornem o indivíduo diferente dos outros; *imutabilidade*: Os elementos registrados devem permanecer sempre, sem mudar e sem sofrer a ação de qualquer fator endógeno ou exógeno; os aspectos não mudam ao longo do tempo;

> *classificabilidade*: O método deve permitir não só uma classificação adequada, como também fácil, pois é necessária metodologia no arquivamento e rapidez e facilidade na busca dos registros. E, por fim, a *praticabilidade*, permitindo que o método disponha de elementos de fácil obtenção e registro. (COSTA *apud* SAUTHIER, 2015)

Há ainda um quinto fundamento, a *perenidade,* no qual as características identificáveis devem permanecer mesmo com o passar do tempo ou até com a morte (PORTAL DA EDUCAÇÃO, 2012).

2.2 IDENTIFICAÇÃO CRIMINAL

Como visto, a identificação criminal é considerada uma exceção no ordenamento jurídico pátrio. No entanto, é essencial à segurança quanto à aplicação das penas, pois a responsabilidade criminal é de caráter pessoal (ROSA, 2015).

Sendo assim, mesmo que em caráter excepcional, a Constituição da República prevê essa modalidade de identificação no inciso LVIII do art. 5º, que foi posteriormente regulamentado na Lei n. 12.037/2009, para diversas situações, *in verbis*:

> Art. 3º Embora apresentado documento de identificação, poderá ocorrer identificação criminal quando:
>
> I – o documento apresentar rasura ou tiver indício de falsificação;
>
> II – o documento apresentado for insuficiente para identificar cabalmente o indiciado;
>
> III – o indiciado portar documentos de identidade distintos, com informações conflitantes entre si;
>
> IV – a identificação criminal for essencial às investigações policiais, segundo despacho da autoridade judiciária competente, que decidirá de

ofício ou mediante representação da autoridade policial, do Ministério Público ou da defesa;

V – constar de registros policiais o uso de outros nomes ou diferentes qualificações;

VI – o estado de conservação ou a distância temporal ou da localidade da expedição do documento apresentado impossibilite a completa identificação dos caracteres essenciais.

Via de regra[4], a identificação criminal inclui o processo *datiloscópico*[5] e o *fotográfico*[6], os quais são juntados aos autos da comunicação da prisão em flagrante ou do inquérito policial – ou outra forma de investigação conforme prevê o art. 5º da Lei n. 12.037/2009 –, caso não haja identificação por meio de documento civil.

A novidade fica por conta da identificação criminal genética, tema do presente trabalho. Ela se diferencia do processo *datiloscópico* principalmente pela *perenidade*, pois os elementos utilizados para a tipagem genética resistem a longos lapsos temporais, durando inclusive após a morte. Em contraponto, esse método não é tão *praticável*, devido

---

4 "Pois se faz também registro das características físicas de identificação visual (como cor dos olhos, cabelo, pele, altura, peso, idade), dados sociofamiliares (como filiação, residência, local de atividade laboral, apelido), etc., além de todos os outros dados de interesse policial". (ALFERES, 2009)

5 A datiloscopia baseia-se na leitura das cristas papilares dos dedos, que são individuais, contendo particularidades e os mais diversos tipos de desenhos. Tais desenhos são imutáveis e podem ser observados a partir do sexto mês de vida intrauterina. É atualmente o método mais usado em todo o mundo devido sua *praticabilidade* (SAUTHIER, 2015).

6 Na identificação criminal, são feitas duas fotos, sendo uma de frente e outra de perfil direito, com a câmera na vertical e com fundo branco, focando o rosto do identificado, objetos como óculos, bonés etc. são retirados. Ver *Manual de Identificação Criminal do Paraná* (2016).

aos altos custos e treinamentos específicos para este tipo de atividade (SAUTHIER, 2015).

2.3 INVESTIGAÇÃO CRIMINAL GENÉTICA

Conforme se extrai do art. 5º, IV, da Lei n. 12.037/2009, a identificação criminal apresenta dupla função; ao mesmo tempo que identifica, propicia elementos fundamentais para a investigação, o que a torna preferível à persecução penal. Assim, uma impressão digital deixada em um local de crime e confrontada com a do suspeito, por exemplo, poderia revelar a autoria (SAUTHIER, 2015).

Com o advento da Lei n. 12.654/2012, no caso de a identificação criminal ser essencial às investigações policiais (art. 3º, IV, da Lei n. 12.037/2009), segundo despacho da autoridade judiciária competente, que decidirá de ofício ou mediante representação da autoridade policial, do Ministério Público ou da Defensoria Pública, a identificação criminal poderá incluir coleta de material biológico para obtenção do perfil genético (parágrafo único do art. 5º da Lei n. 12.037/2009, incluído pela Lei n. 12.654/2012).

Conforme ressalta Rosa (2015), a identificação criminal genética prevista no parágrafo único do art. 5º da Lei n. 12.037/2009 c/c o inciso IV do art. 3º do mesmo diploma não é mera identificação criminal, mas uma forma de produção antecipada de prova, e em razão disso não pode ser tratada como identificação e sim como investigação, respeitados os princípios inerentes à investigação, tais como *proporcionalidade, devido processo legal, não autoincriminação*.

Queijo (2012) corrobora tal entendimento, afirmando que, muito embora a identificação criminal não possa ser objeto de recusa do não identificado, tendo em vista que identificar um suspeito é uma obrigação

da autoridade policial[7], para que não se atinja esfera de terceiros, a Lei n. 12.654/2012 mascara o procedimento com investigação, uma vez que, de outro modo não seria possível a realização compulsória, por desrespeitar os princípios fundamentais como o *nemo tenenetur se detegere*.

Surge, assim, a questão focal do presente trabalho: um banco de dados apenas com perfis genéticos de voluntários não implicaria uma persecução penal eficiente. Diante disso, como lidar com a provável e até esperada recusa dos submetidos à tipagem genética?

2.4 NEGATIVA DE CONSENTIMENTO PARA COLETA DE FRAGMENTOS CORPORAIS MEDIANTE INTERVENÇÃO CORPORAL

O não consentimento para a coleta de fragmentos corporais é, portanto, o problema crucial para a implementação de uma investigação criminal mais eficiente, sem que o uso de banco de dados de perfis genéticos configure violação das garantias fundamentais conquistadas ao longo do tempo, como o *devido processo legal*, a *não autoincriminação (nemo tenetur se detegere)* e a *proporcionalidade* (SAUTHIER, 2015).

De acordo com Queijo (2012), da recusa do submetido à tipagem de perfil genético, nascem três possibilidades, quais sejam: i) imputação ao agente um tipo penal pela desobediência; ii) execução da tipagem com o emprego da força; e iii) interpretação desfavorável de tal atitude.

Ainda, o pacote de alterações trazidas em 2019, chamado "pacote anticrime" – Lei n. 13.964/2019 –, criou uma quarta forma de coerção

7 "A redação do art. 1º da Lei n. 12.037/2009 não deixa dúvidas quanto à obrigatoriedade, pois roga que o imputado *será* submetido à identificação criminal. Não dando assim possibilidade a interpretação ou discricionariedade do agente policial." (SAUTHIER, 2015)

do já condenado e cumprindo pena a realizar a tipagem genética. Foi incluído ao Art. 9º-A um novel § 8º, nos seguintes termos: "Constitui falta grave a recusa do condenado em submeter-se ao procedimento de identificação do perfil genético."

2.5 CRIME DE DESOBEDIÊNCIA COMO FORMA DE COAÇÃO DIANTE DA RECUSA DA SUBMISSÃO À TIPAGEM DE PERFIL GENÉTICO

Nos Estados Unidos, o indivíduo que se recusa a fornecer material genético incide em um tipo de contravenção penal, além de perder o direito a benefícios que envolvam sua liberdade. Ainda sobre a legislação norte-americana, há tempos que a coleta de material genético é considerada como forma de busca e apreensão, devendo preceder de mandado judicial motivado (LAIDANE, 2014). No entanto, mesmo com a aplicação dessas sanções, o condenado/acusado não estará livre de sofrer a coleta compulsória de material genético em caso de decisão judicial que avaliará a *special needs doctrine*[8] e a *totality of the circumstances*[9].

No Brasil, o crime de desobediência previsto no art. 330 do Código Penal (CP), estabelece como tipo penal a conduta de "desobedecer à ordem legal de funcionário público". Para configuração do delito, é necessário respeitar o princípio da legalidade, ou seja, deve haver, na

8 Exceção à Quarta Emenda, que permite buscas e apreensões sem mandado ou suspeito individualizado. A necessidade especial deve superar o interesse do Estado previsto na lei. Disponível em: https://www.quimbee.com/keyterms/special-needs--doctrine. Acesso em: 9 dez. 2020.

9 Uma consideração de todos os fatores que cercam um conflito. Pondera-se o grau de restrição ao direito individual com o benefício do interesse do Estado. Disponível em: https://www.quimbee.com/keyterms/totality-of-the-circumstances. Acesso em: 9 dez. 2020.

lei, a obrigação da conduta da qual o agente de forma *passiva*[10] e dolosa se abstém de fazer (DIREITO A SABER DIREITO, 2016).

A seguir é apresentado julgado do Tribunal de Justiça do Rio Grande do Sul, no qual, por ausência de previsão legal para a conduta de colocar as mãos na cabeça, o crime de desobediência foi considerado como atípico:

> APELAÇÃO-CRIME. ARTIGO 330 DO CÓDIGO PENAL. DESOBEDIÊNCIA. ATIPICIDADE. SENTENÇA MANTIDA.
>
> 1. Atipicidade de conduta que se reconhece. Caso, em que o agente é processado por ter se negado a colocar "*as mãos na cabeça*".
>
> 2. Mesmo que o art. 330 do Código Penal configure tipo penal aberto, não se pode abrir espaço para criminalizar qualquer comportamento, haja vista que nem toda ordem desobedecida compõe o delito.
>
> 3. O princípio da legalidade impõe que a ordem seja formal e materialmente legal, segundo ensina Rogério Greco. Encostar em muros, em paredes, ajoelhar no chão, deitar no chão, entre outras, são práticas desajustadas aos princípios legais que norteiam o direito positivo brasileiro, embora possam ser adequadas a uma ou outra situação específica, favoráveis apenas à técnica de abordagem policial, referida na denúncia.
>
> 4. Nesse contexto sobressai a disposição constitucional segundo a qual "ninguém será obrigado a fazer ou deixar de fazer alguma coisa, senão em virtude de lei" (art. 5º, inc. II, da Constituição da República). Ferrajoli adverte a tal respeito, ao referir que "é punível só aquilo que é proibido pela lei, tudo o que a lei não proíbe não é punível, mas é livre ou permitido".

10 Para Greco (2014, p. 529), o crime de desobediência deve ser passivo, pois do contrário estaríamos diante do crime de resistência previsto no art. 329 do Código Penal, muito mais grave.

> 5. Tampouco há que se cogitar que eventual disposição normativa infralegal, como Nota de Instrução ou Resolução de caráter genérico, possa conferir poderes para exigir determinada conduta, pena de desobediência. A própria teoria dos poderes implícitos deve ser vista com reservas, como referiu o Min. Celso de Mello, ao apreciar o HC 94.173/BA. Não se pode cogitar que encargo atribuído a determinado órgão de Estado implique deferimento implícito de todo e qualquer meio necessário à ultimação dos fins a ele atribuídos.
>
> 6. Se a ordem desobedecida fosse de apresentar documentos, de permitir revista ou busca pessoal, nos casos dos arts. 240 e 244 do CPP, diversa poderia ser a situação.
>
> 7. Não havendo lei que determine a obrigatoriedade da conduta imputada pela denúncia, a desobediência à ordem de "colocar as mãos na cabeça" não caracteriza crime. (EJC n. 71005712732 – n. CNJ: 0042375-98.2015.8.21.9000 – 2015/Crime)

Marteleto Filho (2012) afirma que a Lei n. 12.654/2012 não autorizou intervenções corporais no Brasil, logo não seria possível aplicar um crime de desobediência sem a previsão legal à qual o sujeito está de fato desobedecendo, previsão essa que deve ser expressa e taxativa quanto ao método e à situação à qual se aplicaria.

Greco (2014) afirma que, quando a conduta, mesmo que prevista em lei, puder causar prejuízo ou autoincriminação do agente, se praticá-la, este não pode ser punido pelo seu não cumprimento, afastando-se assim o delito de desobediência.

Nesse sentido a Suprema Corte decidiu:

> *HABEAS CORPUS*. CRIME DE DESOBEDIÊNCIA. RECUSA A FORNECER PADRÕES GRÁFICOS DO PRÓPRIO PUNHO, PARA EXAMES PERICIAIS, VISANDO A INSTRUIR PROCEDIMEN-

TO INVESTIGATÓRIO DO CRIME DE FALSIFICAÇÃO DE DOCUMENTO. *NEMO TENETUR SE DETEGERE*.

Diante do princípio *nemo tenetur se detegere*, que informa o nosso direito de punir, é fora de dúvida que o dispositivo do inciso IV do art. 174 do Código de Processo Penal há de ser interpretado no sentido de não poder ser o indiciado compelido a fornecer padrões gráficos do próprio punho, para os exames periciais, cabendo apenas ser intimado para fazê-lo a seu alvedrio. É que a comparação gráfica configura ato de caráter essencialmente probatório, não se podendo, em face do privilégio de que desfruta o indiciado contra a autoincriminação, obrigar o suposto autor do delito a fornecer prova capaz de levar à caracterização de sua culpa. Assim, pode a autoridade não só fazer requisição a arquivos ou estabelecimentos públicos, onde se encontrem documentos da pessoa a qual é atribuída a letra, ou proceder a exame no próprio lugar onde se encontrar o documento em questão, ou ainda, é certo, proceder à colheita de material, para o que intimará a pessoa, a quem se atribui ou pode ser atribuído o escrito, a escrever o que lhe for ditado, não lhe cabendo, entretanto, ordenar que o faça, sob pena de desobediência, como deixa transparecer, a um apressado exame, o CPP, no inciso IV do art. 174. *Habeas corpus* concedido.

Extrai-se do acórdão que, pelo privilégio que o princípio do *nemo tenentur se detegere* confere aos acusados, o indiciado não tem o dever de colaborar com a investigação, e diante da ausência desse dever, nenhuma sanção é cabível (GRECO, 2014).

Por fim, mesmo que aplicado um delito de desobediência, não teríamos solucionado o impasse que hora se apresenta, continuando ainda sem a total eficácia da Lei n. 12.654/2012, ou seja, sem a amostra biológica do acusado (SAUTHIER, 2015).

2.6 TIPAGEM GENÉTICA COMPULSÓRIA

Para Sauthier (2015), esta é a única saída diante da recusa para que a identificação e investigação criminal genética não acabem por se tornarem obsoletas, não atingindo assim o fim esperado pela persecução penal.

O autor ressalta que esse é o meio utilizado pela maioria dos países em que se pratica a identificação e investigação criminal genética, priorizando-se o *persecutio criminis* em detrimento de diversos direitos de defesa do acusado.

Marteleto Filho (2012), por sua vez, considera que a tipagem genética compulsória esbarra no princípio da legalidade, pois a lei é silente sobre o emprego de coerção física, ainda mais em se tratando de princípios fundamentais tão relevantes, como a integridade física e a não autoincriminação. Em seu entendimento, para habilitarem-se intervenções corporais no Brasil, haveria a necessidade de uma lei mais específica e com estrita observância do princípio da proporcionalidade.

Rosa (2015) lembra que o recolhimento de material genético para comparação deixado no local do crime é plenamente cabível e não exige autorização judicial. Já a obtenção que exija método *invasivo*[11] está vedada, por violar a dignidade humana transformando o acusado em objeto de prova.

Queijo (2012) assenta que, por se tratar de instrumento probatório, a coleta compulsória afetaria diretamente o princípio *nemo tenetur se detegere*. A lei deveria, assim, prever de forma expressa, e em casos

11 Morais (2015, p. 238) preleciona quanto às provas invasivas: "são as intervenções corporais que pressupõem penetração no organismo humano, por instrumentos ou substâncias, em cavidades naturais ou não, implicando na utilização (ou extração) de alguma parte dele ou na invasão física do corpo humano (...)."

excepcionais, outros meios de prova antes desta, tão invasiva, de modo a priorizar o respeito ao princípio da proporcionalidade (proporcionalidade em sentido estrito, vide 3.3 do presente trabalho).

Não obstante, o Comitê Gestor da Rede Integrada de Bancos de Perfis Genéticos, por meio do art. 8º da Resolução n. 3/2014, consignou que, em caso de recusa, a coleta não deve ser realizada, ou seja, afastou a possibilidade da via coativa de coleta.

2.7 INTERPRETAÇÃO DESFAVORÁVEL DIANTE DA RECUSA

A solução adotada, principalmente no direito civil, é a presunção da culpabilidade (SAUTHIER, 2015), conforme prevê o art. 232 do Código Civil: "a recusa à perícia médica ordenada pelo juiz poderá suprir a prova que se pretendia obter com o exame", a exemplo dos casos de exames de DNA para confirmar a paternidade.

Porém, mesmo na seara civil, a presunção de culpabilidade diante da recusa de submeter-se a exame de DNA é relativa (*juris tantum*), conforme pode se extrair do enunciado n. 301 da Súmula do Superior Tribunal de Justiça, *in verbis*: "Em ação investigatória, a recusa do suposto pai a submeter-se ao exame de DNA induz presunção *juris tantum* de paternidade."

Para Oliveira (2008), essa seria a alternativa a ser empregada também no processo penal, pois uma recusa, sem causa justa, a um meio de prova legal que comprovadamente não coloque em risco o acusado abriria a possibilidade de interpretação em seu desfavor.

> (...) o Juiz Criminal, quando diante de um quadro probatório existente, mas ainda insuficiente, possa valer-se da presunção (legal) para, diante da ausência de explicações minimamente razoáveis para a citada

> recusa (ao meio de prova válido), convencer-se em um outro sentido. (OLIVEIRA, 2008)

Todavia, no processo penal, temos o ampliado princípio *nemo tenetur se detegere*, que, como já vimos, se manifesta em diversos outros preceitos.

Rosa (2015) afirma que, pelo princípio da presunção de inocência, o acusado deve iniciar a ação penal como absolvido, inocente, e só perder esse *status* ao final do processo, quando provada sua culpa. A carga probatória fica toda por conta da acusação.

O próprio CPP dispõe, no parágrafo único do art. 186, que: "O silêncio, que não importará em confissão, não poderá ser interpretado em prejuízo da defesa." Já Lopes Júnior (2006) lembra que essa postura engloba qualquer dever de contribuir contra sua própria condenação, seja no momento da defesa oral, seja na participação de reconstruções de cenas de crimes.

Desse modo, tanto a doutrina majoritária quanto a jurisprudência pátria entendem que não é possível nem cabível, diante da recusa do réu em submeter-se às provas que possam incriminá-lo, extrair qualquer presunção de culpabilidade (QUEIJO, 2012).

3. CONCLUSÃO

Diante da análise realizada por este trabalho, é possível verificar algumas questões que tomam conta do cenário jurídico brasileiro, atualmente marcado pela crescente tendência à relativização das garantias fundamentais em prol de políticas criminais que prometem resolver os problemas da segurança pública com o direito penal. Tais práticas, muitas vezes inconstitucionais e violadoras de garantias fundamentais inerentes ao Estado Democrático de Direito, legitimam-se pelo simples

argumento de que conseguiremos punir mais e colocar mais criminosos atrás das grades.

Nesse ponto, o processo penal passa por um momento delicado e perigoso, pois nessa área do direito lidamos com a liberdade dos cidadãos e há de se ter muito cuidado para não se cometer injustiça, conforme a velha máxima: mais vale um criminoso solto que um inocente preso. Ademais, punir a qualquer custo vai de encontro a tudo que conquistamos com o processo penal *acusatório*, e nos traz a sombra das barbáries realizadas na Idade Média, no processo penal *inquisitório*, com os mesmos argumentos de punir mais e mais.

Quanto ao tema do presente trabalho, trata-se de uma inovação legal que funde tecnologia com ciência, tendência mundial, e que traz possibilidades interessantíssimas na busca por resoluções de delitos. Os exames de DNA têm seu maior diferencial na *perenidade* das amostras biológicas, pois, diferentemente das digitais, perduram por muitos anos, inclusive após a morte.

Vale lembrar que a coleta de material genético voluntário sempre foi permitida, uma vez que se trata de um meio de prova pericial, podendo ser requerido por qualquer uma das partes. Contudo, o grande problema enfrentado aqui se dá quanto à recusa do acusado em submeter-se à coleta de material genético.

Primeiramente indagou-se a respeito do cabimento de algum tipo de responsabilização penal pela desobediência, conforme exemplo dos Estados Unidos, onde a recusa obriga o acusado a responder por contravenção penal e a abrir mão de benefícios processuais. Essa possibilidade, contudo, já foi refutada, no Brasil, pelo fato de a Lei n. 12.654/2012 não prever expressamente a coleta compulsória. Além disso, o Supremo Tribunal Federal, em julgamento de situação semelhante, qual seja, a do exame grafotécnico, entendeu não caber punição ao acusado por exercer seu direito à não autoincriminação.

Depois analisou-se o cabimento da coleta de forma compulsória, que,

conforme doutrina majoritária pesquisada, parece a única solução para se obter real eficácia na identificação e investigação criminal genética. Entretanto, essa solução esbarra em importantes princípios, como o da *legalidade*, *proporcionalidade* e *dignidade da pessoa humana*. Vale lembrar que, por não serem absolutos, tais preceitos devem ser sopesados com bastante cuidado, o que parece não ter ocorrido com a Lei n. 12.654/2012, dado que não houve nesse diploma previsão expressa quanto à coleta compulsória, bem como aos crimes nos quais o procedimento seria cabível.

Por fim, arguiu-se a alternativa de uma interpretação desfavorável ao acusado que se recusasse ao procedimento, conforme já vemos em larga escala no direito civil, com os exames de DNA para comprovação de paternidade. Todavia, no direito penal, temos que a carga probatória é toda por conta da acusação; logo, não estamos falando de um hipossuficiente, mas de toda a máquina estatal contra o acusado, considerada a presunção legal de inocência.

Conclui-se, diante desse contexto, que a Lei n. 12.654/2012, muito embora tenha a intenção de trazer avanços ao sistema de identificação e persecução penal atual, na busca da elucidação dos delitos, não se presta para o fim esperado, estando fadada a cair na obsolescência, em razão da maneira como veio redigida, silente quanto à previsão expressa da coleta coercitiva de material genético.

REFERÊNCIAS

ALFERES, Eduardo Henrique. Lei n. 12.037/2009: novamente a velha identificação criminal. *Revista Jus Navigandi*, Teresina, ano 15, n. 2554, jun. 2010. Disponível em: https://jus.com.br/artigos/15124. Acesso em: 15 nov. 2020.

ARAUJO, Tarso. Ciência contra o crime: a ciência e a tecnologia es-

tão revolucionando a perícia criminal e tornando o trabalho dos CSI de verdade muito mais incrível do que na ficção. *Superinteressante*, vol. 257, out. 2008. Disponível em: http://super.abril.com.br/ciencia/ciencia-contra-o-crime. Acesso em: 12 mar. 2016.

BONACCORSO, Norma Sueli. *Aspectos técnicos, éticos e jurídicos relacionados com a criação de bancos de dados criminais de DNA no Brasil*. 2010. Tese (Doutorado em Direito Penal). Faculdade de Direito, Universidade de São Paulo, São Paulo, 2010. Disponível em: http://www.teses.usp.br/teses/disponiveis/2/2136/tde-04102010-141930/. Acesso em: 28 fev. 2016.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 5 abr. 2016.

BRASIL. *Decreto n. 7.950, de 12 de março de 2013*. Brasília, Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7950.htm. Acesso em: 3 abr. 2016.

BRASIL. *Decreto-Lei n. 2.848, de 7 de dezembro de 1940.* Código Penal. Brasília, Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 15 maio 2016.

BRASIL. *Decreto-Lei n. 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Rio de Janeiro, Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 1º jul. 2016.

BRASIL. *Lei n. 7.210 de 11 de julho de 1984*. Lei de Execução Penal. Brasília, Presidência da República. Casa Civil. Subchefia para Assun-

tos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L7210.htm. Acesso em: 25 jul. 2016.

BRASIL. *Lei n. 10.406, de janeiro de 2002*. Código Civil. Brasília, Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 26 jul. 2016.

BRASIL. *Lei n. 12.037, de 1º de outubro de 2009*. Brasília, Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12037.htm. Acesso em: 5 jul. 2016.

BRASIL. *Lei n. 12.654, de 28 de maio de 2012*. Brasília, Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12654.htm. Acesso em: 21 mar. 2016.

BRASIL. *Lei n. 13.964, de 24 de dezembro de 2019*. Brasília, Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13964.htm. Acesso em: 16 out. 2020.

BRASIL. Ministério da Justiça e Segurança Pública. *Resolução n. 3, de março de 2014*. Brasília, Disponível em: http://www.justica.gov.br/sua-seguranca/ribpg/resolucoes/resolucao3-coleta_12654.pdf. Acesso em: 23 jul. 2016.

BRASIL. Supremo Tribunal Federal. *ADI 855/PR*. Rel. min. Sepúlveda Pertence. Julgado em 2 mar. 2008. *DJe* 26 mar. 2009. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=583759. Acesso em: 4 jul. 2016.

CAPEZ, Fernando. *Curso de direito penal*: parte geral. 11. ed. São Paulo: Saraiva, 2007.

CAPEZ, Fernando. *Curso de processo penal*. 21. ed. São Paulo: Saraiva, 2014.

DIREITO A SABER DIREITO. 2016. Disponível em: http://caduchagas.blogspot.com.br/2016/05/art-330-desobediencia-codigo-penal.html. Acesso em: 10 jul. 2016.

ESTADOS UNIDOS DA AMÉRICA. Federal Bureau of Investigation. *CODIS-NDIS Statistics*. Disponível em: https://www.fbi.gov/about-us/lab/biometric-analysis/codis/ndis-statistics. Acesso em: 3 abr. 2016.

ESTADOS UNIDOS DA AMÉRICA. Federal Bureau of Investigation. *Frequently Asked Questions (FAQs)*. Disponível em: https://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-fact-sheet. Acesso em: 3 abr. 2016.

ESTADOS UNIDOS DA AMÉRICA.. Lei n. 106-546, de 19 de dezembro de 2000. *DNA Analysis Backlog Elimination Act of 2000*. EUA, Disponível em: https://www.congress.gov/106/plaws/publ546/PLAW-106publ546.pdf. Acesso em: 3 abr. 2016.

ESTADOS UNIDOS DA AMÉRICA. Lei n. 108-405, de 30 de outubro de 2004. *Justice For All Act Of 2004*. EUA, Disponível em: https://www.congress.gov/108/plaws/publ405/PLAW-108publ405.pdf. Acesso em: 3 abr. 2016.

GODINHO, Neide Maria de Oliveira. Banco de dados de DNA: uma ferramenta a serviço da justiça. *Rebesp*, Goiânia, v. 7, n. 2, 2014. Disponível em: https://revista.ssp.go.gov.br/index.php/rebesp/article/view/193. Acesso em: 3 abr. 2016.

GRECO, Rogério. *Curso de direito penal*: parte especial, vol. 4. Rio de Janeiro: Impetus, 2014.

GRECO, Rogério. *Curso de direito penal*: parte geral. Rio de Janeiro: Impetus, 2014.

INTERPOL. *Connecting Police for a Safe World*. Disponível em: http://www.interpol.int/INTERPOL-expertise/Forensics/DNA. Acesso em: 3 abr. 2016.

JACQUES, Guilherme. Banco de perfis genéticos: A ciência em prol da justiça. *Revista Jurídica Consulex*, vol. 369, 1º abr. 2013.

JACQUES, Guilherme Silveira; MINERVINO, Aline Costa. Aspectos éticos e legais dos bancos de dados de perfis genéticos. *Revista Perícia Federal,* Brasília, ano IX, n. 26, p. 17-20, jun./2007-ago./2008. Disponível em: https://apcf.org.br/cat/revistas/. Acesso em: 21 mar. 2016.

LAIDANE, Carolina Franco Rodrigues. Banco de dados de criminosos: a lição norte-americana. *Revista de Doutrina da 4ª Região*, Porto Alegre, n. 62, out. 2014. Disponível em: http://www.revistadoutrina.trf4.jus.br/artigos/edicao062/Carolina_Laidane.html. Acesso em: 16 fev. 2016.

LIMA, George Marmestein. As funções dos princípios constitucionais. *O neofito*: informativo jurídico. 2002. Disponível em: http://egov.ufsc.br/portal/sites/default/files/anexos/14051-14052-1-PB.pdf. Acesso em: 15 mai. 2016.

LOPES JR., Aury. *Introdução crítica ao processo penal*: fundamentos da instrumentalidade constitucional. Rio de Janeiro: Lumen Juris, 2006.

MARTELETO FILHO, Wagner. *O direito à não autoincriminação no processo penal contemporâneo*. Belo Horizonte: Del Rey, 2012.

NETTO, Octavio Brandão Caldas. *Perícia federal*: banco de dados de

perfis genéticos – o DNA a serviço da justiça. Brasil: APCF, v. 26, jun. 2007. Disponível em: https://apcf.org.br/cat/revistas/. Acesso em: 28 fev. 2016.

NUCCI, Guilherme de Souza. *Manual de direito penal*. 9. ed. São Paulo: Revista dos Tribunais, 2012.

NUSSBAUM, Robert L.; MCLNNES, Roderick R.; WILLARD, Huntington F. *Genética médica*. 7. ed. Rio de Janeiro: Saunders Elsevier, 2007.

OLIVEIRA, Eugênio Pacelli de. *Curso de processo penal*. Rio de Janeiro: Lumen Juris, 2008.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Convenção americana sobre direito humanos:* Pacto de São José da Costa Rica. 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 15 maio 2016.

PARANÁ. *Manual de identificação criminal do Paraná*. Disponível em: http://www.institutodeidentificacao.pr.gov.br/arquivos/File/Manual%20de%20Identificacao%20Criminal%20-%20Versao%203.pdf. Acesso em: 15 jul. 2016.

PORTAL DA EDUCAÇÃO. *Tipos de identificação criminal*. 2012. Disponível em: https://siteantigo.portaleducacao.com.br/conteudo/artigos/medicina/tipos-de-identificacao-criminal/13603#:~:text=Segundo%20Esp%C3%ADndula%20(2007)%2C%20a,na%20identifica%C3%A7%C3%A3o%20de%20uma%20pessoa. Acesso em: 30 jul. 2016.

PROJECT, Innocence. *Our Work*. Disponível em: http://www.innocenceproject.org/free-innocent. Acesso em: 3 abr. 2016.

QUEIJO, Maria Elizabeth. *O direito de não produzir prova contra si mesmo*: o princípio *nemo tenetur se detegere* e suas consequências no processo penal. São Paulo: Saraiva, 2012.

RABELO, Graziele Martha. O princípio da proporcionalidade no Direito Penal. *Âmbito Jurídico*, Rio Grande, XII, n. 71, dez 2009. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/o-principio-da-proporcionalidade-no-direito-penal/#:~:text=O%20princ%C3%ADpio%20da%20proporcionalidade%20integra,a%20prote%C3%A7%C3%A3o%20dos%20interesses%20p%C3%BAblicos. Acesso em: jul. 2016.

ROSA, Alexandre Morais da. *Guia compacto do processo penal conforme a teoria dos jogos*. Florianópolis: Empório do Direito, 2015.

SAUTHIER, Rafael. *A identificação e a investigação criminal genética*: à luz dos direitos fundamentais e da Lei 12.654/2012. Curitiba: CRV, 2015.

SILVA, Maíra Saad da. *Análise da Constitucionalidade da Lei n. 12.654/2012 que Prevê a Coleta de Perfil Genético como Forma de Identificação Criminal e dá Outras Providências*. 2012. 63 f. Monografia. Curso de Bacharel em Direito, Centro Universitário de Brasília – Uniceub Faculdade de Ciências Jurídicas e Sociais – Fajs, Brasília, 2012. Disponível em: https://core.ac.uk/download/pdf/185253949.pdf. Acesso em: 15 maio 2016.

TORRE, Senador Demóstenes. *Parecer*. Brasília: Senado, 2011. Disponível em: http://legis.senado.leg.br/mateweb/arquivos/mate-pdf/94995.pdf. Acesso em: 3 abr. 2016.

APONTAMENTOS SOBRE A ANÁLISE DE DNA E OS BANCOS DE DADOS DE PERFIS GENÉTICOS PARA FINS CRIMINAIS À LUZ DOS DIREITOS FUNDAMENTAIS

Thales Messias Pires Cardoso[1]

RESUMO

O presente trabalho objetiva examinar como o uso da tecnologia afeta os direitos fundamentais, especificamente quanto à utilização para a persecução penal de dados genéticos identificativos, os perfis genéticos, únicos para cada indivíduo. Aborda, com referência ao direito comparado, os dois momentos cruciais da análise de DNA: o da obtenção das amostras de DNA, inclusive mediante intervenção corporal, e o tratamento dos perfis genéticos, principalmente no que toca a seu armazenamento em banco de dados. O estudo pretende demonstrar, ainda, que o emprego dessa ferramenta para a persecução penal é admissível

1 Graduado em direito pela Universidade de São Paulo. Especialista em direito público pela Escola Paulista da Magistratura e em controle, detecção e repressão a desvios de recursos públicos pela Universidade Federal de Lavras. Mestrando em direito constitucional pela *Universidad de Sevilla*. Procurador da República e professor convidado da Universidade de Uberaba.

à luz da Constituição Federal, desde que observada a dignidade humana e a proporcionalidade da intervenção relativamente aos direitos fundamentais, em especial os referentes à intimidade e privacidade, à proteção de dados pessoais, à integridade física, à não produção de provas contra si mesmo e à presunção de inocência.

Palavras-chave: Direitos fundamentais. Perfil genético. Análise de DNA. Intervenções corporais. Banco de dados de perfis genéticos.

ABSTRACT

This paper aims to examine how the use of technology affects fundamental rights, specifically the use of genetic profiles for the criminal prosecution. It addresses, with references to the comparative law, the two crucial moments of DNA analysis for this purpose: the collection of DNA samples, including taken from a person, and the treatment of genetic profiles, especially with regard to their storage in a database. It intends to demonstrate that the use of this tool for criminal prosecution observing human dignity and the principle of proportionality when intervening in fundamental rights, especially the rights to privacy, to the protection of personal data, to physical integrity, against self-incrimination, and to innocence, is compatible to the Brazilian Constitution.

Keywords: Fundamental rights. Genetic profile. DNA analysis. Bodily interventions. Database of genetic profiles.

1. A ANÁLISE DE ÁCIDO DESOXIRRIBONUCLEICO (DNA) E SUAS DIFERENTES APLICAÇÕES

O progresso tecnológico gera profundas mudanças não só nas relações humanas mas também entre o homem e a natureza. Com isso, emergem novas realidades determinadas por circunstâncias como a

globalização, a internet, a exaustiva exploração dos recursos naturais e os avanços da biotecnologia, as quais afetam os direitos e a liberdade das pessoas em escala planetária. Em consequência, nas últimas décadas, o processo histórico de reivindicação dos direitos humanos se concentrou nessas questões, trazendo à tona os direitos de terceira geração, cuja referência está no princípio da solidariedade e inclui a busca da paz e a melhoria da qualidade de vida em relação à biotecnologia e aos avanços da ciência da computação (PEREZ LUÑO, 2006, p. 30-35).

Nesse contexto, a biotecnologia, expressão cunhada em 1914 pelo engenheiro agrônomo húngaro Karl Ereky, é definida por Muñoz de Malajovich (2012, p. 26) como "uma atividade baseada no conhecimento multidisciplinar, que utiliza agentes biológicos para fazer produtos úteis ou resolver problemas". A genética é um ramo da biotecnologia, cujos avanços têm grande relevância na medicina, permitindo a prevenção e tratamento de doenças, reprodução assistida e precisão na identificação humana (PIERCE, 2012, p. 3-5).

O Projeto Genoma Humano, um esforço internacional de treze anos, representou um marco no estudo da genética. Iniciado em 1990, foi concluído em 2003. O genoma é o mapa dos genes, que contém todas as informações necessárias armazenadas no DNA das células humanas para formar e manter os seres vivos ao longo de suas vidas (ÁLVARES GONZÁLES, 2017, p. 11). O projeto mapeou e sequenciou 99% do genoma, utilizando métodos matemáticos e computacionais. Todo o resultado dessa pesquisa foi guardado em enormes bancos de dados, que servem de base para múltiplas aplicações práticas e novas pesquisas (U.S. DEPARTMENT OF ENERGY, 1990-2003).

O genoma humano possui um componente material, a molécula de DNA, que carrega seu elemento intangível, ou seja, as informações transportadas pelos genes, relacionadas às características hereditárias das pessoas, o que permite a identificação única de cada indivíduo (NICOLÁS JIMÉNEZ, 2006, p. 105). Assim, o DNA guarda a herança

genética e proporciona a individualização dos seres humanos, cujos traços diferenciais se manifestam no fenótipo. O DNA também é a base molecular para a evolução (MORENTE PARRA, 2011, p. 34), pois as crianças não necessariamente herdam as mutações de seus pais causadas por imperfeições tênues em sua replicação (NICOLÁS JIMÉNEZ, 2006, p. 105).

Apesar de sua importância, apenas uma pequena parte do genoma é composta de DNA codificado, dotado de sequências para produção de proteínas que indicam características físicas ou patológicas da pessoa. Cerca de 98% do genoma é composto por *sequências de DNA não codificadas*[2], localizadas entre genes, que possuem outras funções orgânicas, não diretamente relacionadas à herança, mas *fundamentais para fins identificativos* (NATIONAL HUMAN GENOME RESEARCH INSTITUTE).

A pesquisa das informações contidas no DNA humano resultou em várias aplicações, que aumentam com o tempo, de acordo com as necessidades e o desenvolvimento tecnológico (GÓMEZ SÁNCHEZ, 2008, p. 68). Em geral, essas diferentes aplicações podem ser reunidas em três grupos principais: prevenção, diagnóstico e tratamento de doenças; pesquisa científica; e identificação (NICOLÁS JIMÉNEZ, 2006, p. 35-50).

Interessa ao presente artigo a análise de DNA destinada à identificação. Essa examina, em suma, as variantes de uma determinada sequência de DNA, os polimorfismos, os quais se manifestam no DNA não codificante, que, conforme mencionado, forma a maior parte do

2 Embora seja chamada de DNA lixo (*Junk DNA*), porque não tem funções de produção de proteínas, sabe-se que essa parte majoritária do genoma pode ser útil para a estabilidade da molécula de DNA no núcleo celular (BECHMULLER LIMA, 2007, p. 7-10).

genoma[3]. Trata-se da prova forense, que serve a finalidades legais, como o esclarecimento da autoria de crimes, a verificação de vínculos familiares biológicos e o reconhecimento de vítimas de crimes e desastres.

2. A IMPRESSÃO DIGITAL GENÉTICA ÚNICA DE CADA PESSOA

Em 1984, o geneticista britânico Alec Jeffreys descobriu a impressão digital genética, ou perfil genético[4], valendo-se de uma técnica que identifica sequências de DNA únicas de cada indivíduo, com exceção de gêmeos monozigóticos. O perfil genético é atemporal e, ao mesmo tempo, novo, sem precedentes e constante no tempo. É também irrepetível, ou seja, jamais se reproduzirá exatamente, por meios naturais, na existência da humanidade (GONÇALVES DA CRUZ, 2009, p. 276-277).

A identificação humana por perfis genéticos é inovadora, pois o DNA pode ser extraído de amostras biológicas de qualquer parte do corpo humano, como saliva, sangue, cabelos, fluido amniótico, unhas e sêmen, mesmo que em pequenas quantidades, por meio de métodos de amplificação genética, como o *Polymerase Chian Reaction* (PCR). Além disso, o DNA tem grande estabilidade no ambiente, por isso é possível

---

3 O DNA codificante, ao contrário, manifesta pouca variabilidade entre os indivíduos, ou seja, é pouco polimórfico, por isso é de pouco interesse para a identificação dos indivíduos (CARUSO FONTÁN, 2012, p. 144).

4 Conforme a Decisão n. 2008/616/JHA do Conselho da União Europeia, de 23 de junho de 2008, que trata da implementação da Decisão n. 2008/615/JHA sobre o aprofundamento da cooperação transfronteiriça, em particular no combate ao terrorismo e ao crime transfronteiriço, o perfil do DNA pode ser definido como "um código alfabético ou numérico representando um conjunto de características de identificação da parte não codificante de uma amostra de DNA humana analisada, ou seja, a estrutura molecular específica nos vários *loci* de DNA (posições)" (UNIÃO EUROPEIA, 2008b).

analisá-lo mesmo após um longo período e até quando o material em análise, obtido a partir de diferentes objetos que estiveram em contato com algum indivíduo – como uma garrafa com água, um chiclete mascado, uma balaclava ou outra roupa –, encontra-se degradado (PÉREZ MARÍN, 2008, p. 102). Dadas essas características, a impressão digital genética apresenta vantagens sobre a identificação mediante outras técnicas modernas, como impressão digital dactilar e reconhecimento facial. De fato, a epiderme dos dedos pode ser destruída pela ação do tempo, pelo uso de produtos químicos ou por cirurgia plástica[5]. Por sua vez, o reconhecimento facial, além da possibilidade de cirurgia plástica, é limitado por fatores como o envelhecimento e a pose da pessoa[6].

Dada a precisão da identificação resultante das análises de DNA, essas têm sido de grande importância para a perícia forense nas investigações de crimes que podem deixar restos biológicos (ROMEO CASABONA, 2002, p. 254-256). O presente artigo se centra no uso do perfil de DNA para identificação criminal, ou seja, no seu emprego para contribuir com o reconhecimento de uma pessoa como autora ou não de um crime, mediante a comparação entre, de um lado, o DNA recolhido de amostras biológicas obtidas da cena do crime, e, de outro, do DNA recolhido do investigado ou processado, ou ainda do armazenado em banco de perfis genéticos. Trataremos a seguir da obtenção da amostra de DNA e do tratamento dos dados dos perfis genéticos, sobretudo em banco de dados, à luz dos direitos fundamentais.

5 Sobre as impressões digitais dactilares, ver Interpol (2020a).

6 Sobre o reconhecimento facial, ver Interpol (2020b).

3. OBTENÇÃO DO PERFIL DE DNA

A análise de DNA é uma ferramenta avançada que contribui para o esclarecimento de crimes, a partir do exame de vestígios biológicos humanos presentes no local dos fatos. Por isso, é fundamental que, logo de início, os responsáveis pelas investigações busquem tais vestígios, por exemplo, em objetos, no corpo da vítima, em suas roupas e em outros pertences.

O interesse da investigação penal reside sobretudo na *comparação de perfis de DNA*, isto é, entre os dados coletados, de origem desconhecida, e outros extraídos diretamente do corpo de um indivíduo – geralmente investigado pelo crime – ou armazenados em um banco de dados de perfis genéticos. O cruzamento das informações permite avaliar o nível de coincidência dos perfis comparados. O pertinente laudo sobre a perícia genética serve como evidência para investigação, *podendo assumir caráter inculpatório ou exculpatório* (AMORIM, 2015, p. 9-11).

3.1 A COLETA DE AMOSTRAS DO LOCAL DO CRIME

A análise de DNA a partir de amostras de pessoas desconhecidas se inicia com a busca no local dos fatos ou na vítima, passando para a coleta e o envio ao laboratório e, finalmente, para a análise dos perfis de DNA obtidos (PÉREZ MARÍN, 2008, p. 110). Uma vez que tais medidas não incidem sobre uma pessoa em particular, consistindo em simples atos de busca e coleta, *não implicam a afetação direta de direitos fundamentais*. Por outro lado, exigem cautelas para garantir a *autenticidade e a inalterabilidade da fonte de futuras provas periciais*. Nesse sentido, é necessário realizar um estudo preliminar sobre as condições em que o local do crime se encontra e adotar as precauções para assegurar a preservação das amostras e evitar a contaminação. Assim deve-se principalmente isolar o local e trocar ou esterilizar os

instrumentos utilizados (PÉREZ MARÍN, 2008, p. 108-110). Uma vez localizadas, as amostras devem ser identificadas, documentadas, coletadas e preservadas, mantendo a cadeia de custódia, a fim de garantir a validade da prova. A cadeia de custódia é uma garantia processual da autenticidade das provas, ou seja, de que a amostra biológica coletada na cena do crime corresponde à analisada e valorada pelo perito[7]. Após a coleta, o material deve ser enviado ao laboratório para ser processado. Nesse momento, ocorre a extração do DNA, ampliação e obtenção do perfil de DNA (AMORIM, 2015, p. 11).

No ordenamento jurídico brasileiro, a coleta de amostras no local do delito se enquadra nas diligências iniciais da polícia ao tomar conhecimento da ocorrência de um crime (art. 6º do Código de Processo Penal Brasileiro – CPP). Além disso, o CPP estabelece que a coleta de vestígios deve ser realizada preferencialmente por perito oficial, ou seja, do Estado, investido por lei (art. 158-C do CPP[8]). Em geral, as provas periciais são produzidas na fase investigativa sem a presidência do juiz e a participação dos investigados[9]. No entanto, na fase processual, o

7 Nesse sentido, vale citar o entendimento do Tribunal Constitucional da Espanha (ESPANHA, 2014b) no sentido de que a cadeia de custódia da amostra biológica obtida consiste na garantia de ser a mesma usada para a análise comparativa dos perfis de DNA posteriormente realizadas em laboratório.

8 Trata-se de dispositivo que figura entre os adicionados ao CPP sobre a cadeia de custódia pela Lei n. 13.964/2019, que "aperfeiçoa a legislação penal e processual penal" (pacote anticrime).

9 Diferentemente de outros ordenamentos jurídicos, a legislação brasileira não prevê inspeção ocular em processos criminais, ato processual presidido pelo juiz de instrução e com a participação do investigado para a coleta, descrição e conservação de vestígios ou provas materiais do delito (veja-se, por exemplo, o art. 326 e seguintes da *Ley de Enjuiciamiento Criminal* espanhola), embora a doutrina admita a aplicação da inspeção judicial prevista no Código de Processo Civil, por analogia, no campo do processo penal (vide, *v.g.*, NUCCI, 2016, p. 352).

réu pode formular perguntas ao perito, a serem respondidas durante a audiência de instrução ou por meio de laudo pericial complementar, indicar assistente técnico e acessar, por intermédio deste, o material objeto da perícia (art. 159, CPP), exercendo o contraditório de forma diferida, conforme admitido pelo Supremo Tribunal Federal (STF)[10].

3.2 COLETA DE AMOSTRAS DIRETAMENTE DA PESSOA

Em comparação à coleta no local do delito, a extração de amostras diretamente do corpo de uma pessoa envolve menos problemas de confiabilidade e autenticidade da prova, pois se conhece de antemão a origem do material biológico. Por outro lado, *acarreta questões importantes sobre direitos fundamentais*, pois o investigado ou processado se torna objeto da prova, o que desestabiliza a tradicional separação entre sujeito e objeto do processo mediante a interação entre os dois elementos (PÉREZ MARÍN, 2008, p. 14).

As diligências no interesse da persecução penal, em especial as que tenham a pessoa como objeto, naturalmente colidem com direitos fundamentais. Assim sucede no que toca à coleta de amostras do corpo do indivíduo, que afeta direitos fundamentais materiais (os direitos à intimidade e privacidade e à integridade física), e processuais (de não produzir provas contra si mesmo e à presunção de inocência). No entanto, esses direitos *não são absolutos* e, portanto, devem ser ponderados a fim de determinar a possibilidade de serem limitados no interesse da persecução penal, para a garantia do direito da sociedade e da vítima à efetividade na prevenção, investigação e processamento de delitos. Em seguida trataremos dessas diligências e dos direitos fundamentais afetados.

---

10 *V.g.* Agravo Regimental (AgR) no *Habeas Corpus* (HC) n. 154.237, relatora ministra Rosa Weber, Primeira Turma, julgado em 18-12-2018, publicado em 14-3-2019.

3.2.1 INTERVENÇÕES CORPORAIS

A lacuna legislativa no Direito brasileiro a respeito da prova de DNA no interesse da persecução penal perdurou até 2012, quando a Lei n. 12.654, de 28 de agosto de 2012, alterou a Lei n. 12.037, de 1º de outubro de 2009, acrescentando a coleta de material biológico para a obtenção de perfil genético entre os casos em que o juiz pode determinar a identificação criminal para fins de investigação criminal e seu armazenamento no banco de dados de perfis genéticos. A referida lei alterou ainda a Lei n. 7.210, de 11 de julho de 1984 – Lei de Execução Penal –, tornando obrigatório que os condenados por determinados crimes graves sejam submetidos à identificação por DNA e seus perfis genéticos armazenados em banco de dados.

Em relação às diligências sobre o corpo humano, nem a lei nem a jurisprudência dos tribunais brasileiros as classificam[11], referindo-se

11 O Tribunal Constitucional da Espanha (1997), por exemplo, distingue as medidas no interesse da persecução penal que dizem respeito ao corpo de um indivíduo, segundo o critério do direito fundamental predominantemente afetado, em duas ordens: a mera inspeção ou busca no corpo, que não lhe causa nenhum ferimento, como o reconhecimento de pessoas, a coleta de impressão dactilar, os exames antropomórficos, eletrocardiogramas e exames ginecológicos, os quais não afetam, em princípio, o direito fundamental à integridade física, embora possam afetar o direito à intimidade corporal quando incorrem em zonas íntimas do corpo; e as intervenções corporais propriamente ditas, que objetivam obter elementos e substâncias, internos ou externos do corpo humano, para serem submetidos a análises periciais, como sangue, urina, saliva, cabelo e unhas, a fim de servirem como provas do crime ou de sua autoria, as quais afetam, em regra, o direito à integridade física. As intervenções corporais, de acordo com o grau de sacrifício que geram ao direito à integridade física, podem ser leves, que não causam perigo à vida, tais como a remoção de elementos externos do corpo – cabelos e unhas, por exemplo – ou internos – sangue –; e graves, que presumem adoção de procedimento agressivo ao corpo, como a perfuração lombar e a extração de líquidos cefalorraquidianos.

esta última de forma geral às intervenções corporais. Os precedentes aludem principalmente à interferência no direito de permanecer em silêncio (art. 5º, LXIII, da Constituição Federal[12]), o qual geralmente é interpretado pela doutrina e pela jurisprudência como um direito amplo e geral a não produzir provas contra si mesmo[13]. Ele abarcaria inclusive a colaboração passiva, ou seja, o simples deixar-se fazer[14], configurando-se como um direito praticamente absoluto[15].

Não obstante, existem precedentes do Superior Tribunal de Justiça (STJ) e de tribunais regionais federais considerando que não infringem o direito de não produzir provas contra si mesmo a submissão, voluntária ou não, do investigado a exame de raio-x abdominal para comprovação do crime de tráfico de drogas, bem como a intervenção corporal para extração de cápsulas de cocaína ingeridas[16].

---

12 "Art. 5º (...) LXIII – o preso será informado de seus direitos, entre os quais o de permanecer calado, sendo-lhe assegurada a assistência da família e de advogado;"

13 Nesse sentido, em geral, a jurisprudência do STF, *v.g.*, HC n. 99.289, relator ministro Celso de Mello, Segunda Turma, julgado em 23-6-2009, publicado em 4-8-2011.

14 Assim se posiciona parte considerável da doutrina brasileira em relação à coleta de material genético para a análise de DNA com fins criminais, afastando a possibilidade de obtê-lo sem o consentimento da pessoa (*v.g.*, MORAES PITOMBO, 2004, p. 10; GARRIDO, 2018, p. 894-895).

15 Consequência de uma tendência da doutrina e da jurisprudência brasileira de atribuir peso superlativo à garantia dos direitos dos investigados e processados em detrimento do interesse coletivo, ou seja, do dever de proteção do Estado, que engloba a persecução efetiva dos crimes (FISCHER, 2017, p. 74-75).

16 Apesar de serem tratadas como intervenções corporais, essas medidas configuram inspeções e registros corporais. *V.g.* HC n. 149.146, STJ, Sexta Turma, relator ministro Og Fernandes, julgado em 5-4-2011, publicado em 19-4-2011; e HC n. 0050137-40.2008.4.01.0000, TRF da 1ª Região, Terceira Turma, relatora desembargadora Assusete Magalhães, julgado em 10-11-2008.

Porém, a jurisprudência do STF em relação ao teste de DNA tem historicamente caminhado na direção oposta. Na esfera cível, julgado de 1994 entendeu que a execução forçada para a coleta de material biológico para exame de DNA na investigação de paternidade viola a dignidade humana, o direito à privacidade e a intangibilidade do corpo humano (HC n. 71.373, Plenário, relator ministro Marco Aurélio, julgado em 11-10-1994, publicado em 22-11-1996). Na mesma linha, em 2008, o STF entendeu que forçar o investigado a submeter-se ao teste de alcoolemia viola o direito de não produzir provas contra si mesmo (HC n. 93.916, Primeira Turma, relatora ministra Cármen Lúcia, julgado em 6-10-2008, publicado em 27-6-2008).

Nesse ínterim, em 2002, no conhecido caso Gloria Trevi, o STF autorizou, mesmo sem a permissão da afetada, a coleta de material biológico da placenta após o parto, para análise de DNA em investigação de paternidade, ante a alegação da mãe de que a gravidez seria resultante de estupro praticado por policiais na prisão onde se encontrava detida aguardando o processo de extradição. Não obstante, a medida se justificava por não envolver intervenção corporal, pois se tratava de DNA obtido de material biológico naturalmente expelido pelo corpo no momento do parto. No caso, enquanto todos os policiais supostamente envolvidos concordaram em fornecer seus materiais genéticos, a custodiada se recusou. O Tribunal decidiu que a coleta de material biológico da placenta após o parto se justificava ante a prevalência dos bens jurídicos constitucionais moralidade administrativa, persecução penal pública e segurança pública, ademais dos direitos à imagem e honra dos policiais acusados do crime de estupro, sobre os direitos da custodiada grávida à privacidade e a preservar a identidade do pai de seu filho (Questão de Ordem na Reclamação n. 2.040, Plenário, relator ministro Néri da Silveira, julgado em 21-2-2002, publicado em 27-3-2003).

Após a Lei n. 12.654, de 28 de agosto de 2012, observam-se duas

linhas jurisprudenciais. Há acórdãos do STJ tanto admitindo[17] como rejeitando[18] a obtenção de material genético para a investigação de crimes. Igualmente, há decisões dos tribunais regionais federais autorizando a coleta de amostras do corpo humano para a comparação entre os perfis genéticos dos investigados e os obtidos na cena do crime[19], inclusive de maneira forçada[20], e existem outras a negando com base no direito de não produzir provas contra si mesmo e na indispensabilidade do consentimento do investigado[21].

De qualquer forma, a questão da constitucionalidade das intervenções corporais para a coleta de amostras para análise de DNA no interesse da persecução penal, inclusive no caso da recusa do interessado em se submeter ao exame, permanece aberta na jurisprudência do STF[22]. O recurso extraordinário (RE) com repercussão geral em relação ao tema ainda está pendente de julgamento (RE n. 973.837, relator ministro Gilmar Mendes[23]).

---

17 Recurso em *Habeas Corpus* (RHC) n. 69.127, Quinta Turma, relator ministro Felix Fisher, julgado em 27-6-2016, publicado em 26-10-2016. No entanto, esse é um caso em que houve consentimento da parte investigada.

18 RHC n. 76.344, Sexta Turma, relatora ministra Maria Thereza de Assis Moura, julgado em 8-11-2016, publicado em 22-11-2016. A medida foi considerada desnecessária no caso específico, posto que não essencial para a investigação.

19 *V.g.*, HC n. 5014096-87.2017.4.04.0000 do Tribunal Regional Federal da 4ª Região, Sétima Turma, relator desembargador federal Márcio Antônio Rocha, julgado em 23-5-2017.

20 *V.g.*, Apelação Criminal (ACR) n. 0000528-62.2017.4.05.0000 do Tribunal Regional Federal da 5ª Região, Segunda Turma, relator desembargador federal Leonardo Carvalho, julgado em 2-4-2019.

21 *V.g.*, ACR n. 0000089-71.2019.4.01.3822 do Tribunal Regional Federal da 1ª Região, Quarta Turma, relator desembargador federal Néviton Guedes, julgado 7-5-2019.

22 Conforme já apontava Moro (2006, p. 439-440) e, mais recentemente, Suxberger e Furtado (2018, p. 831).

23 "Repercussão geral. Recurso Extraordinário. Direitos fundamentais. Penal. Processo Penal. 2. A Lei 12.654/12 introduziu a coleta de material biológico para a obtenção

Nesse contexto, precedente de 2018 pode indicar *moderação do STF em seu entendimento histórico* quanto às intervenções corporais, a qual pode repercutir quando do julgamento da questão pendente. Em recurso extraordinário, com repercussão geral reconhecida (RE n. 971.959, Plenário, relator ministro Luiz Fux, julgado em 14-11-2018, publicado em 31-7-2020), a Corte discutiu a constitucionalidade da tipificação penal do comportamento do condutor de veículo que, para fugir de possível responsabilidade penal ou civil, evade-se do local do acidente em que está envolvido, entendendo, por maioria (7 votos a 4), que o respectivo dispositivo (art. 305 do Código de Trânsito Brasileiro) não viola o núcleo irredutível do direito fundamental à não autoincriminação, uma vez que não obriga o investigado ou processado a atuar ativamente para produzir provas contra si mesmo. Considerou, também, que a restrição parcial à liberdade do cidadão gerada pela lei penal é proporcional ao fim pretendido, isto é, a persecução penal de delito contra a administração da Justiça. E não é só: os fundamentos desse julgamento indicam tendência em admitir a constitucionalidade das intervenções corporais passivas, em linha com o direito comparado. Vejamos trecho da ementa do acórdão:

---

do perfil genético, na execução penal por crimes violentos ou por crimes hediondos (Lei 7.210/84, art. 9-A). Os limites dos poderes do Estado de colher material biológico de suspeitos ou condenados por crimes, de traçar o respectivo perfil genético, de armazenar os perfis em bancos de dados e de fazer uso dessas informações são objeto de discussão nos diversos sistemas jurídicos. Possível violação a direitos da personalidade e da prerrogativa de não se autoincriminar – art. 1º, III; art. 5º, X, LIV e LXIII, da CF. 3. Tem repercussão geral a alegação de inconstitucionalidade do art. 9-A da Lei 7.210/1984, introduzido pela Lei 12.654/2012, que prevê a identificação e o armazenamento de perfis genéticos de condenados por crimes violentos ou por crimes hediondos. 4. Repercussão geral em recurso extraordinário reconhecida."

12. A garantia contra a não autoincriminação tem como corolário a preservação do direito do investigado ou réu de não ser compelido a, deliberadamente, produzir manifestação oral que verse sobre o mérito da acusação.

13. O direito de o investigado ou réu não realizar condutas ativas que importem na introdução de informações ao processo também comporta diferentes níveis de flexibilização, embora a regra geral seja a da sua vedação. A jurisprudência do STF, historicamente, adotava uma postura restrita quanto à admissibilidade das chamadas intervenções corporais. Contudo, na linha do que se visualiza no cenário internacional, a jurisprudência desta Corte Superior, gradativamente, iniciou uma caminhada em sentido oposto, do que constitui precedente exemplificativo a RCL 2.040/DF, de relatoria do Min. Néri da Silveira, julgada na data de 21/02/2002, ocasião em que se decidiu que a autoridade jurisdicional poderia autorizar a realização de exame de DNA em material colhido de gestante mesmo sem autorização daquela última, tudo com o objetivo de investigar possível crime de estupro de que tenha sido vítima.

14. O direito comparado, à luz da legislação, da doutrina e da jurisprudência dos principais países da Europa Continental, admite a intervenção corporal coercitiva, desde que autorizada judicialmente, se restrinja à cooperação passiva do sujeito investigado ou acusado e não ofenda a dignidade humana do examinado.

15. O Brasil, quanto à intervenção corporal para fins de investigação penal, assenta fundamento constitucional no inciso XII do art. 5º da Constituição Federal de 1988, que abriga cláusula de reserva de jurisdição para o controle quanto ao tangenciamento dos direitos fundamentais à intimidade, privacidade e imagem consagrados na norma constitucional. Nesse contexto normativo, não há dúvidas de que o constituinte brasileiro admitiu a possibilidade de que o legislador autorize intervenções estatais na vida privada, inclusive no que condiz às supracitadas intervenções corporais.

Trata-se de precedente que *harmoniza* o interesse da persecução penal e o respeito aos direitos fundamentais, em linha com os esforços de outros países e organizações internacionais no sentido do combate à criminalidade transnacional.

4. BANCOS DE DADOS DE PERFIS GENÉTICOS

Em um mundo globalizado e integrado como sociedade da informação, o uso da tecnologia se torna ainda mais importante para a prevenção e o combate aos crimes. No que se refere à análise de DNA, a criação de bancos de dados de perfis genéticos constitui *valiosa associação entre a genética forense e a tecnologia da informação*, permitindo a comparação automatizada dos perfis de DNA de pessoas não identificadas, obtidos a partir de amostras biológicas encontradas na cena do crime, com os perfis de pessoas identificadas armazenadas nas bases supracitadas, *sem a necessidade do procedimento legal e médico de extração e análise de uma amostra biológica de investigados* (PÉREZ MARÍN, 2008, p. 201). Os bancos de dados de perfis genéticos possibilitam, também, estabelecer conexões entre os delitos, diante da coincidência de perfis de pessoas não identificadas obtidos em diferentes cenas de crime. Ainda quanto aos perfis genéticos de pessoas identificadas, os bancos de dados de perfis de DNA propiciam, além da comparação com perfis de pessoas não identificadas, o confronto com os que venham a ser obtidos a partir de vestígios de crimes cometidos no futuro, certificando a reincidência (ROMEO CASABONA, 2002, p. 264-265).

É evidente que a implementação desse importante instrumento para a persecução penal afeta direitos fundamentais, sendo imperioso um *equilíbrio*, de forma que as restrições aos direitos sejam proporcionais à finalidade coletiva pretendida. Disso resultam limites à composição e utilização dos bancos de dados de perfis genéticos para fins de identifi-

cação criminal. Nesse sentido, o direito à intimidade genética exige que os perfis a serem inseridos em bancos de dados genéticos sejam obtidos apenas da parte não codificante do DNA e sejam utilizados somente para a persecução penal[24]. Seguindo a dogmática internacional e de outros países[25], a Lei n. 12.037/2012 estabelece que "as informações genéticas contidas nos bancos de dados de perfis genéticos não poderão revelar traços somáticos ou comportamentais das pessoas, exceto determinação genética de gênero, consoante as normas constitucionais e internacionais sobre direitos humanos, genoma humano e dados genéticos".[26]

---

24 Nesse sentido, o Princípio 3 da Recomendação (92) do Conselho da Europa, de 10 de fevereiro de 1992, sobre o uso das análises de DNA no marco do Sistema de Justiça Criminal: "*Samples collected for DNA analysis and the information derived from such analysis for the purpose of the investigation and prosecution of criminal offences must not be used for other purposes*."

25 Veja-se a Resolução n. 97/C do Conselho da Europa, de 9 de junho de 1997, relativa ao intercâmbio de resultados de DNA, cujo parágrafo I.2, prevê que: "As possibilidades de intercâmbio limitar-se-ão ao intercâmbio de dados da parte não portadora de códigos da molécula de ADN, partindo-se do princípio de que não contêm informações sobre determinadas características hereditárias específicas" (UNIÃO EUROPEIA, 1997). A esse respeito, a Decisão n. 2008/615/JHA, de 23 de junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras ("Decisão Prüm"), prevê em seu art. 2º.2 que, no que diz respeito aos índices de referência provenientes dos dados contidos nos bancos de dados nacionais de análise de DNA, "não devem conter quaisquer dados que permitam a identificação directa da pessoa em causa" (UNIÃO EUROPEIA, 2008a). Da mesma forma, a legislação espanhola refere-se às informações genéticas que revelam a identidade da pessoa e de seu sexo como as únicas a serem extraída das análises de DNA, seja em relação à coleta de amostras biológicas (art. 129 bis do Código Penal), seja para o registro dos identificadores obtidos no banco de dados de perfis genéticos (art. 4º da Ley Orgánica 10/2007 e art. 129 bis do Código Penal).

26 "Art. 5º-A Os dados relacionados à coleta do perfil genético deverão ser armazenados em banco de dados de perfis genéticos, gerenciado por unidade oficial de perícia

Todavia, mesmo em se tratando da parte não codificante do DNA, assume relevância a questão do uso futuro desses dados, diante da possibilidade de que os avanços científicos venham a permitir a obtenção de informações hereditárias a partir dos marcadores de DNA atualmente utilizados[27]. A esse respeito, o Tribunal Europeu de Direitos Humanos (CONSELHO DA EUROPA, 2006), no caso *Van der Velden c. Holanda*, de 7 de dezembro de 2006, considerou que, diversamente do armazenamento de dados datiloscópicos, o uso futuro que se possa fazer do material celular obtido excede o escopo da identificação neutra do indivíduo, interferindo no direito à privacidade previsto no § 1º do art. 8º da Convenção Europeia sobre Direitos Humanos, de modo que tal ingerência sobre o direito fundamental deve estar prevista em lei e justificada como necessária para servir ao interesse da comunidade, no caso a prevenção e repressão de infrações penais, atividade do Estado que desempenha papel essencial na proteção dos direitos individuais contra a agressão de terceiros[28].

---

criminal. § 1º As informações genéticas contidas nos bancos de dados de perfis genéticos não poderão revelar traços somáticos ou comportamentais das pessoas, exceto determinação genética de gênero, consoante as normas constitucionais e internacionais sobre direitos humanos, genoma humano e dados genéticos." (Incorporado pela Lei n. 12.654, de 28 de maio de 2012).

27 Atenta a essa circunstância, a Resolução n. 2001/C 187/01 do Conselho da Europa, em seu apartado III, item 2, estabelece: "Caso a ciência evolua de modo a permitir determinar que algum dos marcadores de ADN recomendados na presente resolução contém informação sobre características hereditárias específicas, recomenda-se aos Estados-Membros que deixem de utilizar esse marcador. Também se recomenda aos Estados-Membros que se preparem para suprimir os resultados das análises de ADN que tiverem recebido, se se verificar que os referidos resultados das análises de ADN têm informações sobre características hereditárias específicas."

28 Veja-se sobre este ponto a sentença do TEDH no caso *Caruana c. Malta* (CONSELHO DA EUROPA, 2018).

O Tribunal Constitucional da Espanha (Sentença n. 199/2013, de 5 de dezembro de 2013) ponderou os interesses em jogo e considerou que os riscos gerados pelo uso futuro do perfil de DNA armazenado em bancos de dados para fins de identificação não constituem interferência atual na intimidade do afetado[29]. Nessa mesma linha, a Suprema Corte dos EUA, em 3 de junho de 2013, no caso *Maryland v. King*, asseverara que embora

> a ciência possa sempre avançar e esse progresso pode vir a ser relevante na perspectiva da Quarta Emenda, os alelos nos marcadores CODIS [banco de dados de perfis genéticos identificativos norte-americano] não fornecem atualmente nenhuma outra informação que não seja aquela relativa à identidade do sujeito. (LII, 2013 – Tradução livre)

Não obstante, a *garantia do direito à proteção de dados pessoais* assume particular importância no âmbito do tratamento dos dados genéticos armazenados em bancos de dados de DNA para fins criminais. Releva notar que o conteúdo do direito à proteção de dados pessoais é semelhante ao do direito à intimidade, com especificidades projetadas para lidar com novas realidades, sobressaindo a dimensão positiva do direito à intimidade, singularizada pela garantia do poder de controlar

---

29 "*Se pone así en evidencia que la lesión contra la que se pretende reaccionar derivaría de la conservación y utilización futura del perfile de ADN obtenido a partir de la saliva del demandante, pero no de la comparación neutral y exclusivamente identificativa del perfil de ADN del demandante con el extraído de los vestigios del delito investigado. De este modo, aun cuando cabe admitir que el peligro de futuros usos desviados del perfil de ADN del demandante podría eventualmente constituir una injerencia actual en la intimidad personal por el mero riesgo, huelga ahora realizar toda consideración al respecto en el seno de un proceso de amparo como este en la medida en que no es el supuesto concretamente analizado*." (ESPANHA, 2014a)

e dispor sobre o uso e a destinação dos dados pessoais, ou seja, aqueles que identificam ou permitem identificar indivíduos (ROIG, 2010, p. 15). Compreende um conjunto de princípios e faculdades cujo exercício obriga o Estado e particulares a garantirem às pessoas o direito de consentir previamente para a coleta de dados pessoais, a serem informados sobre a finalidade da coleta dos dados e do destinatário das informações, bem como de acessar, corrigir e retificar tais dados. O STF reconheceu o direito fundamental à proteção de dados pessoais como implícito no texto constitucional. O caso concreto diz respeito à Medida Provisória (MP) n. 954, de 17 de abril de 2020[30], que ordenava às operadoras de telefonia fixa e móvel, em um prazo de sete dias[31], o fornecimento dos nomes, números de telefone e endereços de seus consumidores, pessoas físicas e jurídicas, ao Instituto Brasileiro de Geografia e Estatística (IBGE), com a finalidade de produção estatística oficial durante o período da pandemia causada pelo novo coronavírus (covid-19).

Trata-se, portanto, de caso muito semelhante ao examinado pelo Tribunal Constitucional Federal alemão em 1983 (ALEMANHA, 1983), quando, reconhecendo pela primeira vez o direito à autodeterminação informativa, declarou inconstitucional alguns dispositivos da Lei do Censo Populacional. Nesse sentido, o STF suspendeu, em decisão cautelar (Medida Cautelar na Ação Direta de Inconstitucionalidade n. 6.387, Plenário, relatora ministra Rosa Weber, julgamento em 7-5-2020, publicação em 3-6-2020), a eficácia da medida provisória em tela, com base no direito fundamental à proteção de dados pessoais, consa-

30 A MP n. 954/2020 teve seu prazo de vigência encerrado em 14 de agosto de 2020, conforme Ato Declaratório do Presidente da Mesa do Congresso Nacional n. 112, de 2020.

31 Contados da publicação do ato formalizado pelo órgão receptor, a dispor sobre o procedimento mediante o qual seriam fornecidos os dados, ou seja, 17 de abril de 2020.

grando um direito fundamental autônomo garantido pela Constituição Federal, distinto da proteção da privacidade e da intimidade. A partir de uma interpretação integrada do texto constitucional, o STF reputou à proteção de dados pessoais um direito fundamental emanado da dignidade humana, a partir da renovação permanente da força normativa da proteção constitucional da intimidade diante das ameaças geradas pelos avanços tecnológicos e da centralidade do *habeas corpus* como instrumento de proteção material ao direito à autodeterminação informativa (MENDES, 2020). Dessa forma, a decisão representa um marco que, associado à entrada em vigor da nova Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n. 13.709, de 14 de agosto de 2018), consagra um sólido âmbito de proteção desse direito fundamental na ordem jurídica brasileira.

Em consequência, é imperioso garantir o uso dos dados genéticos apenas para a finalidade em razão da qual foram obtidos e o seu armazenamento, com segurança, por um período definido de tempo nos bancos de dados genéticos (TORRES SOTO, 2018, p. 225). O consentimento da parte afetada é condicionante para a coleta da amostra e a inserção do perfil genético correspondente no banco de dados de DNA, podendo ser excepcionado, por decisão judicial fundamentada (ÁLVAREZ DE NEYRA KAPPLER, 2008, p. 235). Os direitos de acesso, retificação e cancelamento são permeados por períodos específicos de armazenamento de dados, determinados pela legislação de cada país.

Em relação à definição das pessoas cujos dados genéticos serão incorporados aos bancos de dados, o ideal, sob o ponto de vista puramente da persecução penal, seria que fossem incluídos os perfis genéticos de toda a população. Tal medida maximizaria as chances de cruzamento entre os perfis obtidos nos locais dos delitos e diretamente das pessoas, aumentando consideravelmente a eficácia da Justiça criminal. Mas essa alternativa encontra condicionamentos econômicos, dados os custos financeiros envolvidos, e, principalmente, jurídicos, diante da necessidade

de que haja *proporcionalidade* entre, por um lado, a legítima finalidade buscada pela medida de conservação de perfis e amostras de DNA em bancos de dados, ou seja, a prevenção e a elucidação dos crimes de forma mais rápida e efetiva, e, de outro, as possíveis violações de direitos fundamentais (ÁLVAREZ DE NEYRA KAPPLER, 2008, p. 138-139).

As diferentes legislações nacionais estabelecem critérios quanto à vinculação da pessoa (suspeita, investigada, processada, ou condenada) cujo perfil genético será incluído no banco de dados de DNA a determinados tipos de crimes, geralmente os mais graves, assim considerados pela importância do bem jurídico protegido, pela intensidade da agressão e pela maior propensão à reincidência por seus autores (ROMEO CASABONA, 2002, p. 264-266).

5. OBTENÇÃO DO PERFIL DE DNA E BANCO DE DADOS DE PERFIS GENÉTICOS NO BRASIL

No que se refere à identificação genética para a investigação criminal, a Lei n. 12.037/2009 não relaciona crimes cujos investigados terão seus perfis genéticos obtidos e armazenados nos bancos de dados de perfis genéticos, mas dispõe que a medida será tomada quando essencial para investigações policiais de acordo com despacho da autoridade judicial[32], de ofício ou a pedido da Polícia, do Ministério Público ou

32 "Art. 3º Embora apresentado documento de identificação, poderá ocorrer identificação criminal quando: (...) IV – a identificação criminal for essencial às investigações policiais, segundo despacho da autoridade judiciária competente, que decidirá de ofício ou mediante representação da autoridade policial, do Ministério Público ou da defesa; (...) Art. 5º-A Os dados relacionados à coleta do perfil genético deverão ser armazenados em banco de dados de perfis genéticos, gerenciado por unidade oficial de perícia criminal. § 1º As informações genéticas contidas nos bancos de dados de perfis genéticos não poderão revelar traços somáticos ou comportamentais das

da defesa. Quanto às pessoas condenadas, a Lei n. 7.210/1984 – Lei de Execução Penal – se refere aos delitos dolosos praticados com violência grave contra a pessoa e aos crimes hediondos, previstos no art. 1º da Lei n. 8.072, de 25 de julho de 1990. Não é preciso decisão judicial específica para a inclusão dos perfis genéticos de pessoas condenadas, sendo a medida consequência da pena. A lei também não é expressa quanto à indispensabilidade do trânsito em julgado da sentença condenatória, havendo precedente do STJ que a considera necessária[33], assim como a doutrina a respeito, com base no direito à presunção de inocência (SUXBERGER; FURTADO, 2018, p. 829).

É obrigatório submeter-se à diligência para obtenção de DNA[34], que deve ser realizada por *técnica adequada e indolor*, de acordo com a norma relativa aos condenados, garantia que, sem dúvidas, estende-se aos investigados (SUXBERGER; FURTADO, 2018, p. 824).

A legislação brasileira, portanto, nos casos em que prevê, determina a *submissão obrigatória* à identificação do perfil genético, mediante a extração do DNA por meio de técnica adequada e indolor, mas não estabelece regras específicas relativas à intervenção corporal para a coleta da amostra. A Comissão Gestora da Rede Integrada de Bancos de Perfis Genéticos, com base em sua atribuição de promover a padronização dos procedimentos e técnicas para a coleta e a análise do material genético, bem como a inclusão, o armazenamento e a ma-

---

pessoas, exceto determinação genética de gênero, consoante as normas constitucionais e internacionais sobre direitos humanos, genoma humano e dados genéticos."

33 RHC n. 76.344, Sexta Turma, relatora ministra Maria Thereza de Assis Moura, julgado em 8-11-2016, publicado em 22-11-2016.

34 Conforme o art.9-A da Lei n. 7.210, de 11 de julho de 1984 – Lei de Execução Penal, relativo às pessoas condenadas. A obrigação, evidentemente, estende-se aos investigados, uma vez que, no que se refere a eles, a medida é necessariamente determinada por uma autoridade judicial.

nutenção de perfis genéticos em bancos de dados, fixada no Decreto n. 7.950, de 12 de março de 2013, expedido para a execução da Lei n. 12.654, de 28 de agosto de 2012[35], define o procedimento para a coleta da amostra diretamente do corpo humano, por meio da Resolução n. 10, de 28 de fevereiro de 2019. Esta dispõe sobre a padronização de procedimentos relativos à coleta obrigatória de material biológico para fins de inclusão, armazenamento e manutenção dos perfis genéticos nos bancos de dados que compõem a rede integrada brasileira. Determina a tomada de células de mucosa oral como a técnica a ser empregada e estabelece que os métodos de extração de sangue não devem ser utilizados. A referida resolução dispõe também que, antes da coleta de material genético, o interessado deve ser informado da fundamentação legal da medida na presença de pelo menos uma testemunha, além do responsável pelo procedimento. Em caso de recusa, prevê que o fato deve ser registrado em ata assinada pela testemunha e pelo responsável pelo procedimento e comunicada à autoridade judiciária competente, solicitando que esta decida sobre a submissão do interessado à coleta compulsória ou a outras providências que entender cabíveis, a fim de atender à obrigatoriedade prevista na Lei n. 12.654/2012.

Assim, as situações em que a pessoa afetada se recusar ao simples deixar-se fazer para a tomada de células da mucosa oral serão encaminhadas ao Poder Judiciário, que, *conforme as circunstâncias do caso e observados a dignidade da pessoa e seus direitos fundamentais de acordo com o princípio da proporcionalidade*, decidirá a respeito,

35 Lei que incorporou à legislação brasileira a identificação criminal por meio do perfil genético para fins de investigação de delitos e seu armazenamento em banco de dados de perfis genéticos, bem como a obrigação de que as pessoas condenadas por determinadas crimes graves sejam submetidas à identificação por DNA e seus perfis genéticos armazenados em banco de dados.

podendo inclusive determinar o uso de técnica alternativa, indolor e adequada, como a coleta de um fragmento de unha (SUXBERGER; FURTADO, 2018, p. 828).

As informações armazenadas nos bancos de dados de perfis genéticos são secretas, podendo ser acessadas no interesse da investigação criminal, mediante autorização judicial (art. 5º-A e art. 7º-B da Lei n. 12.037/2009 e art. 9º-A da Lei n. 7.210/1984). No que diz respeito ao período de conservação dos perfis genéticos, esses devem ser excluídos do banco de dados caso o interessado seja absolvido, silenciando a lei quanto às hipóteses de arquivamento do procedimento investigatório e de não recebimento da denúncia. No entanto, é razoável concluir que a exclusão também deve prevalecer nessas hipóteses, a menos que a investigação venha a ser reaberta[36]. Em caso de condenação, os dados genéticos devem ser excluídos depois de decorridos vinte anos desde o cumprimento da pena (art. 7º-A da Lei n. 12.037/2009). A legislação brasileira não dispõe sobre as faculdades de cancelamento, retificação e acesso aos dados armazenados nos bancos de dados de perfis genéticos, o que dificulta a garantia do direito à proteção de dados pessoais neste âmbito, já que a nova LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivamente de atividades de investigação e repressão de infrações penais (art. 4º, III, *d*), podendo o interessado, para a garantia do direito fundamental, manejar o *habeas data*, ademais da eventual aplicação analógica dos dispositivos pertinentes da LGPD, a despeito do referido dispositivo.

A Rede Integrada de Bancos de Perfis Genéticos é composta pelo Banco Nacional de Perfis Genéticos, vinculado ao laboratório do Departamento de Polícia Federal, e pelos bancos de dados genéticos vinculados aos laboratórios oficiais dos Estados e do Distrito Federal, que

36 Nos termos do art. 18 do Código de Processo Penal.

são incorporados à rede por meio de acordo de cooperação técnica entre a União e o respectivo Estado ou Distrito Federal. Atualmente, compartilham perfis genéticos na rede 20 laboratórios: o federal, o do Distrito Federal e os de 18 dos 26 estados[37].

Em maio de 2020, segundo o XII Relatório Semestral do Comitê Gestor da Rede Integrada de Bancos de Perfis Genéticos (2020, p. 25-29), esta continha 77.685 perfis de DNA relacionados à esfera criminal, dos quais 12.051 correspondiam a perfis anônimos, derivados de amostras coletadas do cenário do crime, e 65.634 eram de pessoas identificadas, correspondendo a 0,031% da população brasileira. Destes, 64.352 correspondiam a pessoas condenadas e 767 a identificadas criminalmente, 383 foram incluídos por decisão judicial e 132 foram coletados de restos mortais identificados. Foram registradas 1.508 coincidências entre perfis desconhecidos e 420 coincidências entre conhecidos e desconhecidos, o que auxiliou 1.406 investigações criminais. O número de *stain-person matches per person* no Brasil, ou seja, o número de correspondências entre perfis de DNA conhecidos e desconhecidos pelo número total de pessoas incluídas no banco de dados é de 16%. O número de perfis genéticos armazenados nos bancos de dados brasileiros vem aumentando significativamente, de um total de 1.605 em novembro de 2014 para 77.685 em maio de 2020.

Conforme mencionado, parte da doutrina brasileira, atribuindo um peso superlativo à garantia dos direitos dos investigados e processados em detrimento do interesse coletivo, sustenta, com base no direito de não produzir provas contra si mesmo, a impossibilidade de submissão passiva obrigatória dos investigados, processados ou condenados à medida de

37 Amazonas, Amapá, Bahia, Ceará, Espírito Santo, Goiás, Maranhão, Minas Gerais, Mato Grosso do Sul, Mato Grosso, Pará, Paraíba, Rio de Janeiro, Rio Grande do Sul, Santa Catarina e São Paulo.

intervenção corporal para a coleta de amostras de DNA (SUXBERGER; FURTADO, 2018, p. 826-827). Essa visão não merece prevalecer, pois atribui um *caráter absoluto* a um direito e implica o condicionamento da persecução eficaz dos delitos à vontade do investigado ou processado, *prejudicando o cumprimento do dever de proteção pelo Estado*[38] e ignorando a necessidade de uma *harmonização equilibrada entre os direitos e bens constitucionais em conflito* (MEDINA GUERRERO, 1996, p. 52).

A constitucionalidade do art. 9-A da Lei n. 7.210/1984, no que diz respeito à identificação e ao armazenamento de perfis genéticos de condenados por crimes violentos ou hediondos, está pendente de apreciação pelo STF (RE n. 973.837, relator ministro Gilmar Mendes, tema de repercussão geral). Oportuno transcrever o seguinte trecho do parecer apresentado pela Procuradoria-Geral da República no processo:

> A investigação criminal tem se valido, sobretudo nos tempos atuais, dos mais modernos meios de investigação, como escutas telefônicas, interceptação telemática, ações controladas, reconstituições criminais. Estes novos meios de prova têm sido acompanhados pelo Ministério Público e sempre autorizados pelo Judiciário, o que dá ao cidadão a garantia de que seus direitos serão preservados, ou restringidos somente ao necessário à investigação criminal, sem que lhes seja afetado o núcleo essencial.
>
> A partir da noção de dignidade humana, da concepção de que todos os homens são iguais e determinam suas próprias ações, cabe ao Estado não só permitir o aprimoramento dos instrumentos existentes para a investigação criminal mas, também, prover os meios para tanto necessários, a fim, inclusive, de assegurar os direitos fundamentais de

38 De fato, a Constituição Federal garante a segurança como direito individual (art. 5º, *caput*) e social (art. 6º, *caput*), além de estabelecer a Segurança Pública como dever do Estado, direito e responsabilidade de todos (art. 144, *caput*).

> todos os cidadãos, entre eles, o direito à vida, à segurança, ao livre desenvolvimento da personalidade, à integridade física e moral, à liberdade de ideias e crenças, à honra, à própria imagem e a todos aqueles inerentes à própria condição de ser humano.
>
> O instrumento aqui em discussão, portanto, em vez de abstrair a dignidade humana, tem por finalidade precípua promovê-la, sem afetar o núcleo essencial de qualquer direito assegurado a investigados e condenados.

A consolidação e o avanço do emprego do perfil genético para fins de persecução penal no Brasil dependem, portanto, da decisão do STF proferida nesse processo.

6. CONCLUSÃO

A legislação brasileira estabelece que a coleta de amostras diretamente do corpo humano deve ser realizada por técnica adequada e indolor e que o perfil genético obtido, a partir da parte não codificante do DNA, deve ser armazenado por um período limitado, em um banco de dados que somente será acessado mediante autorização judicial. O método de tomada de células da mucosa oral, uma *intervenção corporal levíssima*, afeta minimamente os direitos à integridade física e à intimidade. E, tratando-se de um deixar-se fazer, não há violação do direito ao silêncio, entendido como o direito de não produzir provas contra si mesmo[39], nem

39 A omissão do legislador quanto ao procedimento específico de intervenção corporal em caso de recusa do interessado já gera discussões nos tribunais. Vide, *v.g.*, precedentes do Tribunal de Justiça de São Paulo (HC n. 2057654-47.2019.8.26.0000 e AE 9001992-23.2019.8.26.0050), do Tribunal de Justiça do Rio Grande do Sul (HC n. 70076369479) e do Tribunal de Justiça do Estado de Minas Gerais (HC n. 1.0000.15.035575-8/000).

da presunção de inocência, uma vez que o teste de DNA tem valor relativo, devendo ser valorado em conjunto com as demais provas do processo, além de poder exculpar o investigado ou processado. O tratamento de dados da parte não codificante do DNA, ou seja, que não fornece informações sobre as características físicas ou patológicas da pessoa, reduz consideravelmente a afetação ao direito à intimidade e privacidade.

Assim, na linha do direito comparado, a coleta e o armazenamento de dados genéticos identificativos previstos na legislação brasileira para a investigação e o processamento de crimes afetam os direitos fundamentais em tela, garantidos pela Constituição Brasileira, mas *de forma proporcional e justificada ante a finalidade constitucional pretendida*, isto é, a garantia da persecução penal e da segurança pública.

Espera-se que a Corte Suprema harmonize os direitos e bens constitucionais em jogo, a fim de possibilitar a constante otimização[40] do uso de uma importante ferramenta para a garantia de direitos fundamentais, *não apenas em sua perspectiva de proibição do excesso, mas também de dever de proteção* (FISCHER, 2017, p. 72-74).

REFERÊNCIAS

ALEMANHA. Tribunal Constitucional. *BvR 209*, 15 dez. 1983. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html. Acesso em: out. 2020.

40 De fato, embora o número de perfis genéticos incluídos nos bancos de dados brasileiros ainda seja pequeno, as coincidências dos perfis genéticos armazenados na Rede Integrada de Bancos de Perfis Genéticos têm servido para auxiliar na resolução de casos relevantes, como crimes de estupro em série e roubo de empresa de transporte de valores mobiliários em cidade paraguaia na fronteira com o Brasil. Veja-se XII Relatório da Rede Integrada de Bancos de Perfis Genéticos (RIBPG), *cit.*, p. 41.

ÁLVARES GONZÁLEZ, Susana. Derecho a la Privacidad e Información Genética. *In*: ÁLVARES GONZÁLEZ, Susana, GARRIGA DOMÍNGUEZ, Ana (Dir.). *Un Nuevo Reto para los Derechos Fundamentales*: los datos genéticos. Madrid: Dykinson, 2017. p. 11-31.

ÁLVAREZ DE NEYRA KAPPLER, Susana. *La Prueba de ADN en el Proceso Penal*. Granada: Comares, 2008.

AMORIM, Antonio. *Genética Forense*. Lisboa: Academia das Ciências de Lisboa, 2015. Disponível em: http://www.acad-ciencias.pt/document-uploads/5900090_amorim,-antonio---genetica-forense.pdf. Acesso em: 2 out. 2020.

CARUSO FONTÁN, Viviana. Bases de Datos Policiales Sobre Identificadores Obtenidos a partir del ADN y Derecho a La Intimidad Genética. *Revista Nueva Época*, v. 15, n. 1, 2012, p. 135-167.

CONSELHO DA EUROPA. *Recommendation n. R (92) 1*, on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system, 10 fev. 1992. Disponível em: https://rm.coe.int/09000016804e54f7. Acesso em: out. 2020.

CONSELHO DA EUROPA. Tribunal Europeu de Direitos Humanos. *Caruana v. Malta*. 15 maio 2018. Disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-183511%22]}. Acesso em: out. 2020.

CONSELHO DA EUROPA. Tribunal Europeu de Direitos Humanos. *Van der Velden v. The Netherlands.* 7 dez. 2006. Disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-78858%22]}. Acesso em: out. 2020.

CRUZ, Antônio Carlos Gonçalves da. Bases de Dados Genéticos. *Nascer e Crescer*, v. XVIII, n. 4, 2009, p. 276-277.

ENFSI. *Análise e Recomendações de Gerenciamento de Banco de Dados de DNA*, 2016. Disponível em: https://enfsi.eu/wp-content/uploads/2016/09/final_version_enfsi_2016_document_on_dna-database_management_0.pdf. Acesso em: 2 out. 2020.

ESPANHA. Tribunal Constitucional. *Acórdão 207/1996, de 16 de dezembro*. BOE n. 19, 22 jan. 1997. Disponível em: https://hj.tribunalconstitucional.es/es/Resolucion/Show/3259. Acesso em: out. 2020.

ESPANHA, Tribunal Constitucional. *Acórdão 199/2013, de 5 de dezembro*. BOE n. 7, 8 jan. 2014a. Disponível em: https://hj.tribunalconstitucional.es/es/Resolucion/Show/23715. Acesso em: out. 2020.

ESPANHA. Tribunal Constitucional. *Acórdão 43/2014, de 27 de março*. BOE n. 87, 10 abr. 2014b. Disponível em: https://hj.tribunalconstitucional.es/es/Resolucion/Show/23862. Acesso em: out. 2020.

FISCHER, Douglas. O que é Garantismo (Penal) Integral? *In*: CALABRICH, Bruno; FISCHER, Douglas e PELELLA, Eduardo. *Garantismo Penal Integral*. 4. ed. Porto Alegre: Verbo Jurídico, 2017. p. 59-95.

GARRIDO, Rodrigo Grazinoli. Crítica científica de Investigação criminal genética – banco de perfis genéticos, fornecimento compulsório de amostra biológica e prazo de armazenamento de dados – Apontamentos sobre a inconstitucionalidade da Lei 12.654/2012. *Revista Brasileira de Direito Processual Penal*, v. 4, 2018, p. 889-900.

GÓMEZ SÁNCHEZ, Yolanda. La protección de los datos genéticos: el derecho a la autodeterminación informativa. *Derecho y salud*, v. 16, n. Extra 1, p. 2008, 59-78.

GONZÁLEZ DE LA VEGA, Alberto. Biotecnología aplicada a la identificación humana. *Revista del Colegio Oficial de Biólogos de la Comunidad de Madrid*, n. 17, 2008, p. 12-15.

INTERPOL. *Grupo de Expertos para el seguimiento en materia de ADN*, 2015. Disponível em: https://www.interpol.int/es/content/download/4876/file/14Y1787%20S%20RECOMENDACIONES%20GT%20ADN.pdf. Acesso em: out. 2020.

INTERPOL. *Impressões digitais*. 2020. Disponível em: https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Huellas-dactilares. Acesso em: out. 2020.

INTERPOL. *Reconhecimento facial*. 2020b. Disponível em: https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Reconocimiento-facial. Acesso em: out. 2020.

LII. Legal Information Institute. *Maryland v. King*, n. 12-207, 2013. Disponível em: https://www.law.cornell.edu/supremecourt/text/12-207. Acesso em: out. 2020.

LIMA, Helio Bechmuller. DNA x Criminalidade. *Revista Perícia Federal,* n. 26, p. 7-10. Disponível em: https://apcf.org.br/revistas/edicao-no-26-banco-de-dados-de-perfis-geneticos/. Acesso em: out. 2020.

MEDINA GUERRERO, Manuel. *La vinculación negativa del legislador a los derechos fundamentales*. Madrid: McGraw-Hill, 1996.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais, *Jota*, 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: out. 2020.

MORENTE PARRA, Vanessa. *Nuevos Retos Biotecnológicos para Viejos Derechos Fundamentales*: La Intimidad e la Integridad Personal. Tese (Doutorado em Direito). Universidad Carlos III de Madrid, Madrid, 2011.

MORO, Sergio Fernando. Colheita compulsória de material biológico para exame genético em casos criminais. *Revista dos Tribunais*, v. 853, 2006, p. 429-441.

MUÑOZ DE MALAJOVICH, María Antonia. *Biotecnología*. Bernal: Universidad Nacional de Quilmes, 2012.

NATIONAL HUMAN GENOME RESEARCH INSTITUTE. *Talking Glossary of Genetic Terms*. Disponível em: https://www.genome.gov/es/genetics-glossary/ADN-no-codificante. Acesso em: out. 2020.

NICOLÁS JIMÉNEZ, Pilar. *La Protección Jurídica de Los Datos Genéticos de Carácter Personal*. Bilbao: Cátedra Interuniversitaria Fundación BBVA-Diputación Foral de Bizkaia de Derecho y Genoma Humano, 2006.

NUCCI, Guilherme de Souza. *Manual de processo penal e execução penal*, 13. ed. Rio de Janeiro: Forense, 2016.

PEREZ LUÑO, Antonio Enrique. *La Tercera Generación de Derechos Fundamentales*. Cizur Menor Navarra: Thomson-Aranzadi, 2006.

PÉREZ MARÍN, María Ángeles. *Inspecciones Registros e Intervenciones Corporales*: Las pruebas de ADN y otros métodos de investigación en el proceso penal. Valencia: Tirant to Blanch, 2008.

PIERCE, Benjamin A. *Genética:* un enfoque conceptual. Madrid: Médica Panamericana, 2015.

PITOMBO, Antônio Sérgio Altieri de Moraes. Identificação criminal e banco de dados genéticos. *Revista do Advogado*, n. 78, 2004, p. 7-12.

REDE INTEGRADA DE BANCOS DE PERFIS GENÉTICOS. *XII Relatório da RIBPG* – Dados estatísticos e resultados – nov./2019 a maio/2020. Brasília: Ministério da Justiça e Segurança Pública, 2020,

p. 25-29. Disponível em: https://www.justica.gov.br/sua-seguranca/seguranca-publica/ribpg/relatorio/xii-relatorio-da-rede-integrada-de-bancos-de-perfis-geneticos.pdf/@@download/file. Acesso em: out. 2020.

ROIG, Antoni. *TiCs (Direitos Fundamentais e Tecnologias de Informação e Comunicações)*. Barcelona: Bosch, 2010.

ROMEO CASABONA, Carlos María. *Los Genes y sus Leyes*: El Derecho ante el Genoma Humano. Bilbao: Catedra de Derecho y Genoma Humano, 2002.

SUXBERGER, Antonio Henrique Graciano; FURTADO, Valtan Timbó Martins Mendes. Investigação criminal genética: banco de perfis genéticos, fornecimento compulsório de amostra biológica e prazo de armazenamento de dados. *Revista Brasileira de Direito Processual Penal,* v. 4, n. 2, 2018, p. 809-842.

TORRES SOTO, María Luisa de. Información genética y derecho a la intimidad. *Revista CES Derecho*, n. 9, 2018, p. 208-236.

UNIÃO EUROPEIA. Conselho da União Europeia. Resolução 97/C 193/02, de 9 de junho de 1997. Relativa ao intercâmbio de resultados de análises de DNA. *Jornal Oficial da União Europeia*, n. C 193/2, 24 jun. 1997. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31997Y0624(02)&from=PT. Acesso em: out. 2020.

UNIÃO EUROPEIA. Conselho da União Europeia. Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008. Relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras. *Jornal Oficial da União Europeia*, L 210/1, 6 ago. 2008a. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008D0615&from=PT. Acesso em: out. 2020.

UNIÃO EUROPEIA. Conselho da União Europeia. Decisão 2008/616/JAI do Conselho, de 23 de junho de 2008. Referente à execução da Decisão 2008/615/JAI, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras, *Jornal Oficial da União Europeia*, L 210/12, 6 ago. 2008b. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008D0616&from=EN. Acesso em: out. 2020.

U.S. DEPARTMENT OF ENERGY. *Human Genome Project Information Archive 1990-2003*. Disponível em: https://web.ornl.gov/sci/techresources/Human_Genome/publicat/index.shtml. Acesso em: 2 out. 2020.

VILLALOBOS RANGEL, Héctor. Las pruebas de ADN en el contexto forense. *Revista de Ciencias Forenses de Honduras*, v. 3, n. 2, 2017, p. 27-37.

O DIREITO À PROVA, O PRINCÍPIO DA NÃO AUTOINCRIMINAÇÃO E A COLETA DE MATERIAL GENÉTICO NA INVESTIGAÇÃO CRIMINAL

Fernanda Fernandes da Silva[1]
Hernando Fernandes da Silva[2]

RESUMO

A Constituição Federal de 1988 dispõe sobre a identificação civil do indivíduo e, excepcionalmente, nas hipóteses previstas em lei, a criminal. Esta passou a ser regulamentada pela Lei n. 12.037, de 1º de outubro de 2009. O presente artigo tem como objetivo geral refletir sobre a coleta de perfis genéticos como meio de obtenção de prova no processo penal. Para isso, serão discutidos os processos da identificação

---

1 Mestranda em Proteção e Efetivação em Direitos Fundamentais – linha de pesquisa na área de concentração do processo coletivo –, pela Fundação Universidade de Itaúna/MG. Pós-graduada em Processo Civil, pela PUC Minas. Servidora pública do Estado de Minas Gerais.

2 Mestre em Educação. Especialista em Direito e Processo do Trabalho; Direito Administrativo; gerenciamento de micro e pequena empresa; Direito Civil e Processo Civil. Bacharel em Direito; graduado em História. Procurador-geral do Município de Pará de Minas. Professor universitário.

criminal e do princípio da não autoincriminação, para, posteriormente, investigar-se a (in)constitucionalidade e aplicabilidade da coleta compulsória de material genético. Na expectativa de embasar essa discussão, foi realizada análise bibliográfica de autores que versam o tema. Justifica-se o estudo pela necessidade de se estimularem a discussão científica e a reflexão crítica acerca da identificação criminal, do respeito ao princípio da não autoincriminação e da consequente mitigação dos direitos fundamentais do condenado em conformidade à Carta da República e ao Estado Democrático de Direito.

Palavras-chave: Identificação criminal. Perfil genético. Bancos de dados. Não autoincriminação.

ABSTRACT

The 1988 Federal Constitution provides for the civil identification of the individual and, exceptionally, in the cases provided for by law, his criminal identification. Law n. 12.037, of October 1, 2009, regulated the constitutional provision mentioned above, providing on the criminal identification nuances of the civilly identified. The general purpose of the referring article is to reflect on the collection of genetic profiles as a means of obtaining evidence in criminal proceedings. As specific objectives, the criminal identification processes and the principle of non-self-incrimination will be discussed, in order to later investigate the (in)constitutionality and applicability of the compulsory collection of genetic material. A bibliographical analysis of authors on the subject was carried out in the expectation of supporting this discussion. The study is justified in order to stimulate scientific discussion and critical reflection about criminal identification, the principle of non self-crimination and the consequent mitigation of the fundamental rights of the condemned in accordance with the Constitution of the Republic and the Democratic State of Law.

Keywords: Criminal identification. Genetic profile. Databases. Non self-incrimination.

1. INTRODUÇÃO

A Constituição Federal de 1988, em seu art. 5º, LVIII, dispõe sobre a identificação civil do indivíduo e, excepcionalmente, nas hipóteses previstas em lei, a criminal. Esta passou a ser regulamentada pela Lei n. 12.037, de 1º de outubro de 2009.

Em 28 de maio de 2012, foi promulgada a Lei n. 12.654, que alterou as de n. 12.037 (Lei de Identificação Criminal) e n. 7.210/1984 (Lei de Execução Penal), introduzindo no ordenamento pátrio a coleta de material genético como forma de identificação criminal.

Conforme o *Dicionário Jurídico da Academia Brasileira de Letras Jurídicas* (1991, p. 280), a identificação é o "ato ou efeito de qualificar uma pessoa, com os dados característicos individuais, inclusive datiloscópicos, para que seja reconhecida como a própria". Nesse sentido, Tourinho Filho (2009, p. 264) conceitua identificação como "o processo usado para se estabelecer a identidade", que, por sua vez, vem a ser "o conjunto de dados e sinais que caracterizam o indivíduo".

Eduardo Henrique Alferes (2010) ensina que a "identificação criminal" é o termo utilizado para a "reunião de informações visando a individualizar uma determinada pessoa sujeita a um processo criminal ou ao inquérito policial, com objetivo de auxiliar o sistema penal". Pode ser feita em indivíduo vivo ou morto, quando não for possível a identificação pelo sistema civil, sobretudo ante envolvimento com crimes, seja no papel de vítima, seja no de suspeito.

Mirabete e Fabbrini (2014, p. 45) ensinam que a identificação pelo perfil genético consiste na coleta de material biológico do suspeito, na análise e descrição, mediante identificação da sequência de bases

nitrogenadas no interior da molécula de DNA (ácido desoxirribonucleico) que constitui o código genético caracterizador de cada ser.

Uma vez introduzida essa técnica no ordenamento jurídico pátrio, passou-se a questionar a obrigatoriedade do fornecimento, pelo condenado, de material utilizado para traçar seu perfil genético, em face da ofensa ao princípio da não autoincriminação e, consequentemente, da presunção de inocência.

A Constituição Federal traz, no bojo do seu art. 5º, rol exemplificativo de direitos fundamentais da pessoa humana. Para a elaboração deste estudo, cumpre pontuar, ainda que superficialmente, alguns princípios essenciais à compreensão do tema, os quais auxiliarão na conclusão da hipótese científica apontada.

O princípio da dignidade da pessoa humana, um dos fundamentos do Estado Democrático de Direito, reconhece a "prerrogativa de todo ser humano em ser respeitado como pessoa, de não ser prejudicado em sua existência (a vida, o corpo e a saúde) e de fruir de um âmbito existencial próprio". Esse preceito "zela pela dignidade da pessoa, que é o valor supremo absoluto cultivado pela Constituição Federal" (AWAD, 2006, p. 113).

De igual importância, o princípio da presunção de inocência, previsto no art. 5º, LVII, da Carta de 1988, pressupõe que "ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória".

Há ainda o princípio da não autoincriminação (*nemo tenetur se detegere*). No plano internacional, ele está previsto na Convenção Americana de Direitos Humanos (Pacto de São José da Costa Rica) e no Pacto Internacional dos Direitos Civis e Políticos. No direito interno, embora não citado expressamente no texto constitucional, é consubstanciado no art. 5º, LXIII, por meio do direito ao silêncio.

O princípio do *nemo tenetur se detegere* se consolidou nos séculos XVIII e XIX tanto na Europa, sobretudo na Inglaterra, quanto na América, em particular nos Estados Unidos. Decorreu da influência do movimento Iluminista e da consequente mudança no sistema processual,

que elevou o acusado à condição de sujeito de direitos e não mais como mero objeto de prova (NORONHA FILHO, 2014, p. 38).

Para a construção deste artigo, parte-se de um pressuposto geral de que os direitos fundamentais do indivíduo representam elementos essenciais da ordem jurídica nacional no contexto de um Estado Democrático de Direito. Nesse viés, os princípios da dignidade da pessoa humana, da presunção de inocência e da não autoincriminação, atuam como obstáculos ao arbítrio do Estado na busca pela verdade processual.

É a partir dessa perspectiva que se pretende desenvolver o presente trabalho, buscando-se compreender a coleta de material genético durante a fase de investigação criminal à luz da ordem constitucional e dos princípios que fundamentam o Estado Democrático de Direito.

Nessa linha, serão discutidos os processos da identificação criminal e do princípio da não autoincriminação para, posteriormente, investigar-se a (in)constitucionalidade e aplicabilidade da coleta compulsória de material genético. Trata-se de tema polêmico, capaz de fomentar intensas discussões na mídia e nos ambientes acadêmicos. Não se pretende, portanto, esgotá-lo aqui, mas antes estimular o debate a seu respeito.

Para tanto, a presente pesquisa utilizou-se da metodologia da revisão bibliográfica, com abordagem qualitativa, focada nas legislações constitucionais e infraconstitucionais do ordenamento pátrio.

Iniciamos nosso estudo discutindo brevemente a Lei n. 12.037/2009 (Lei de Identificação Criminal). Em seguida, tecemos considerações acerca da identificação criminal por meio do perfil genético e acerca da cadeia de custódia. Após essa abordagem, tratamos das nuances referentes à criação dos bancos de perfis criminais, para então enfrentarmos a questão conceitual da prova e analisarmos os atuais meios de prova existentes no processo penal brasileiro. Por fim, analisamos o princípio da não autoincriminação, bem como os reflexos da coleta de perfis genéticos na investigação criminal e sua correlação com o preceito *nemo tenetur se detegere.*

2. BREVES CONSIDERAÇÕES ACERCA DA IDENTIFICAÇÃO CRIMINAL NO BRASIL

A identificação do homem é um procedimento empregado por aqueles responsáveis, em sentido amplo, pela persecução penal. A eles são disponibilizados métodos de identificação para conhecer ou confirmar a identidade de pessoas apontadas como autoras de delitos e, posteriormente, fixar a elas eventuais envolvimentos com outros crimes (SOBRINHO, 2003, p. 75).

Como já foi dito, o art. 5º, LVIII, da Constituição Federal dispõe que, excepcionalmente, o cidadão estará sujeito à identificação criminal.[3] Para tal, determina a necessidade de se editar lei que regule o procedimento. Desse modo, em 1º de outubro de 2009, foi publicada a Lei de Identificação Criminal – de n. 12.037.

Em seu art. 2º, é prevista, como forma de identificação civil, a apresentação de qualquer documento público que permita identificar o indiciado, tais como expressamente determinado: as carteiras de identidade, de trabalho, profissional, de identificação funcional, bem como o passaporte. O dispositivo estabelece, ainda, que, para as finalidades da lei, os documentos de identificação civis são equiparados aos militares.

Já o art. 3º preconiza a possibilidade de ocorrer identificação criminal, embora apresentado documento, nas seguintes situações:

---

3 Importante ressaltar que, antes da promulgação da Constituição de 1988, havia o entendimento consubstanciado pelo STF no verbete n. 568 da Súmula de que "a identificação criminal não constitui constrangimento ilegal, ainda que o indiciado já tenha sido identificado civilmente". Assim, o indivíduo poderia ser identificado criminalmente por meio da submissão ao processo datiloscópico e fotográfico. O enunciado foi editado com base no disposto no art. 6º, VIII, do Código de Processo Penal brasileiro (Decreto-Lei n. 3.689, de 3 de outubro de 1941), o qual dispõe que, ao ter conhecimento da prática da infração penal, a autoridade policial deverá "ordenar a identificação do indiciado pelo processo datiloscópico, se possível, e fazer juntar aos autos sua folha de antecedentes".

> I – o documento apresentar rasura ou tiver indício de falsificação;
>
> II – o documento apresentado for insuficiente para identificar cabalmente o indiciado;
>
> III – o indiciado portar documentos de identidade distintos com informações conflitantes entre si;
>
> IV – a identificação criminal for essencial às investigações policiais, segundo despacho da autoridade judiciária competente, que decidirá de ofício ou mediante representação da autoridade policial, do Ministério Público ou da defesa;
>
> V – constar de registros policiais o uso de outros nomes ou diferentes qualificações;
>
> VI – o estado de conservação ou a distância temporal ou da localidade da expedição do documento apresentado impossibilite a completa identificação dos caracteres essenciais.

Em 28 de maio de 2012, foi promulgada a Lei n. 12.654, que introduziu, no ordenamento pátrio, a coleta de material genético para obtenção do perfil genético em duas situações: na *identificação criminal*, dispondo que essa "poderá incluir a coleta de material biológico para a obtenção do perfil genético"; e na *execução penal*, ao prever que

> os condenados por crime praticado, dolosamente, com violência de natureza grave contra pessoa, ou por qualquer dos crimes previstos no art. 1º da Lei n. 8.072, de 25 de julho de 1990, serão submetidos, obrigatoriamente, à identificação do perfil genético, mediante extração de DNA – ácido desoxirribonucleico, por técnica adequada e indolor.

Eduardo Henrique Alferes (2010) conceitua identificação criminal como

> termo utilizado para a reunião de informações visando a individualizar uma determinada pessoa sujeita a um processo criminal ou ao

> inquérito policial com objetivo de auxiliar o sistema penal, propiciando a seus órgãos informações válidas e confiáveis.

Segundo Corazza e Carvalho (2014, p. 419), "a identificação criminal pode ser feita em pessoas vivas ou mortas, quando não for possível identificá-las pelo sistema de identificação civil, principalmente quando envolvidas em crimes (vítimas ou suspeitos)" (*apud* GARRIDO; GIOVANELLI, 2012, p. 149).

Importante ressaltar que "identificação criminal" não é sinônimo de "qualificação". Esta consiste na "individualização do investigado ou do acusado, por meio da obtenção de dados como nome, naturalidade, estado civil, filiação, domicílio", e não implica constrangimento de qualquer natureza, diferentemente do que ocorre com a identificação criminal, que "supõe coleta de impressões digitais, procedimento fotográfico e, quando prevista, coleta de material biológico para confecção do perfil genético (dados estes inconfundíveis e intransferíveis)" (AVENA, 2017, p. 187).

O art. 5º da Lei n. 12.037/2009 dispôs que "a identificação criminal incluirá o processo datiloscópico e o fotográfico". E, por força da alteração imposta pela Lei n. 12.654/2012, seu parágrafo único passou a determinar que essa identificação, quando essencial às investigações policiais, segundo despacho da autoridade judiciária competente (art. 3º, IV, da Lei n. 12.037/2009), inclui, também, a coleta de material biológico para obtenção do perfil genético do indivíduo.[4]

---

4 Avena (2017, p. 187) ressalta que, "nos tempos modernos, outros métodos de identificação biométrica estão sendo aperfeiçoados, tais como a identificação por voz, a identificação através da íris, da retina, da face". Nesse contexto, questiona-se a possibilidade de esses novos procedimentos resultarem em constrangimento ilegal. Segundo o autor, "em que pese a existência de algumas opiniões considerando que devam ser permitidos estes outros meios de identificação criminal, compreende em sentido oposto.

Desse modo, infere-se que a norma legal não limitou a identificação a tais procedimentos, havendo, portanto, outros.

3. IDENTIFICAÇÃO CRIMINAL POR MEIO DO PERFIL GENÉTICO

Conforme exposto, a Constituição de 1988 incluiu a identificação criminal como direito e garantia individual, de modo que o civilmente identificado não deve ser submetido àquele procedimento, salvo nas hipóteses previstas em lei.

A Lei n. 12.654 limitou a coleta de material genético a duas situações: na *identificação criminal* e na *execução penal*. Na primeira, o art. 5º, parágrafo único, da Lei n. 12.037/2009, incluído pela Lei n. 12.654/2012, estabelece que, "na hipótese do inciso IV do art. 3º, a identificação criminal poderá incluir a coleta de material biológico para a obtenção do perfil genético".

As informações relacionadas à coleta do perfil genético deverão ser armazenadas em banco de dados de perfis genéticos gerenciado por unidade oficial de perícia criminal (art. 5º-A). O material não poderá revelar traços somáticos ou comportamentais, exceto determinação genética de gênero, consoante as normas constitucionais e internacionais sobre direitos humanos, genoma humano e dados genéticos (§ 1º).

A segunda situação prevista, por sua vez, refere-se à identificação obrigatória do perfil genético, mediante extração de DNA, por técnica adequada e indolor, dos condenados pela prática de crimes dolosos com uso de violência grave contra pessoa ou da forma prevista no art. 1º da Lei n. 8.072, de 25 de julho de 1990.

Isso porque o art. 5º, LVIII, da CF é peremptório quando proíbe a identificação criminal do indivíduo civilmente identificado, salvo nas hipóteses previstas em lei".

O banco de perfis genéticos será regulamentado por ato do Poder Executivo (§ 1º), que deverá versar garantias mínimas de proteção de dados genéticos, observadas as melhores práticas da genética forense (§ 1º-A). Seu caráter é sigiloso; portanto, aquele que permitir ou promover sua utilização para fins diversos dos previstos em lei ou em decisão judicial (§ 2º) responderá civil, penal e administrativamente.

Deve ser viabilizado ao titular de dados genéticos o acesso aos respectivos dados constantes nos bancos de perfis genéticos, bem como a todos os documentos da cadeia de custódia que gerou os dados, de maneira que possa ser contraditado pela defesa (§ 3º).

Por fim, o § 4º estabelece que o condenado pelos crimes previstos no *caput* do art. 9º-A que não tiver sido submetido à identificação do perfil genético por ocasião do ingresso no estabelecimento prisional deverá sê-lo durante o cumprimento da pena. Constitui falta grave a recusa do condenado (§ 8º).

A palavra "gene" surgiu em 1910, como referência a uma unidade abstrata de herança que governa traços específicos de uma determinada espécie. Após o aprofundamento dos estudos científicos, surgiu o conceito abstrato de gene como unidade fundamental da herança. Contudo, embora a carga genética seja responsável pela hereditariedade, cada indivíduo apresenta uma combinação diferente, o que garante a diversidade.

Andrade e Ana Maria Caldeira (2009, p. 140) destacam que o modelo da estrutura da molécula de DNA, elaborado por James Dewey Watson (1928) e Francis Harry Compton Crick (1916-2004), teve papel importante nos estudos do tema e permitiu o desenvolvimento da Biologia Molecular, ocorrido a partir da segunda metade do século XX.

> A molécula de DNA, tal como é aceita atualmente, foi descrita em 1953 pelo biólogo James Dewey Watson e pelo físico e bioquímico Francis Harry Compton Crick, em um artigo publicado na revista *Nature*. Os dois pesquisadores tiveram a oportunidade de trabalhar no

> mesmo laboratório em Cambridge, na Inglaterra, o Cavendish Laboratory. No cenário das pesquisas referentes à elucidação do modelo de DNA, vários grupos estavam envolvidos: além do Cavendish, na Inglaterra, havia também o grupo do King's College, onde trabalhavam Maurice Wilkins (1916-2004) e Rosalind E. Franklin (1920-1958). Nos Estados Unidos, havia o grupo do Instituto de Tecnologia da Califórnia, conhecido como Caltech, onde trabalhava Linnus Pauling (1901-1994). (ANDRADE; CALDEIRA, 2009, p. 147)

Marteleto Filho estabelece que a primeira aplicação do teste de DNA em uma investigação criminal ocorreu em 1986:

> Tratava-se de investigação de dois delitos de estupro seguidos de homicídio, praticados em um intervalo de dois anos e meio, tendo como vítimas duas adolescentes de 15 anos de idade, ocorridos nas adjacências de Londres. Os crimes geraram uma grande revolta na população, raramente vista no local. Em agosto de 1986, um jovem de 17 anos, de nome Richard Buckland, confessou o segundo delito, fornecendo detalhes a princípio desconhecidos da população. À guisa de confirmar a autoria, e principalmente ligar o suspeito também ao primeiro homicídio, amostras de sêmen preservadas nos dois casos foram enviadas ao Dr. Alec Jeffreys, da Universidade de Leicester, que havia acabado de desenvolver o processo denominado "DNA *fingerprint*" (impressão de DNA). Após a análise das amostras, o perito espantou a todos ao concluir que Buckland não era o autor dos crimes. Asseverou, ainda, que duas vítimas realmente haviam sido mortas pelo mesmo indivíduo. A polícia, então, frustrada com o andamento da investigação, iniciou uma campanha na comunidade, solicitando que homens entre 13 e 34 anos cedessem sangue para exame, realizando um verdadeiro "arrastão genético". Um morador, de nome Colin Pitchfork, relatou à esposa que tinha receio de fornecer a amostra, pois já havia sido detido anteriormente; para se esquivar,

> solicitou a um amigo que fornecesse a amostra em seu lugar. A trama acabou sendo descoberta pela polícia e Colin Pitchfork foi detido, vindo a confessar os dois homicídios. As amostras foram comparadas através do teste de DNA desenvolvido por Alec Jeffreys e a identidade do autor dos delitos foi confirmada. (MARTELETO FILHO, 2012, p. 149-150)

Lemos conceitua o DNA como a "molécula que carrega toda informação genética de uma pessoa". Ela é subdividida em uma parte codificante e outra não codificante.

> A primeira indica todas as informações genéticas do seu titular, desde suas características físicas até a propensão a uma determinada doença. A segunda pode ser comparada a um código de barras que serve apenas para identificar, sem informar características. Nos países onde já se utilizam bancos de dados genéticos, eles são alimentados com amostras de DNA não codificantes, "simples" marcadores genéticos, denominados perfis genéticos. (LEMOS, 2014, p. 17)

Segundo Corazza e Carvalho (2014, p. 419),

> a prova pelo DNA visa, basicamente, ao esclarecimento da autoria do crime e é realizada pela identificação de uma sequência de bases nitrogenadas no interior da molécula de ácido desoxirribonucleico (DNA), cuja ordem sequencial é diferente e única para cada indivíduo. (*Apud* MACHADO, 2012)

Mirabete e Fabbrini (2014, p. 45) conceituam a identificação pelo perfil genético como sendo o processo que consiste na

> coleta de material biológico do suspeito, como sangue, tecido, saliva, esperma etc., e em sua análise e descrição, mediante a identificação da

> sequência de bases nitrogenadas no interior da molécula do DNA que constitui o código genético que caracteriza cada indivíduo.

Ainda de acordo com os autores, ao introduzir a identificação pelo perfil genético no ordenamento jurídico pátrio, o legislador se inspirou em experiências de outros países que já adotavam técnicas de comparação de DNA como método de investigação criminal, criando para isso bancos de dados, dos quais o mais conhecido se encontra nos Estados Unidos, mantido pelo FBI.

A edição da Lei n. 12.654 fez emergir o questionamento acerca da obrigatoriedade do condenado de fornecer material para traçar seu perfil genético e da ofensa ao princípio constitucional da não autoincriminação, pontos que serão abordados no último tópico desta pesquisa.

A esse respeito, Bonaccorso (2010, p. 114) considera a identificação genética uma "revolução em relação ao tradicional sistema de impressão digital, principalmente em função do fato de que o teste de DNA pode ser realizado com amostras mínimas de qualquer parte do corpo", além de oferecer "muito mais informações sobre a pessoa do que a técnica meramente identificatória".

3.1 CADEIA DE CUSTÓDIA DOS PERFIS GENÉTICOS

Bonaccorso (2010, p. 25) conceitua cadeia de custódia como o "conjunto de procedimentos efetuados no levantamento do local de crime e no tratamento dos vestígios que, em última instância, irá garantir a credibilidade das provas e a imparcialidade na sua formação".

> Refere-se a um conjunto de documentos que demonstrem todos os "passos percorridos" por um determinado vestígio no decorrer do seu processo de análise, incluindo as condições em que ele foi coletado, a

> identidade de todas as pessoas que a ele tiveram acesso (...), a duração da custódia, as condições de segurança e armazenamento a que ele foi submetido e a maneira utilizada para se registrar todas as transferências do material a pessoas diferentes em cada fase.

A regulamentação da cadeia de custódia foi instituída pelo Pacote Anticrime (Lei n. 13.964/2019), por meio dos arts. 158-A a 158-F do Código de Processo Penal (CPP).

No mesmo sentido do conceito apresentado por Bonaccorso, o art. 158-A define cadeia de custódia como o

> conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte.

O art. 158-A, § 1º, institui que o início da cadeia de custódia se dá com a preservação do local de crime ou com procedimentos policiais ou periciais nos quais seja detectada a existência de vestígio – "todo objeto ou material bruto, visível ou latente, constatado ou recolhido, que se relaciona à infração penal" (§ 3º).

A Lei n. 13.964/2019, em seu art. 3º, ao inserir o art. 158-B no CPP, descreveu, uma a uma, todas as etapas da cadeia de custódia:

> Art. 158-B. A cadeia de custódia compreende o rastreamento do vestígio nas seguintes etapas:
>
> I – reconhecimento: ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;
>
> II – isolamento: ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime;

III – fixação: descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento;

IV – coleta: ato de recolher o vestígio que será submetido à análise pericial, respeitando suas características e natureza;

V – acondicionamento: procedimento por meio do qual cada vestígio coletado é embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior análise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento;

VI – transporte: ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;

VII – recebimento: ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu;

VIII – processamento: exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada às suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que deverá ser formalizado em laudo produzido por perito;

IX – armazenamento: procedimento referente à guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente;

X – descarte: procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial.

Certo é que cautelas obrigatórias devem ser tomadas para a coleta do material e manutenção da cadeira de custódia dos perfis genéticos.

Nessa esteira, Bonaccorso (2010, p. 129) anota que a identificação genética "depende de uma técnica complexa que necessita de controle e de garantia da qualidade para que seus resultados sejam confiáveis e possam ser utilizados em procedimentos judiciais".

4. CRIAÇÃO DO BANCO DE PERFIS CRIMINAIS

O art. 9º-A, § 1º, da Lei de Execução Penal (LEP) prevê que "a identificação do perfil genético será armazenada em banco de dados sigiloso, conforme regulamento a ser expedido pelo Poder Executivo".

O Decreto-Lei n. 7.950, de 12 de março de 2013, instituiu o Banco Nacional de Perfis Genéticos e a Rede Integrada de Bancos de Perfis Genéticos, no âmbito do Ministério da Justiça. O primeiro tem como objetivo armazenar dados de perfis genéticos coletados para subsidiar ações destinadas à apuração de crimes (§ 1º). Já a segunda permite o compartilhamento e a comparação de dados constantes dos bancos de perfis genéticos da União, dos Estados e do Distrito Federal (§ 2º).

Bancos de dados de perfis genéticos, para fins forenses, são

> bases que armazenam dados procedentes de indivíduos já condenados por tipos específicos de crimes ou, a depender do país, de suspeitos ou indiciados bem como perfis obtidos de vestígios biológicos encontrados em locais de crimes; e, em alguns casos, perfis de vítimas. (SANTANA; ABDALLA FILHO, 2012, p. 37)

Bonaccorso (2010, p. 66), em sua tese de doutorado, ensina que, normalmente, bancos de dados de DNA de interesse criminal são constituídos por dois conjuntos de perfis distintos: um composto por amostras

cedidas voluntária ou coercitivamente e outro por material oriundo de locais em que real ou supostamente ocorreu um crime.

É também Bonaccorso (2010, p. 143) quem afirma: "para os defensores da criação dos bancos de dados, a sua utilização permite grandes avanços na investigação de delitos graves, sobretudo nos de caráter sexual, devido à grande taxa de reincidência". Contudo, adverte que parte da doutrina propõe um estudo mais aprofundado acerca das repercussões na intimidade e em outros direitos fundamentais da pessoa, antes de ser cogitada a criação desses órgãos:

> Não se pode negar que os bancos de dados genéticos podem ser decisivos para a investigação e para a resolução de casos criminais, inclusive através da exclusão da participação de suspeitos, mas pode gerar sérios problemas fora dos processos originais. Isso tem levado uma parte da doutrina a propor que não se criem bancos de dados genéticos que contenham dados de identidade de pessoas condenadas por crimes sem antes estudar a fundo suas repercussões na intimidade e em outros direitos fundamentais da pessoa e, muito menos, se não dispuser primeiro de uma cobertura legal que habilite sua criação. (BONACCORSO, 2010, p. 148)

É preciso ponderar os benefícios do uso e da expansão dos bancos em relação aos custos sociais. A autora (2010, p. 151) alerta sobre as razões para que haja

> preocupação com o uso e expansão das bases de dados policiais, incluindo o seu impacto sobre a privacidade individual, o seu potencial de utilização abusiva por parte de governos, da discriminação e da possibilidade de erro nas condenações.

Ainda segundo ela (2010, p. 153), "expandir os bancos de dados faz colocar um número crescente de pessoas inocentes em uma lista de

suspeitos, independentemente, do fato de essas pessoas nunca terem sido acusadas ou condenadas".[5]

> Poucas pessoas têm problemas com a utilização de DNA em casos criminais. A manutenção permanente de DNA em um banco de dados para uso em investigações futuras é, no entanto, outra questão. Um indivíduo capturado por um policial e submetido a exame de DNA torna-se um suspeito automático para todas as futuras investigações criminais em que pesquisas de dados são utilizadas. Isso enfraquece o princípio da presunção de inocência que é central para muitos sistemas de justiça penal. (BONACCORSO, 2010, p. 154)

Os testes de DNA, entretanto, não são infalíveis.

> As amostras de DNA podem ser trocadas ou contaminadas. As análises podem ser mal interpretadas, especialmente quando crime contiver misturas de amostras de DNA de mais de uma pessoa. (BONACCORSO, 2010, p. 155)

Ademais, quando ocorre degradação do material, "os resultados podem ser erroneamente relatados".

Pelo exposto, para que os bancos de dados de perfis genéticos sejam realmente eficazes, devem ser observadas algumas questões técnicas. É necessária uma legislação específica, que regule minuciosamente o

---

5 De acordo com Bonaccorso (2010, p. 182), "devido à preocupação com a má utilização do DNA, algumas legislações obrigam a sua destruição. Isto ocorre na Nova Zelândia, que desde 1995, nas amostras de sangue (referência) das investigações criminais, apenas o registro informatizado do perfil de DNA é conservado. A amostra biológica original e todos os outros produtos de análise de DNA são destruídos no prazo de três meses a contar da recepção no laboratório forense".

funcionamento desses órgãos e observe as reais necessidades apuradas. Para tanto, é imprescindível promover discussões jurídicas e políticas aprofundadas e, principalmente, ponderar interesses, visando ao equilíbrio entre as necessidades de investigação criminal do Estado e os direitos fundamentais dos cidadãos.

5. CONCEITO E MEIOS DE OBTENÇÃO DA PROVA NO PROCESSO PENAL

Conforme apresentado, o objetivo geral desta pesquisa é refletir sobre a coleta de perfis genéticos como meio de obtenção de prova no processo penal. Para tanto, faz-se necessário conceituar prova e apresentar os meios de sua obtenção.

Avena (2017, p. 492) define prova como "conjunto de elementos produzidos pelas partes ou determinados pelo juiz visando à formação do convencimento quanto a atos, fatos e circunstâncias".

Greco (2004, p. 399) destaca que é no campo das provas que

> o processo pode se aproximar da realidade da vida, contribuindo para que a justiça consiga dar razão a quem tem direito e, mesmo quando não o fizer, para que a sociedade possa nela confiar por ter feito o máximo possível para realizar esse ideal.

O CPP, a partir do Título VII, contempla um grupo de regras referentes ao método de produção de provas no âmbito do processo criminal. Para tanto,

> estabeleceu normas gerais relacionadas aos critérios a serem utilizados pelo magistrado na valoração dos elementos de convicção carreados ao processo e ao ônus probante bem como disciplinou determinados meios específicos de prova. (AVENA, 2017, p. 491)

Greco Filho (1998, p. 199) conceitua meios de prova como sendo "os instrumentos pessoais ou materiais aptos a trazer ao processo a convicção da existência ou inexistência de um fato".

Avena (2017, p. 491) destaca que "a regulamentação dos meios de prova existente no CPP não é taxativa, podendo ser aceitos meios de provas atípicos ou inominados", ou seja, sem regulamentação expressa em lei. Assim, desde que não importe violação à Constituição Federal e às normas processuais gerais, são admitidas provas atípicas. Segundo o autor, essa amplitude se justifica na busca da verdade real.

O art. 155, *caput*, do CPP, dispõe que

> o juiz formará a sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão, exclusivamente, nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas.

Pelo teor do dispositivo, extrai-se que o CPP adotou, como regra, o sistema "do livre convencimento motivado", "da persuasão racional", "da livre convicção", "do livre convencimento" ou "da verdade real".

Avena (2017, p. 498) destaca três características básicas em relação a esse sistema: 1) não limita o juiz aos meios de prova regulamentados em lei; 2) não cria hierarquia entre os meios de prova[6]; e 3) exige, para fins de condenação, que as provas nas quais se fundamenta a decisão do

6 Dizer que o sistema do livre convencimento motivado (persuasão racional) se caracteriza pela ausência de hierarquia entre os meios de prova não significa afirmar que o magistrado tem liberdade valorativa absoluta. O livre convencimento do juiz encontra restrições impostas pela lei e pela Constituição, quais sejam: *motivação* e *presença de provas constantes dos autos do processo judicial* (assim, não pode o juiz formar sua convicção com base em elementos estranhos ao processo criminal) (AVENA, 2017, p. 498).

juiz tenham sido produzidas em observância às garantias constitucionais do contraditório e da ampla defesa.

Desse modo, conforme ensina Cagliari (2001, p. 91), "mantém-se ao juiz a liberdade de apreciação e de valoração das provas, mas vincula o seu convencimento ao material probatório constante dos autos, e o obriga a fundamentar sua decisão".

6. O PRINCÍPIO DA NÃO AUTOINCRIMINAÇÃO (*NEMO TENETUR SE DETEGERE*)

Etimologicamente, a expressão *nemo tenetur se detegere* significa que "ninguém precisa se descobrir", conceito que está diretamente relacionado ao direito ao silêncio.

Não há consenso na doutrina acerca da determinação da origem do princípio da não autoincriminação.[7] Para alguns autores, dentre os quais se destaca Maria Elizabeth Queijo (2012, p. 28), nem sequer é possível identificar a origem do referido princípio, uma vez que ele estaria inserido nas "regras gerais de direito, sendo impossível identificar suas raízes".

Para fins de contextualização histórica, considera-se que o *nemo tenetur se detegere* se consolidou nos séculos XVIII e XIX, em decorrência do movimento Iluminista e da consequente mudança no sistema processual, que elevou o acusado à condição de sujeito de direitos e não mais como mero objeto de prova (NORONHA FILHO, 2014, p. 38).

Noronha Filho (2014, p. 41) destaca que o princípio tem assumido contornos garantistas no sentido da

7 Trois Neto (2011, p. 82) elucida que "os autores não são concordes na determinação da origem do direito a não autoincriminação, e nem há facilidade de identificar sua razão de existência – e sobrevivência ao longo da história".

> proteção das liberdades de manifestação intelectual e moral do acusado, convergindo em sua capacidade processual de autodeterminação perante o Estado, o que possibilita, ao acusado, a escolha de cooperar ou não na fase investigativa ou judicial.

Contudo, como assevera Marteleto Filho (2012, p. 37), o preceito "não deve ser considerado sob uma ótica hipertrofiada, como se seu escopo fosse o de auxiliar o acusado a se eximir ou se esquivar de uma condenação lícita".

O *nemo tenetur se detegere* tem sido considerado como "direito fundamental de primeira dimensão, que assegura a esfera de liberdade ao indivíduo, em face dos excessos e abusos cometidos por parte do Estado" (NORONHA FILHO, 2014, p. 47).

No plano internacional, esse princípio está previsto expressamente na Convenção Americana de Direitos Humanos (Pacto de São José da Costa Rica)[8] e no Pacto Internacional dos Direitos Civis e Políticos[9]. No direito interno, está consubstanciado no art. 5º, LXIII, da Constituição da República de 1988 por meio do direito ao silêncio: "o preso será informado de seus direitos, entre os quais, o de permanecer calado, sendo-lhe assegurada a assistência da família e de advogado".

Quanto à relação entre esse direito e o princípio da não autoincriminação, Queijo (2012) aduz:

---

8 "Artigo 8. Garantias Judiciais. (...) (2) Toda pessoa acusada de delito tem direito a que se presuma sua inocência enquanto não se comprove legalmente sua culpa. Durante o processo, toda pessoa tem direito, em plena igualdade, às seguintes garantias mínimas: (...) g) direito de não ser obrigado a depor contra si mesma, nem a declarar-se culpada."

9 "Artigo 14. (...) (3) Toda pessoa acusada de um delito terá direito, em plena igualmente, a, pelo menos, as seguintes garantias: (...) g) de não ser obrigada a depor contra si mesma, nem a confessar-se culpada."

> O princípio *nemo tenetur se detegere* tem sido considerado direito fundamental do cidadão e, mais especificamente, do acusado. Nesse sentido, Vassali, Grevi e Zuccala já se manifestaram. (...) Nessa óptica, o princípio *nemo tenetur se detegere*, como direito fundamental, objetiva proteger o indivíduo contra excessos cometidos pelo Estado, na persecução penal, incluindo-se nele o resguardo contra violências físicas e morais, empregadas para compelir o indivíduo a cooperar na investigação e apuração de delitos, bem como contra métodos proibidos no interrogatório, sugestões e dissimulações. Como direito fundamental, o *nemo tenetur se detegere* insere-se entre os direitos de primeira geração, ou seja, entre os direitos da liberdade. O titular de tais direitos é o indivíduo diante do Estado. (QUEIJO, 2012, p. 54-55)

Nessa esteira se manifesta Oliveira (2006, p. 27), esclarecendo que o direito ao silêncio e à não autoincriminação não só permitem que o acusado ou aprisionado permaneça calado durante toda a investigação e mesmo em juízo, como impedem que ele seja compelido a produzir ou a contribuir com a formação da prova contrária ao seu interesse. Segundo o autor, "nessa última hipótese, a participação do réu somente poderá ocorrer em casos excepcionalíssimos em que, além da previsão expressa na lei, não haja risco de afetação dos direitos fundamentais da pessoa".

Vale ressaltar que o direito ao silêncio não deve ser tratado como sinônimo do *nemo tenetur se detegere*, uma vez que tal equivalência corresponde a uma concepção bastante restritiva do princípio. "Na realidade, o direito ao silêncio é a mais tradicional manifestação do *nemo tenetur se detegere*, mas o citado princípio não se restringe a ele." Aquele se apresenta como uma de suas decorrências, pois, "como direito fundamental e garantia do cidadão no processo penal, como limite ao arbítrio do Estado, é bem mais amplo e há diversas outras decorrências igualmente importantes que dele se extraem" (QUEIJO, 2012, p. 233).

7. COLETA DE MATERIAL GENÉTICO E O DIREITO À NÃO AUTOINCRIMINAÇÃO

Neste tópico, serão abordados os aspectos constitucionais e infraconstitucionais da identificação criminal obrigatória da LEP, baseada no perfil genético, e a sua correlação com o princípio *nemo tenetur se detegere.*

A Declaração Universal dos Direitos Humanos, adotada pela Organização das Nações Unidas (ONU) em 10 de dezembro de 1948, estabelece, em seu art. 11, que "toda pessoa acusada de um ato delituoso presume-se inocente até que a sua culpabilidade fique legalmente provada no decurso de um processo público em que todas as garantias necessárias de defesa lhe sejam asseguradas".

Nucci (2010, p. 692) destaca que a identificação criminal não é uma aceitação de culpa:

> Não se trata a identificação criminal de uma aceitação de culpa, mas de um procedimento para tornar exclusiva determinada pessoa, direito do estado, evitando-se com isto o nefasto erro judiciário. Não se confunda, ainda, a identificação criminal com o reconhecimento da pessoa. Neste caso, terceiros poderão apontar o indiciado ou réu como autor do crime. Naquela situação, nada disso tem relevo, pois se busca, apenas, identificar a pessoa que está sob investigação ou respondendo a processo-crime.

Muito se questiona acerca da obrigatoriedade de o condenado fornecer material para traçar seu perfil genético, em face da ofensa ao princípio da não autoincriminação e, consequentemente, da presunção de inocência.

Nos dizeres de Mirabete e Fabbrini (2014, p. 47), o exame de constitucionalidade das normas que preveem a identificação por perfil genético "há que se realizar não somente em face do art. 5º, LVIII, da CF, mas também e, principalmente, em sua relação com os princípios

e garantias que regem a investigação criminal e a produção de prova no processo penal".

Há forte tendência nos ordenamentos em mitigar as garantias advindas do princípio da não autoincriminação, "dando-se prevalência ao interesse do Estado e da sociedade na persecução penal" (QUEIJO, 2012, p. 50).

Nesse sentido, Marteleto Filho (2012, p. 3) aduz que o réu tem deveres de cooperação passiva, o que legitima a realização de inspeções, buscas pessoais, registros, reconhecimentos pessoais e mesmo a prática das intervenções corporais coercitivas, no sentido de se colher material genético para realização de exames de DNA e outras perícias.

Noronha Filho (2014, p. 64) defende que a mitigação das garantias advindas do princípio da não autoincriminação "decorre da própria necessidade de prevalência dos interesses do Estado e, por conseguinte, da sociedade na persecução criminal, na busca de uma Justiça mais célere e eficiente".

Contudo, conforme lecionam Thamiris Oliveira Bastos e Fernando Shimidt de Paula (2016, p. 8), parte da doutrina insurge-se contra a compulsoriedade da extração do perfil genético sob a alegação de que "o constituinte originário descreve, como garantias fundamentais de todo cidadão, a presunção de inocência bem como o direito do preso de permanecer calado". Sob esse fundamento, "o réu não poderia ser obrigado a ceder seu perfil genético, visto que se trata de uma prova invasiva".

Aqueles que defendem a impossibilidade de obrigar o investigado a fornecer material genético argumentam, ainda, que é preciso considerar, inclusive, a possibilidade de discriminação e estigmatização a partir de dados genéticos.

Nesse sentido, Lemos (2014, p. 18, *apud* JACQUES e MINERVINO, 2008) elucida que os maiores temores em relação ao uso inadequado das amostras genéticas constantes dos bancos de dados residem na possibilidade de se manipular e divulgar informação sensível dos indivíduos,

por exemplo, "a propensão a determinadas doenças, o que permitiria a empresas e a seguradoras negarem assistência e/ou emprego e promover a discriminação genética".[10]

Por todo o exposto, verifica-se que os questionamentos acerca da (in)constitucionalidade da identificação genética criminal obrigatória se dão porque tanto a extração prévia do DNA da amostra quanto as análises genéticas posteriores podem restringir os direitos fundamentais do investigado.

Diante disso, o debate gira em torno de dois interesses constitucionais: por um lado, o reconhecimento dos direitos fundamentais do indivíduo; por outro, o dever ou a obrigação dos poderes públicos de averiguar a verdade como forma de reprimir as condutas delituosas (BONACCORSO, 2010, p. 132).

Neste tópico, buscou-se demonstrar que os direitos fundamentais não têm caráter absoluto, logo admitem o mandamento da ponderação dos interesses constitucionais. Assim, no transcorrer da investigação criminal, tais direitos podem sofrer restrições ou limitações. Ou seja, "alguns direitos constitucionalmente relevantes cederão em favor de

---

10 Beck e Ritter (2015, p. 339) argumentam que uma solução viável e até então pouco aventada para esta celeuma seria a "criação de um banco de dados a partir da identificação de todos os indivíduos, independentemente de terem sido ou não condenados por um crime. Assim, quando da identificação civil da pessoa, além da coleta da impressão digital, poderia ser colida uma amostra do perfil genético, por meio da saliva, gota de sangue (existem vários dispositivos praticamente indolores para tanto) ou mesmo um fio de cabelo. Em algumas décadas, o País teria um banco de dados de identificação de todos os cidadãos nacionais, que poderia, inclusive, servir de parâmetro de comparação com materiais genéticos encontrados em cenas de crimes. Dessa forma, estaria resolvido o problema da seletividade, simbolismo e ineficácia encontrados na forma de criação e alimentação de dados de perfis genéticos trazido na Lei n. 12.654/2012. Em suma, o fornecimento do perfil genético se equivaleria ao do perfil digital".

outros interesses, direitos ou valores, igualmente protegidos, mas que, em circunstâncias concretas, tendem a ser sacrificados em benefício de outros direitos com os quais colidem" (BONACCORSO, 2010, p. 132).

8. CONCLUSÃO

Muito se questiona acerca da obrigatoriedade de o condenado fornecer material para traçar seu perfil genético em face da ofensa ao princípio da não autoincriminação e, consequentemente, da presunção de inocência.

Para a realização do exame de DNA, é necessário adquirir amostra do material biológico retirado do corpo do investigado. A partir dessa premissa, alguns direitos fundamentais desse indivíduo podem ser limitados.

Os direitos fundamentais não têm caráter absoluto, podendo, eventualmente, ceder espaço a outros interesses, direitos ou valores também protegidos. Tal aspecto se traduz pelo mandamento da ponderação dos interesses constitucionais que estão em jogo. "Por um lado, se reconhecem os direitos do indivíduo. Por outro lado, tem-se o dever ou a obrigação dos poderes públicos de averiguar a verdade como forma de reprimir as condutas delituosas" (BONACCORSO, 2010, p. 132).

Assim, em determinados casos, no transcorrer da investigação criminal, eles podem sofrer restrições e limitações. Bonaccorso (2010, p. 131) cita, por exemplo, o direito que a vítima e a sociedade têm de que os crimes sejam combatidos de forma eficaz e seus culpados sejam punidos de acordo com a lei. Existe, portanto, um "interesse social em reprimir comportamentos delituosos e, quando possível, impedi-los".

Portanto, a hipótese científica da pesquisa foi confirmada para se concluir que a coleta de material genético para realização dos exames periciais deverá respeitar os limites da adequação, necessidade e razoa-

bilidade, corolários do princípio da proporcionalidade. Desse modo, o procedimento precisa se dar "por técnica adequada e indolor", conforme preconiza o art. 9º-A da LEP.

REFERÊNCIAS

ALFERES, Eduardo Henrique. Lei n. 12.037/09: novamente a velha identificação criminal. *Jus Navigandi*, Teresina, ano 15, n. 2554, 29 jun. 2010. Disponível em: https://jus.com.br/artigos/15124/lei-n-12-037-09-novamente-a-velha-identificacao-criminal. Acesso em: 30 set. 2020.

ANDRADE, Mariana A. Bologna Soares de; CALDEIRA, Ana Maria de Andrade. O modelo de DNA e a Biologia molecular: inserção histórica para o ensino da Biologia. *Revista Filosofia e História da Biologia*, v. 4, 2009, p. 139-165. Disponível em: http://www.abfhib.org/FHB/FHB-04/FHB-v04-05-Mariana-Andrade-Ana-Maria-Caldeira.pdf. Acesso em: 30 set. 2020.

AVENA, Norberto. *Processo penal.* 9. ed. rev. e atual., Rio de Janeiro: Forense; São Paulo: Método, 2017.

AWAD, Fahd. O princípio constitucional da dignidade da pessoa humana. *Revista Justiça do Direito*, 21 (I), 2006. Disponível em: http://seer.upf.br/index.php/rjd/article/view/2182. Acesso em: 15 out. 2020.

BASTOS, Thamiris Oliveira; PAULA, Fernando Shimidt de. A coleta do perfil genético como forma de identificação criminal e o princípio da não autoincriminação. *Revista do Curso de Direito da Faculdade de Humanidades e Direito*, v. 13, n. 13, 2016. Disponível em: https://www.metodista.br/revistas/revistas-ims/index.php/RFD/article/view/6764/5242. Acesso em: 14 out. 2020.

BECK, Francis Rafael; RITTER, Ruiz. A coleta de perfil genético no âmbito da Lei n. 12.654/2012 e o direito à não autoincriminação: uma necessária análise. *Revista da AJURIS*, v. 42, n. 137, mar. 2015. Disponível em: http://ajuris.kinghost.net/OJS2/index.php/REVAJURIS/article/view/387/321. Acesso em: 14 out. 2020.

BEZERRA, Marina Gabrielle Alves Avelino; RODRIGUES, Filipe Azevedo. A coleta obrigatória de material biológico e o princípio da não autoincriminação. *Revista Eletrônica de Direito Penal e Política Criminal* – UFRGS, v. 4, n. 2, 2016. Disponível em: https://www.seer.ufrgs.br/redppc/article/view/64978/39087. Acesso em: 12 out. 2020.

BONACCORSO, Norma Sueli. *Aspectos técnicos, éticos e jurídicos relacionados com a criação de bancos de dados criminais de DNA no Brasil*. 2010. Tese (Doutorado em Direito Penal). Faculdade de Direito, Universidade de São Paulo. São Paulo, 2010. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-04102010-141930/publico/TESE_CORPO_DO_TRABALHO.pdf. Acesso em: 14 out. 2020.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 set. 2020.

BRASIL. *Decreto-Lei n. 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 14 out. 2020.

BRASIL. *Decreto-Lei n. 7.950, de 12 de março de 2013*. Institui o Banco Nacional de Perfis Genéticos e a Rede Integrada de Bancos de Perfis Genéticos. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7950.htm. Acesso em: 1º out. 2020.

BRASIL. *Lei n. 12.037, de 1º de outubro de 2009*. Dispõe sobre a identificação criminal do civilmente identificado, regulamentando o

art. 5º, inciso LVIII, da Constituição Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12037.htm. Acesso em: 22 set. 2020.

BRASIL. *Lei n. 12.654, de 28 de maio de 2012*. Altera as Leis ns. 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 – Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12654.htm. Acesso em: 22 set. 2020.

BRASIL. Supremo Tribunal Federal. *Súmula n. 568*. Disponível em: http://www.stf.jus.br/portal/jurisprudencia/menuSumarioSumulas.asp?sumula=4016. Acesso em: 30 set. 2020.

CAGLIARI, José Francisco. Prova no processo penal. *Revista Justitia*, São Paulo, v. 63, n. 195, p. 78-100. Disponível em: http://www.revistajustitia.com.br/artigos/299c16.pdf. Acesso em: 9 out. 2020.

CORAZZA, Thaís Aline Mazetto; CARVALHO, Gisele Mendes de. A identificação genética dos civilmente identificáveis como meio de prova de autoria. *Revista Jurídica Cesumar* – Mestrado, v. 14, n. 2, jul./dez. 2014, p. 413-434. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/3621/2429. Acesso em: 30 set. 2020.

GRECO, Leonardo. A prova no processo civil: do Código de 1973 ao novo Código Civil. *In*: COSTA, Hélio Rubens Batista Ribeiro *et al*. (Orgs.). *Linhas mestras do processo civil*. São Paulo: Atlas, 2004.

GRECO FILHO, Vicente. *Manual de processo penal*. 5. ed. São Paulo: Saraiva, 1998.

LEMOS, Cristiane Chaves. *A coleta de perfil genético como forma de identificação criminal*: entre a lógica do controle e a fragilidade

processual penal. Disponível em: https://www.pucrs.br/direito/wp-content/uploads/sites/11/2018/09/cristiane_lemos_2014_2.pdf. Acesso em: 14 out. 2020.

MARTELETO FILHO, Wagner. *O direito à não autoincriminação no processo penal contemporâneo*: investigação genética, interceptações telefônicas e ambientais, agentes infiltrados e outros problemas. Belo Horizonte: Del Rey, 2012.

MIRABETE, Júlio Fabbrini; FABBRINI, Renato N. *Execução penal*. 12. ed. rev. e atual. São Paulo: Atlas, 2014.

NORONHA FILHO, Adalberto Salvador. *A identificação criminal obrigatória da Lei de Execução Penal e o princípio da não autoincriminação (*nemo tenetur se detegere*)*. Monografia – especialização: Universidade Estadual do Ceará. Fortaleza, 2014. Disponível em: http://www.mpce.mp.br/wp-content/uploads/2018/07/A-identifica%C3%A7%C3%A3o-criminal-obrigat%C3%B3ria-da-lei-de-execu%C3%A7%C3%A3o-penal-e-o-princ%C3%ADpio-da-n.pdf. Acesso em: 13 out. 2020.

NUCCI, Guilherme Souza. *Leis penais e processuais penais comentadas*. 5. ed. São Paulo: Revista dos Tribunais, 2010.

OLIVEIRA, Eugênio Pacelli de. *Curso de processo penal*. 6. ed. rev. atual. e ampl., Belo Horizonte: Del Rey, 2006.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. *Declaração universal dos direitos dos homens*. Disponível em: https://www.ohchr.org/en/udhr/documents/udhr_translations/por.pdf. Acesso em: 14 out. 2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. *Convenção Americana de Direitos Humanos* – Pacto de São José da Costa Rica – 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 1º out. 2020.

QUEIJO, Maria Elizabeth. *O direito de não produzir prova contra si mesmo*: o princípio do *nemo tenetur se detegere* e suas decorrências no processo penal. São Paulo: Saraiva, 2012.

SINDOU, Maria José Othon. *Dicionário jurídico da Academia Brasileira de Letras Jurídicas*. 2. ed. Rio de Janeiro: Forense Universitária, 1991.

SOBRINHO, Mário Sérgio. *A identificação criminal*. São Paulo: Revistas dos Tribunais, 2003.

TOURINHO FILHO, Fernando da Costa. *Processo penal*. 31. ed. São Paulo: Saraiva, 2009.

TROIS NETO, Paulo Mário Canabarro. *Direito à não autoincriminação e direito ao silêncio*. Porto Alegre: Livraria do Advogado Editora, 2011.

PRISÃO EM FLAGRANTE E ACESSO A DADOS DE CELULAR: DESAFIOS ENTRE A PRIVACIDADE E A INVESTIGAÇÃO CRIMINAL

Gabriela Buarque Pereira Silva[1]
Tâmara Moura[2]

RESUMO

A aparente contraposição entre o direito de privacidade e a atividade policial por ocasião da prisão em flagrante tem ensejado questionamentos no que tange à necessidade de expedição de prévio mandado judicial para obtenção de acesso ao conteúdo dos *smartphones*. O advento de novas tecnologias e o protagonismo do telefone celular na vida dos indivíduos tornaram tal mecanismo efetivo elemento de prova em algumas investigações criminais, o que acarreta ressignificações no direito de privacidade. O presente trabalho visa, assim, por meio de análise documental e jurisprudencial, adotada a metodologia

1 Mestranda em Direito Público pela Universidade Federal de Alagoas. Assessora judiciária no Tribunal de Justiça de Alagoas. *E-mail*: gabrielabuarqueps@gmail.com.

2 Mestranda em Direitos Humanos pela Universidade Tiradentes. Advogada. *E-mail*: tamaramoura89@gmail.com.

dedutiva de revisão bibliográfica, analisar a necessidade de expedição de mandado judicial para acesso aos dados constantes em aparelho de telefonia móvel apreendido na prisão em flagrante. Por fim, constata-se que o ordenamento brasileiro aponta para a regra geral da necessidade de expedição de mandado para o referido acesso, ressalvadas as situações excepcionais que, sob o prisma da proporcionalidade, ensejem a necessidade de acesso imediato.

Palavras-chave: Prisão em flagrante. *Smartphones*. Dados. Privacidade.

ABSTRACT

The apparent opposition between the right to privacy and police activity at the time of the arrest has raised questions regarding the (un) need to issue a prior court order to obtain access to the content of smartphones. The advent of new technologies and the role of the cell phone in the lives of individuals has made this mechanism an effective element of evidence in some criminal investigations, which also leads to new meanings in the right to privacy. Therefore, the present work aims, through documentary and jurisprudential analysis and deductive methodology of bibliographic review, to analyze the need to issue a court order to access the data contained in smartphones apprehended in the act. Finally, it appears that the Brazilian system points to the general rule of the need to issue a warrant for said access, except for exceptional situations that, from the perspective of proportionality, give rise to the need for immediate access.

Keywords: Arrest. Smartphones. Data. Privacy.

1. INTRODUÇÃO

O advento de novas tecnologias demanda do intérprete a revisitação de alguns conceitos doutrinários e da epistemologia consolidada sobre a questão. O desafio se torna ainda mais complexo quando se trata de definir parâmetros de atuação na atividade policial ao se confrontarem o direito à segurança pública e o direito à privacidade do indivíduo.

A ascensão dos *smartphones* no cotidiano possibilitou o acesso rápido e instantâneo ao conteúdo desses aparelhos, o que permitiu fossem usados como elemento de prova, com o fito de se verificarem relacionamentos e comportamentos do indiciado que possam ajudar na elucidação de crimes e na instrução do processo penal. No entanto, impende verificar se há necessidade de prévia expedição de mandado judicial para tanto ou se basta que haja o acesso pela autoridade policial na ocasião da prisão em flagrante. Constata-se, com isso, um aparente embate de interesses, de modo que tais questões começam a assumir relevância no Judiciário para fins de declaração de nulidade pela ilicitude da prova.

O presente trabalho visa, portanto, por meio de análise documental e metodologia dedutiva de revisão bibliográfica, examinar a necessidade de expedição de mandado judicial para acesso aos dados constantes em aparelhos celulares apreendidos na prisão em flagrante. Com essa finalidade, também serão analisados alguns casos julgados por Turmas do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ) na última década, além de paradigmas internacionais, selecionados por embasarem a fundamentação das decisões dos tribunais pátrios.

2. A PROVA E O DEVIDO PROCESSO LEGAL COMO DIREITOS FUNDAMENTAIS

A palavra "prova" é originária do latim – *probatio* – e apresenta diversos significados, tais como: confirmação, argumento, ensaio, verificação, exame, entre outros. Em âmbito jurídico, prova é a demonstração que se faz, pelos meios legais, da existência ou veracidade de um fato material ou ato jurídico, em virtude do qual se conclui por sua existência ou se firma a certeza a respeito da existência do que demonstrado (SILVA, 1967).

Nesse contexto, pode-se entender que as provas são os instrumentos usados para convencer o juiz quanto à veracidade de uma afirmação sobre determinado fato. Constituem, portanto, importantes elementos capazes de demonstrar a realidade fática com o intuito de que seja valorada pelo magistrado no momento do exercício de seu juízo de racionalidade.

É inegável a importância das provas no ordenamento jurídico, pois, sem a possibilidade de se comprovar a verdade, não se pode falar em Estado Democrático de Direito. Posto isso, sedimenta-se a ideia de ser o direito à prova, na verdade, um direito fundamental, por estar contido implicitamente na Constituição Federal (CF/1988), mais precisamente em seu art. 5º, XXXV – direito ao processo justo – e LIV – devido processo legal (CAMBI, 2001).

O direito à prova está inserido no conceito de *acesso à Justiça*, uma vez que este abrange diversos direitos processuais. Ainda, ao permitir que as partes de um processo produzam provas para sustentarem, de maneira fática, suas alegações, evidencia-se que os demais princípios basilares do processo brasileiro também são respeitados, como o princípio da ampla defesa e do contraditório, ramificações do devido processo legal. A produção de provas é, portanto, essencial para que as partes exerçam o direito de ação e de defesa adequadamente (CAMBI, 2001).

Com efeito, quanto mais eficaz for o meio de prova, maior será a capacidade de se ampararem, com seguridade, os fatos e minimizarem as chances de o magistrado errar ao julgar a causa. Vale ressaltar, contudo,

que, como todo direito fundamental, o direito à prova não é absoluto, pois sofre limitações, sendo vedada a produção de provas ilícitas. Essa vedação, expressa na Carta Magna, decorre do princípio da legalidade, consagrando-se, assim, o Estado Democrático do Direito.

Quanto a esse aspecto, seria totalmente paradoxal se, em um processo criminal, instrumento cuja função precípua é apurar a prática de ilícitos penais, o Estado utilizasse meios que violassem direitos e maculassem a legitimidade do sistema persecutório, tendo em vista que ele próprio estaria se utilizando de uma infração penal para tanto (GOMES FILHO, 1997).

Nessa linha de raciocínio, existem, em regra, dois tipos de provas ilícitas: a originalmente ilícita e a ilícita por derivação. A primeira ocorre quando o crime se camufla de ato processual; e a segunda resulta da propagação da ilegalidade da prova originalmente ilícita, devido ao nexo causal existente entre ambas.

A ideia de propagação da ilicitude probatória surgiu no direito norte-americano com o caso *Silverthorne Lumber Co. v. United States*, em 1920, no qual a Suprema Corte declarou a invalidade de uma intimação que tinha sido realizada com escopo em informações extraídas de forma ilegal. Em 1939, a teoria se consolidou no caso *Nardone v. United States*, ficando conhecida como a teoria dos frutos da árvore envenenada (*fruits of the poisonous tree*) (GIMENEZ, 2018).

O auge desse entendimento foi vislumbrado no caso *Miranda v. Arizona*, de 1966. Ali, a Suprema Corte americana entendeu que as declarações feitas por uma pessoa a um agente policial são inválidas se aquela não tiver sido informada de que tudo que disser pode ser utilizado contra si e dos direitos de ficar em silêncio e constituir defensor ou ter um nomeado. A partir de então, caso os agentes policiais não se atentassem às formalidades supracitadas – *Miranda-warnings* –, eventual confissão e todas as provas conseguidas a partir dela seriam consideradas ilícitas (GIMENEZ, 2018).

No Brasil, de início, a teoria não foi bem recebida. O STF, capitaneado pelo ministro Moreira Alves, refutou a aplicação da teoria dos frutos da árvore envenenada com base na transcrição literal do art. 5º, LVI, da CF/1988. Argumentou que o texto constitucional dispunha somente a respeito das provas ilícitas, as quais seriam inadmitidas no processo, não fazendo menção às provas que derivam das ilícitas (GIMENEZ, 2018).

De acordo com essa teoria, as provas que derivam das originariamente ilícitas também são consideradas ilícitas, logo devem ser desentranhadas do processo, ainda que estejam vinculadas a meios lícitos.

Ressalte-se, entretanto, que, ao permitir a admissão de provas ilícitas com base na prevalência das liberdades públicas, de forma indiscriminada, corre-se o risco de se constituir precedente extremamente perigoso em detrimento dos direitos e das garantias individuais do acusado. Não seria possível estabelecer qualquer limitação à produção probatória, devido à busca incessante pela verdade e à premissa do efetivo combate ao crime (GIMENEZ, 2018).

Nessa esteira, nos casos em que houver colisão entre direitos e garantias fundamentais, no que tange à admissibilidade de provas ilícitas no processo, o parâmetro de entendimento deverá estar atrelado à benesse do acusado injustamente. Assinale-se que a admissão de prova ilícita para incriminar alguém seria flagrante violação de direitos e desrespeito a diversos princípios constitucionais, como o devido processo legal e a presunção de inocência.

Atualmente, a Justiça Penal passa por desafios imprevisíveis nessa seara para cumprir sua função cognitiva. Por isso, é imprescindível a explanação do direito probatório diante da utilização dos meios tecnológicos em prol da obtenção de elementos nas investigações criminais. Com efeito, torna-se cada vez mais comum o acesso ao conteúdo dos aparelhos celulares apreendidos por ocasião da prisão em flagrante, o que suscita reflexões acerca da necessidade de mandado judicial para tal procedimento.

É diante desse cenário que a investigação criminal se apresenta de maneira mais complexa com relação ao momento da valoração probatória, tornando-se imprescindível esclarecer se o acesso às referidas tecnologias apreendidas constitui ou não uma prova ilícita, diante da diversidade do *modus operandi*.

3. DESAFIOS À PRIVACIDADE NA OCASIÃO DO ACESSO AOS DADOS DE APARELHO CELULAR

Dado o papel central que o telefone celular costuma ter na vida de seus titulares e considerada a evolução da tecnologia nas comunicações telefônicas envolvendo dispositivos móveis, acende-se acirrado debate acerca do acesso aos conteúdos neles armazenados para fins de investigação criminal.

O processo penal deve ser conduzido pelos princípios constitucionais de forma a não sacrificar os direitos e garantias estabelecidos na Constituição Federal, o que também deve acontecer nas investigações criminais. Nesse ponto, a Carta de 1988 aduz expressamente, em seu art. 5º, X, que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas.

Para além disso, o art. 5º, XII, do mesmo diploma normativo, estipula que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses legais para fins de investigação criminal ou instrução processual penal. Diante disso, impende indagar se conversa de *WhatsApp* devem ser protegidas com base nesse dispositivo, por se tratar de comunicação telefônica, ou se, assim como fotos, vídeos e áudios, as mensagens de texto armazenadas, em que não há o fluxo de comunicação, são protegidas pelo inciso X do art. 5º da CF/1988 (direito à intimidade).

Levando-se em conta que, hoje, o aparelho celular apresenta uma

multiplicidade de funções e armazena uma série de informações diferentes, parece mais razoável considerar que sua tutela vai além do enquadramento como sigilo de comunicações telefônicas, albergando-se na dimensão geral da privacidade.

Ressalte-se que o próprio Código de Processo Penal (CPP) traz previsões que flexibilizam o direito de privacidade em face de uma necessidade de tutela processual efetiva, tal como os arts. 240[3] e 244[4], que preveem a busca e apreensão domiciliar e pessoal. Deve-se considerar, ainda, o disposto no art. 6º do mesmo diploma normativo, que determina à autoridade policial, assim que tiver conhecimento da prática da infração penal, a apreensão dos objetos relacionados ao fato e a colheita de todas as provas que servirem para o seu esclarecimento.

O presente artigo visa analisar precisamente a atuação durante a prisão em flagrante, tratando da extração de dados em dispositivos móveis apreendidos, mais precisamente no que concerne à possibilidade desse procedimento sem prévia expedição de mandado judicial.

---

3 "Art. 240. A busca será domiciliar ou pessoal. § 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para: a) prender criminosos; b) apreender coisas achadas ou obtidas por meios criminosos; c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos; d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso; e) descobrir objetos necessários à prova de infração ou à defesa do réu; f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato; g) apreender pessoas vítimas de crimes; h) colher qualquer elemento de convicção. § 2º Proceder-se-á à busca pessoal quando houver fundada suspeita de que alguém oculte consigo arma proibida ou objetos mencionados nas letras *b* a *f* e letra *h* do parágrafo anterior."

4 "Art. 244. A busca pessoal independerá de mandado, no caso de prisão ou quando houver fundada suspeita de que a pessoa esteja na posse de arma proibida ou de objetos ou papéis que constituam corpo de delito, ou quando a medida for determinada no curso de busca domiciliar."

Dentro desse contexto, compreende-se a extração de dados como um tipo de interceptação de comunicação: a interceptação telemática. Para tal, segue as mesmas regras de restrição de sua inviolabilidade, sendo necessária, além do cumprimento dos requisitos presentes da Lei n. 9.296/1996 (Lei das Interceptações Telefônicas), uma autorização judicial para que se realize tal feito no curso da investigação.

Nesse prisma, dispõe o art. 2º, II, da Lei n. 9.296/1996 que a interceptação das comunicações não será admitida quando a prova puder ser obtida por outros meios disponíveis. Dentre as medidas restritivas de direitos fundamentais, deve o poder público escolher a menos gravosa, sobretudo quando diante de insidiosa ingerência na intimidade e não só do suspeito, mas também de terceiros que com ele se comunicam.

Por isso, a interceptação telefônica precisa ser utilizada como medida de *ultima ratio*, sob pena de ilicitude da prova. Destarte, entre diversas medidas investigatórias idôneas a atingir o fim proposto, cabe ao magistrado buscar aquela que produza menores restrições à esfera de liberdade individual do agente. Também, sob a perspectiva judicial, tendo em vista a grave restrição ao direito à intimidade decorrente da interceptação das comunicações telefônicas, antes de decretar a medida, é imprescindível que o magistrado verifique a existência de outro meio de prova ou obtenção de prova menos invasivo (prova testemunhal, pericial etc.). Em contexto negativo, ou nos termos da lei, demonstrada a indispensabilidade do meio de prova (art. 5º da Lei n. 9.296/1996), o juiz é obrigado a deixar patente em sua fundamentação a referência à necessidade da medida cautelar, seja para a legitimação de sua atuação, seja para eventual impugnação *a posteriori*. Para além disso, também se ressalta a inutilização das gravações desnecessárias à instrução processual.

A gravação, ou parte dela, que não interessar ao processo deverá ser destruída, em qualquer fase da persecução penal, ou após, por ordem judicial, a requerimento do Ministério Público ou da parte interessada na manutenção do segredo (art. 9º, *caput*). Salientamos,

porém, ser aconselhável aguardar o término das investigações, ou mesmo da instrução processual, para que o magistrado decida sobre a inutilização do conteúdo, exceto se evidente a desnecessidade do material (SILVA, 2010, p. 35).

Observa-se, portanto, que o procedimento judicial é conduzido pela ponderação a respeito da restrição desse direito com a finalidade de deixar sempre a balança equilibrada para ambos os interesses. Sendo assim, deverá seguir sempre os parâmetros do devido processo legal onde haja meios de defesa e o investigado possa ter acesso ao material colhido de forma concreta para efetivar seu direito constitucional previsto no inciso LIV do art. 5º da CF/1988.

Cumpre salientar que a Lei n. 9.472/1997, a qual versa os serviços de telecomunicações, expressa, em seu art. 3º, V, que o usuário de serviços de telecomunicação tem direito à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucionais e legalmente previstas. No mesmo diapasão dispõe a Lei n. 12.965/2014 (Marco Civil da Internet), a determinar, em seu art. 7º, III, a inviolabilidade e o sigilo das comunicações privadas armazenadas, salvo por ordem judicial.

No entanto, a situação de flagrância e a necessidade de tutela da efetividade no processo penal têm ensejado questionamentos acerca da necessidade dessa autorização judicial no momento da prisão, sendo imprescindível analisar suas nuances para avaliar a viabilidade desse procedimento. Esse cenário apresenta uma linha tênue de legalidade, a qual deve ser posta na balança para que não haja necessidade de desentranhamento de material algum no processo por quaisquer nulidades futuras.

Com o advento da sociedade informacional, muitos direitos de personalidade e institutos jurídicos clássicos passam por uma ressignificação, com vistas a tutelar adequadamente, em especial, os novos desafios e riscos oriundos desse meio social. Compreende-se como privacidade "a faculdade de constranger os outros ao respeito e de resistir à violação do

que lhe é próprio, isto é, das situações vitais que, por dizerem a ele só respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão" (FERRAZ JR., 1993, p. 440).

Com efeito, o direito de privacidade, no contexto contemporâneo, abandona a clássica concepção americana de ser mero "direito de estar só", de Samuel Warren e Louis Brandeis (1890), para abranger outras facetas de controle sobre as informações pessoais, especialmente na sociedade digital. Stefano Rodotá (2008, p. 36) desenvolve a concepção de autodeterminação informativa como direito fundamental e argumenta que o exercício do direito de privacidade, hoje, se manifesta, sobretudo, pelo controle do fluxo das nossas informações pessoais.

> Coerentemente com a mudança da própria definição de privacidade, a atenção deve passar do sigilo ao controle. Isso significa, em primeiro lugar, que se torna cada vez mais difícil individuar tipos de informações acerca dos quais o cidadão estaria disposto a "despir-se" completamente, no sentido de renunciar definitivamente a controlar as modalidades de seu tratamento e a atividade dos sujeitos que a utilizam. Essa concepção depende sobretudo da percepção de que até as informações aparentemente mais inócuas podem, se integradas a outras, provocar dano ao interessado. E não se pode dizer que tal comportamento esteja em contradição com a tendência, anteriormente referida, segundo a qual existem categorias inteiras de informações pessoais (como aquelas de conteúdo econômico) cuja divulgação é oportuna ou necessária: publicidade e controle não são termos contraditórios, como são publicidade e sigilo. Exatamente onde se admitir a máxima circulação das informações de conteúdo econômico, deve-se permitir aos interessados exercitar um real poder de controle sobre a exatidão de tais informações, sobre os sujeitos que as operam e sobre as modalidades de sua utilização. Em segundo lugar, e sobretudo, a nova situação determinada pelo uso de computadores no tratamento das informações pessoais torna cada vez

> mais difícil considerar o cidadão como um simples "fornecedor de dados", sem que a ele caiba algum poder de controle. De fato, a obrigação de fornecer dados não pode ser simplesmente considerada como a contrapartida dos benefícios sociais que, direta ou indiretamente, o cidadão pode chegar a aproveitar. As informações coletadas não somente tornam as organizações públicas e privadas capazes de planejar e executar os seus programas, mas permitem o surgimento de novas concentrações de poder ou o fortalecimento de poderes já existentes: consequentemente, os cidadãos têm o direito de pretender exercer um controle direto sobre aqueles sujeitos aos quais as informações fornecidas atribuirão um crescente plus-poder.

Conforme argumenta Magrani (2019, p. 91), o impulso para maior proteção da privacidade adveio de situações relativas a vazamentos de informações e edição de leis gerais para a proteção de dados em países estrangeiros. Exemplos disso foram as denúncias promovidas por Edward Snowden[5] acerca da espionagem do governo americano em nível mundial, que atingiu chefes de Estado, como os do Brasil (Dilma Rousseff, à época) e da Alemanha (Angela Merkel), os quais apresentaram à Assembleia Geral da Organização das Nações Unidas uma proposta com regras para proteger o direito à privacidade na era digital.

Nesse ponto, a discussão assume papel cada vez mais relevente, tendo em vista que a maciça presença de interações virtuais, inteligência artificial, internet das coisas e reconhecimento facial nos submete a

---

5 Snowden – analista de sistemas, ex-administrador de sistemas da Agência Central de Inteligência americana e ex-contratado da Agência de Segurança Nacional dos Estados Unidos – divulgou uma série de programas que constituíam um sistema de vigilância global da agência americana. Os detalhes do caso podem ser encontrados na obra *Eterna vigilância: como montei e desvendei o maior sistema de espionagem do mundo* (2019) e no filme *Snowden: herói ou traidor* (2016).

uma constante vigilância. A ressignificação do direito de privacidade se manifesta, também, a partir da constatação da inexistência de direitos absolutos, que nos impele, constantemente, a refletir acerca da contraposição dos interesses em questão, visando, especialmente, consagrar uma tutela adequada no caso concreto.

Insere-se nessa discussão o direito à segurança pública, que implica a necessária aplicação da proporcionalidade na verificação quanto à licitude das provas obtidas (GIMENEZ, 2018, p. 67). Ressalte-se que a Lei Geral de Proteção de Dados Pessoais (LGPD) define, em seu art. 4º, III, *d*, que sua disciplina não será aplicável quando o tratamento dos dados pessoais for realizado para fins exclusivos de atividades de investigação e repressão de infrações penais.

Essa tensão é fomentada pela vigilância massiva que, muitas vezes, é explorada como mecanismo para assegurar o direito à segurança pública, o que sobreleva o protagonismo do Judiciário na resolução de impasses manifestos, sobretudo, nos casos concretos.

4. PARADIGMAS INTERNACIONAIS E ENTENDIMENTO JURISPRUDENCIAL DO STF E DO STJ

Com o advento da tecnologia, o mundo se encontra cada vez mais globalizado, contando com inúmeras facilidades de acesso à informação e comunicação. No entanto, a atitude de devassar os conteúdos de um celular particular pode acabar violando direitos fundamentais, como a intimidade do indivíduo e o sigilo das mensagens.

A respeito disso, constata-se a existência de duas percepções diferentes. De um lado, é necessário proteger os direitos fundamentais do indivíduo; de outro, faz-se necessário resguardar a efetividade da investigação criminal, já que as informações contidas no dispositivo móvel podem ser apagadas e, consequentemente, prejudicar os órgãos persecutórios na colheita de elementos informativos para eluci-

dação de delitos, os quais estão previstos nos incisos II, III e VII do art. 6º do CPP[6].

A colheita de provas realizada em *smartphones* apreendidos por policiais durante a prisão em flagrante, sem ordem judicial, passou a ser questionada nos tribunais brasileiros, como mostram o julgamento do *Habeas Corpus* (HC) n. 91.867/PA, em 2012, pelo STF, e o exame do Recurso em *Habeas Corpus* (RHC) n. 51.531/RO, em 2016, pelo STJ.

Nessa seara, indaga-se: um policial pode, ao prender em flagrante um indivíduo, sem um mandado judicial, analisar o conteúdo contido em seu aparelho celular e ter acesso a diversas informações particulares? No julgamento do *habeas corpus*, sob a relatoria do ministro Gilmar Mendes e por unanimidade, o STF denegou a ordem do *writ* ao entender que as provas obtidas por meio da coleta de informações em celulares apreendidos durante a prisão em flagrante, no ano de 2004, eram lícitas:

> *HABEAS CORPUS*. NULIDADES: (1) INÉPCIA DA DENÚNCIA; (2) ILICITUDE DA PROVA PRODUZIDA DURANTE O INQUÉRITO POLICIAL; VIOLAÇÃO DE REGISTROS TELEFÔNICOS DO CORRÉU, EXECUTOR DO CRIME, SEM AUTORIZAÇÃO JUDICIAL; (3) ILICITUDE DA PROVA DAS INTERCEPTAÇÕES TELEFÔNICAS DE CONVERSAS DOS ACUSADOS COM ADVOGADOS, PORQUANTO ESSAS GRAVAÇÕES OFENDERIAM O DISPOSTO NO ART. 7º, II, DA LEI 8.906/96 [*sic.*], QUE GARANTE O SIGILO DESSAS CONVERSAS. VÍCIOS NÃO CARACTERIZADOS. ORDEM

6 "Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá: (...) II – apreender os objetos que tiverem relação com o fato, após liberados pelos peritos criminais; III – colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias; (...) VII – determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;"

DENEGADA. (...) 2. Ilicitude da prova produzida durante o inquérito policial – violação de registros telefônicos de corréu, executor do crime, sem autorização judicial. 2.1 Suposta ilegalidade decorrente do fato de os policiais, após a prisão em flagrante do corréu, terem realizado a análise dos últimos registros telefônicos dos dois aparelhos celulares apreendidos. Não ocorrência. 2.2 Não se confundem comunicação telefônica e registros telefônicos, que recebem, inclusive, proteção jurídica distinta. Não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados. 2.3 Art. 6º do CPP: dever da autoridade policial de proceder à coleta do material comprobatório da prática da infração penal. Ao proceder à pesquisa na agenda eletrônica dos aparelhos devidamente apreendidos, meio material indireto de prova, a autoridade policial, cumprindo o seu mister, buscou, unicamente, colher elementos de informação hábeis a esclarecer a autoria e a materialidade do delito (dessa análise logrou encontrar ligações entre o executor do homicídio e o ora paciente). Verificação que permitiu a orientação inicial da linha investigatória a ser adotada, bem como possibilitou concluir que os aparelhos seriam relevantes para a investigação. 2.4 À guisa de mera argumentação, mesmo que se pudesse reputar a prova produzida como ilícita e as demais, ilícitas por derivação, nos termos da teoria dos frutos da árvore venenosa (*fruit of the poisonous tree*), é certo que, ainda assim, melhor sorte não assistiria à defesa. É que, na hipótese, não há que se falar em prova ilícita por derivação. Nos termos da teoria da descoberta inevitável, construída pela Suprema Corte norte-americana no caso Nix x Williams (1984), o curso normal das investigações conduziria a elementos informativos que vinculariam os pacientes ao fato investigado. Bases desse entendimento que parecem ter encontrado guarida no ordenamento jurídico pátrio com o advento da Lei 11.690/2008, que deu nova redação ao art. 157 do CPP, em especial o seu § 2º. 3. Ilicitude da prova das interceptações telefônicas

> de conversas dos acusados com advogados, ao argumento de que essas gravações ofenderiam o disposto no art. 7º, II, da Lei n. 8.906/96 [*sic*.], que garante o sigilo dessas conversas. 3.1 Nos termos do art. 7º, II, da Lei 8.906/94, o Estatuto da Advocacia garante ao advogado a inviolabilidade de seu escritório ou local de trabalho, bem como de seus instrumentos de trabalho, de sua correspondência escrita, eletrônica, telefônica e telemática, desde que relativas ao exercício da advocacia. 3.2 Na hipótese, o magistrado de primeiro grau, por reputar necessária a realização da prova, determinou, de forma fundamentada, a interceptação telefônica direcionada às pessoas investigadas, não tendo, em momento algum, ordenado a devassa das linhas telefônicas dos advogados dos pacientes. Mitigação que pode, eventualmente, burlar a proteção jurídica. 3.3 Sucede que, no curso da execução da medida, os diálogos travados entre o paciente e o advogado do corréu acabaram, de maneira automática, interceptados, aliás, como qualquer outra conversa direcionada ao ramal do paciente. Inexistência, no caso, de relação jurídica cliente-advogado. 3.4 Não cabe aos policiais executores da medida proceder a uma espécie de filtragem das escutas interceptadas. A impossibilidade desse filtro atua, inclusive, como verdadeira garantia ao cidadão, porquanto retira da esfera de arbítrio da polícia escolher o que é ou não conveniente ser interceptado e gravado. Valoração, e eventual exclusão, que cabe ao magistrado a quem a prova é dirigida. 4. Ordem denegada.

A defesa alegou que, considerada a devassa dos aparelhos sem prévia ordem judicial, a obtenção seria ilícita, uma vez que se sujeitaria à reserva absoluta de jurisdição. Todavia, o STF afirmou que não seria caso de desentranhamento de tais provas, pois o inciso XII do art. 5º da CF/1988 protege as comunicações telefônicas e não os registros telefônicos e que, ainda, com base no art. 6º do CPP, a autoridade policial possui o dever de proceder à coleta do material comprobatório da prática da infração penal (GIMENEZ, 2018, p. 58).

Nesse mesmo sentido, conforme destaca Gimenez (2018, p. 58), foi formalizado o acórdão do STF no julgamento do agravo regimental no HC n. 124.322/RS, em 2016 – quando já vigente o Marco Civil da Internet. O relator do caso, ministro Luís Roberto Barroso, consignou que dados relativos à hora, ao local e à duração das chamadas não são comunicações telefônicas e que, portanto, não gozam da proteção constitucional do sigilo das comunicações:

> AGRAVO REGIMENTAL. *HABEAS CORPUS* SUBSTITUTIVO DE RECURSO ORDINÁRIO. ACESSO A DADOS CADASTRAIS E DE USUÁRIOS. SIGILO DAS COMUNICAÇÕES. AUSÊNCIA DE TERATOLOGIA. (...) 2. As decisões proferidas pelas instâncias de origem estão alinhadas com a jurisprudência do Supremo Tribunal Federal, no sentido de que a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação de dados e não dos dados em si mesmos (RE 418.416, Rel. Min. Sepúlveda Pertence, Plenário) (...).

O Supremo decidiu que os registros telefônicos não geravam ao acusado o direito de ter provas desentranhadas, sob o fundamento de ter havido mero acesso, sem violação do direito à intimidade ou ao sigilo das comunicações telefônicas.

A título argumentativo, ressalte-se que o Tribunal Constitucional Alemão, no julgamento do caso *Handy-Verbingunsdaten*, lidou com o acesso a registros de conexão em celular apreendido, distinguindo "comunicação" e "dado", para afirmar não haver razão ao tratamento diferenciado dos dados armazenados em um celular quando comparados a uma carta encontrada em um domicílio (MARANHÃO, 2018, p. 48). Na Alemanha, já havia uma distinção bem consolidada entre o sigilo das comunicações e a proteção de dados em nome da autodeterminação informativa, sendo duas esferas de proteção reconhecidas pela Corte Constitucional.

Com efeito, no HC n. 91.867/PA, a aplicabilidade da Lei de Inter-

ceptações Telefônicas foi afastada, precisamente sob o fundamento de que não haveria fluxo de comunicações, mas apenas acesso aos dados do aparelho. A realidade atual, no entanto, é substancialmente diferente daquela vivenciada por ocasião do julgamento do STF, o que impele questionamentos no sentido da necessidade de também se tutelarem os dados armazenados e não somente aqueles que transitam em um fluxo de comunicação, máxime considerando que os artefatos tecnológicos, hoje, coletam informações que dizem muito a respeito da intimidade do titular em todos os aspectos.

Ademais, hoje, no Brasil, o direito à privacidade parece suprir essa questão e tutelar tanto o sigilo das comunicações como a proteção dos dados, inserido no art. 5º, X, da CF/1988, especialmente com o advento do Marco Civil da Internet e da LGPD.

Posteriormente, em 2016, o STJ julgou o RHC n. 51.531/RO, da relatoria do ministro Nefi Cordeiro, estabelecendo um precedente histórico no que tange ao acesso de *smartphones* por policiais no ato da prisão em flagrante sem prévia ordem judicial:

> PENAL. PROCESSUAL PENAL. RECURSO ORDINÁRIO EM *HABEAS CORPUS*. TRÁFICO DE DROGAS. NULIDADE DA PROVA. AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL PARA A PERÍCIA NO CELULAR. CONSTRANGIMENTO ILEGAL EVIDENCIADO. 1. Ilícita é a devassa de dados, bem como das conversas de *WhatsApp*, obtidas diretamente pela polícia em celular apreendido no flagrante, sem prévia autorização judicial. 2. Recurso ordinário em *habeas corpus* provido, para declarar a nulidade das provas obtidas no celular do paciente sem autorização judicial, cujo produto deve ser desentranhado dos autos.

Nesse caso, fixou-se o entendimento de que a devassa de dados de celulares e conversas do *WhatsApp*, sem prévia ordem judicial, torna as respectivas provas ilícitas.

A respeito dessa discussão, o STJ consolidou seu entendimento através do Informativo n. 583, no qual pontuou inexistir contexto específico para aceitação da extração de dados em celular apreendido no momento do flagrante, uma vez que as provas obtidas por meio não autorizado serão nulas diante dos limites legais:

> DIREITO PROCESSUAL PENAL. EXTRAÇÃO SEM PRÉVIA AUTORIZAÇÃO JUDICIAL DE DADOS E DE CONVERSAS REGISTRADAS NO *WHATSAPP*. Sem prévia autorização judicial, são nulas as provas obtidas pela polícia por meio da extração de dados e de conversas registradas no *WhatsApp* **presentes no celular do suposto autor de fato delituoso, ainda que o aparelho tenha sido apreendido no momento da prisão em flagrante.** Realmente, a CF prevê como garantias ao cidadão a inviolabilidade da intimidade, do sigilo de correspondência, dados e comunicações telefônicas (art. 5º, X e XII), salvo ordem judicial. No caso das comunicações telefônicas, a Lei n. 9.294/1996 regulamentou o tema. Por sua vez, a Lei n. 9.472/1997, ao dispor sobre a organização dos serviços de telecomunicações, prescreveu: "Art. 3º O usuário de serviços de telecomunicações tem direito: (...) V – à inviolabilidade e ao segredo de sua comunicação, salvo nas hipóteses e condições constitucional e legalmente previstas." Na mesma linha, a Lei n. 12.965/2014, a qual estabelece os princípios, garantias e deveres para o uso da internet no Brasil, elucidou que:
>
> > Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial.
>
> No caso, existiu acesso, mesmo sem ordem judicial, aos dados de

> celular e às conversas de *WhatsApp*. Realmente, essa devassa de dados particulares ocasionou violação à intimidade do agente. Isso porque, embora possível o acesso, era necessária a prévia autorização judicial devidamente motivada. Registre-se, na hipótese, que nas conversas mantidas pelo programa *WhatsApp* – que é forma de comunicação escrita e imediata entre interlocutores – tem-se efetiva interceptação não autorizada de comunicações. A presente situação é similar às conversas mantidas por *e-mail*, cujo acesso também depende de prévia ordem judicial (HC 315.220-RS, Sexta Turma, *DJe* 9/10/2015). Atualmente, o celular deixou de ser apenas um instrumento de conversação por voz à longa distância, permitindo, diante do avanço tecnológico, o acesso de múltiplas funções, incluindo a verificação de correspondência eletrônica, de mensagens e de outros aplicativos que possibilitam a comunicação por meio de troca de dados de forma similar à telefonia convencional. Desse modo, sem prévia autorização judicial, é ilícita a devassa de dados e de conversas de *WhatsApp* realizada pela polícia em celular apreendido. (RHC n. 51.531/RO, rel. min. Nefi Cordeiro, julgado em 19-4-2016, *DJe* de 9-5-2016)

Note-se a expressa menção ao caso *Riley v. California*, julgado pela Suprema Corte norte-americana em 2014, em que o acusado, David Riley, foi abordado pela polícia em agosto de 2009 por estar com sua carteira de motorista vencida. Porém, durante a abordagem, foram encontradas duas pistolas no veículo, as quais foram apreendidas juntamente com um aparelho celular, o que permitiu a descoberta de se tratar de membro de uma gangue envolvida em vários casos de homicídios. A despeito do fato narrado, a Suprema Corte dos Estados Unidos já decidiu que um mandado é necessário para acessar o aparelho celular na hipótese da prisão em flagrante, mormente tendo em vista que tais dispositivos guardam conteúdo revelador da intimidade do indivíduo (ESTADOS UNIDOS DA AMÉRICA, 2014).

Ainda em relação ao RHC n. 51.531/RO, também foi mencionada uma decisão emblemática proferida pela Suprema Corte do Canadá, em 2014. O caso, *R. v. Fearon*, envolvia dois homens que haviam roubado um comerciante de joias e foram presos no mesmo dia do assalto, ocasião em que os policiais procederam a uma revista e encontraram um telefone celular. Na sequência, realizaram a devassa do aparelho, acessando mensagens e fotos que os ligavam ao crime.

Nesse evento, a Corte canadense entendeu ser legítimo o acesso pela polícia aos dados situados no aparelho celular no ato da prisão em flagrante, sem prévia ordem judicial. O Tribunal reconheceu a licitude das provas e seguiu a linha de raciocínio que define como lícitas as provas obtidas nesse contexto, desde que auxiliem profundamente a investigação criminal.

Entretanto, a Justiça canadense buscou ponderar os interesses da persecução penal com o direito fundamental à intimidade, e, para isso, estabeleceu condicionantes, tais como: a) prisão lícita; b) acesso imediato aos dados; c) obtenção de informações nos limites do seu objetivo; e d) registro pormenorizado, pelas autoridades policiais envolvidas no exame do aparelho, da diligência, de modo a garantir o efetivo controle judicial *a posteriori*.

Com efeito, no *habeas corpus* de relatoria do ministro Nefi Cordeiro, houve a ressignificação da tutela dos dados veiculados por um aparelho celular, que, hoje, abrange inúmeros aspectos íntimos da vida do titular e não se restringe à capacidade de fluxo de ligações.

Ademais, a conclusão do caso *Riley v. California* é oposta à formalizada no HC n. 91.867/PA, julgado pelo STF em 2012, tendo em vista que este dispensou o mandado para legitimar o acesso aos dados de celular apreendido por ocasião de prisão em flagrante. Não obstante tal precedente, o julgamento do HC n. 51.531 pelo STJ, em 2016, encaminha-se para entendimento consentâneo com o precedente americano, modificando o panorama estabelecido pelo STF.

Essa tendência também é verificada no HC n. 168.052/SP, descrito no Informativo n. 944 do STF, a ser julgado pela Segunda Turma, sob a relatoria do ministro Gilmar Mendes. No caso, pede-se a nulidade da ação penal com fundamento na ilicitude das provas obtidas mediante acesso a conversas registradas no *WhatsApp* sem autorização judicial. Na ocasião, o relator votou pela procedência do pedido, considerando nulas as provas. O julgamento foi suspenso em razão do pedido de vista feito pela ministra Cármen Lúcia.

Em seu voto, o relator asseverou que a jurisprudência do Supremo era no sentido de que a inviolabilidade das comunicações não se aplicava aos dados já registrados, mas, tão somente, às comunicações, adotando uma interpretação mais restrita. No entanto, ressaltou a modificação das circunstâncias fáticas e jurídicas, inclusive com promulgação de novas leis, que o levou a constatar hipótese de mutação constitucional e alterar seu entendimento.

A pertinência da questão também é inequívoca em razão do reconhecimento, em 2019, de repercussão geral – Tema n. 977 – na matéria tratada no Recurso Extraordinário com Agravo (ARE) n. 1.042.075/RJ, da relatoria do ministro Dias Toffoli.

Para além disso, não se sedimentou ainda se, na hipótese de necessidade de mandado judicial, seria preciso um de interceptação telefônica ou de busca e apreensão. Este parece mais coerente, ante a capacidade do aparelho celular de apresentar inúmeras funções que vão além da mera telefonia. A mera apreensão por ocasião da prisão em flagrante, contudo, nos termos do art. 6º do CPP, não deve trazer implícita a ideia de que o ato acarreta o acesso aos dados, uma vez ser necessária a prévia e específica autorização judicial.

A referida oscilação jurisprudencial denota o evidente embate que se delineia entre os interesses jurídicos envolvidos na questão, o que sobreleva a relevância da ponderação e do sopesamento no caso concreto, além da consideração de todas as mutações que a realidade digital diariamente nos impõe.

5. A PONDERAÇÃO DE DIREITOS E A NECESSIDADE DE MANDADO JUDICIAL

O advento das tecnologias incorporou diversas outras funcionalidades aos celulares, sem contar com as inúmeras redes sociais e os aplicativos que retêm informações privadas e íntimas de muitos usuários. O pretérito contexto analógico, por sua vez, parecia tutelar de forma mais robusta o fluxo das informações do que a armazenagem delas. Em regra, os antigos telefones celulares sequer tinham as funcionalidades que hoje conhecemos, limitando-se a receber e realizar ligações, sendo este o contexto da Lei n. 9.296/1996 (Lei de Interceptações Telefônicas).

Atualmente, os aparelhos, em sua maioria, encontram-se conectados à internet de banda larga – os chamados *smartphones* – e geralmente são dotados de aplicativos de comunicação em tempo real. Isso significa dizer que o confisco de um dispositivo de telefonia celular de pessoa presa permite, pelo menos em tese, que a autoridade policial tenha acesso a inúmeros aplicativos de comunicação em tempo real, tais como *WhatsApp, Viber, Line, Wechat, Telegram, BBM, Snapchat* etc., todos dotados das mesmas funcionalidades de envio e recebimento de mensagens, fotos, vídeos e documentos em tempo real (LIMA, 2017, p. 749).

Nesse sentido, no julgamento do caso *Riley V. California*, o ministro John Roberts argumentou:

> Os telefones celulares modernos não são apenas mais uma tecnologia de conveniência. Com tudo o que contêm e tudo o que podem revelar, eles mantêm para muitos americanos "as privacidades de vida" (...). O fato de que a tecnologia agora permite que um indivíduo carregue essas informações em suas mãos não torna a informação menos digna de proteção (...). Nossa resposta para a questão do que a polícia deve fazer antes de vasculhar um telefone apreendido em uma prisão é, portanto,

> simples – obter um mandado[7]. (Tradução livre – ESTADOS UNIDOS DA AMÉRICA, 2014, p. 28)

Impende evidenciar que tal constatação não implica o revestimento de caráter absoluto da privacidade. Não à toa, a própria Constituição brasileira traz flexibilizações do direito à inviolabilidade de domicílio (art. 5º, XI), assentando que nele ninguém poderá penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial. São previsões que buscam, com efeito, equilibrar os interesses em questão, assegurando, concomitantemente, a mínima restrição dos direitos, sobretudo os da privacidade e da segurança pública.

Assinale-se, por relevante, que a segurança também é um direito social expresso nos arts. 6º e 144 da CF/1988, como dever do Estado, direito e responsabilidade de todos, exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio. Quando se trata da atividade policial, a preocupação com esse conflito de interesses é ainda mais sensível, por envolver atividade de risco que demanda respostas muitas vezes ágeis e coercitivas e, ao mesmo tempo, que impõe o inequívoco respeito aos direitos humanos.

O acesso a aparelhos eletrônicos se torna ainda mais complexo quando se constata que, muitas vezes, haverá possibilidade de eliminação remota de informações, a prejudicar a elucidação do crime e

---

7 "*Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life,' Boyd, supra, at 630. The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant.*"

posterior instrução probatória. Sobre esse ponto, Magalhães (2019, p. 553) argumenta que

> (...) não se pode, com seriedade, pretender combater as moléstias da atualidade com as aspirinas do início do século passado, é inviável sustentar que o combate à macrocriminalidade organizada, sofisticada e inteligente do mundo globalizado seja efetuado com mecanismos e interpretações tradicionalmente utilizados para enfrentar a criminalidade de um passado no qual o *modus operandi* prevalecente se restringia ao emprego da violência e da força bruta.

Noutro norte, Zilli (2018, p. 78) assevera que o risco de perecimento da prova não configura ameaça inafastável a ponto de conferir razoabilidade para a dispensa da ordem judicial, podendo tal risco ser afastado com providências simples, tais como a desconexão do aparelho da rede de acesso à internet.

Outrossim, Dezem (2020, p. 13) defende que, em sendo possível flexibilizar o direito da inviolabilidade de domicílio na hipótese de flagrante, também seria razoável considerar tal flexibilização na hipótese de acesso aos aparelhos eletrônicos por ocasião da prisão. Nesse panorama, assume relevância a ideia de ponderação e proporcionalidade, de modo que a busca pela verdade real não terá o condão de legitimar quaisquer medidas estatais de forma irrestrita.

Resta imprescindível, portanto, salientar a imposição da proporcionalidade, materializada no bloqueio do arbítrio estatal e no fomento aos direitos constitucionais, noção aferível nos próprios dispositivos que disciplinam a intervenção estatal e se materializa no embate entre a segurança pública e o direito de privacidade.

Conforme aduz Scaff (2001, p. 236), deve haver correlação entre a exigência estabelecida pela ordem jurídica e o encargo para seu cumprimento, surgindo daí a função da proporcionalidade como bloqueio

de abusos estatais e resguardo, concretizando diversos princípios constitucionais. Nos termos de Ávila (1999, p. 25):

> Pode-se definir o dever de proporcionalidade como um postulado normativo aplicativo decorrente da estrutura principial das normas e da atributividade do Direito, e dependente do conflito de bens jurídicos materiais e do poder estruturador da relação meio-fim, cuja função é estabelecer uma medida entre bens jurídicos concretamente correlacionados.

A proporcionalidade, conforme amplamente ressaltado pela doutrina contemporânea, se perfaz em juízo de adequação, necessidade e proporcionalidade em sentido estrito e é vinculada a uma relação, por se prestar à análise de um meio aplicado à obtenção de uma finalidade. O referido embate parte da premissa do marco teórico da teoria externa dos direitos fundamentais, segundo a qual,

> Ao contrário da teoria interna, que pressupõe a existência de apenas um objeto, o direito e seus limites (imanentes), a teoria externa divide esse objeto em dois: há, em primeiro lugar, o direito em si, e, destacadas dele, as suas restrições. (...) É principalmente a partir dessa distinção que se pode chegar ao sopesamento como forma de solução das colisões entre direitos fundamentais e, mais que isso, à regra da proporcionalidade, com suas três sub-regras: adequação, necessidade e proporcionalidade em sentido estrito. (ALEXY, 2015, p. 588)

Nesse sentido, argumenta-se que os direitos fundamentais possuem suportes fácticos amplos e que suas respectivas restrições são, portanto, fruto de um sopesamento com outros princípios conflitantes. Sob o prisma de Alexy (2015, p. 588), o princípio da proporcionalidade decorre da premissa segundo a qual os princípios são normas que

ordenam que algo seja realizado na maior medida possível dentro das possibilidades jurídicas e fáticas existentes.

Sendo protegidas constitucionalmente as comunicações, inclusive, de dados, entende-se que a sua restrição somente deve ocorrer em *ultima ratio*. Por isso a relevância de utilizar esse procedimento de investigação com a finalidade de suprir a falta de outros meios hábeis de prova, e não ser o principal, além de que sua utilização somente poderá ocorrer em hipóteses excepcionais, justificadas pelas circunstâncias do caso concreto.

Nesse ponto, o ordenamento jurídico brasileiro parece estar se encaminhando no sentido da possibilidade de acesso aos dados dos aparelhos eletrônicos na ocasião da prisão em flagrante, sem prévia autorização judicial. Essa possibilidade ocorreria apenas em situações absolutamente excepcionais, em que efetivamente reste demonstrada a urgência no alcance das informações, corroborada pelo risco de perecimento ou até mesmo pela incolumidade das vítimas e autoridades. Por exemplo, imagine-se a situação hipotética em que haja

> (...) extorsão mediante sequestro em que o agente é flagrado tendo em seu poder uma das vítimas, havendo outras ainda em cativeiro desconhecido. Caso seja apreendido em poder do mesmo um telefone celular ou computador, teria a autoridade policial de formular pedido escrito, protocolizá-lo, aguardar a distribuição, agendar audiência para despachar com o Juízo competente para só então acessar as informações que poderiam servir para salvar a vida de terceiros? Imagine-se também a eventual prisão em flagrante de um agente que ameaça explodir bombas-relógio deixadas em locais desconhecidos e com potencial para ceifar dezenas ou milhares de vidas. Seria exigível, neste caso, a observância prévia das mesmas formalidades acima mencionadas? (MAGALHÃES, 2019, p. 549)

Torna-se imprescindível, assim, avaliar se a prisão é lícita e se o acesso aos dados é absolutamente necessário para o fim da persecução penal, tais como proteção das autoridades ou vítimas. Ademais, a extensão da medida deve ser proporcional, isto é, o acesso deve ser limitado aos dados que tenham pertinência temporal e temática, além de todas as medidas tomadas terem de ser detalhadamente relatadas pela autoridade policial.

Logo, apenas quando a demora na obtenção de mandado acarrete consequências desastrosas ou mesmo irreparáveis, estaria planificada a suficiente razoabilidade para a restrição da privacidade, independentemente de decisão judicial (ZILLI, 2018, p. 79). Ademais,

> As hipóteses dependem da variedade própria da casuística, não sendo possível fixar uma diretriz fechada e restrita. Mas, a localização da vítima, a possibilidade de identificação de comparsas que também se encontrem em situação de flagrante, a possibilidade de se evitar a prática de novo crime e a possibilidade de localização dos objetos da infração são apenas algumas das situações plausíveis. (ZILLI, 2018, p. 87)

A regra geral, portanto, é a dependência do mandado judicial, provocado no próprio inquérito policial, sob pena de considerar-se ilícito o acesso sem prévia autorização. Este seria possível apenas quando verificadas as hipóteses de absoluta imprescindibilidade, caracterizada pelo risco à vida ou incolumidade física, ou, ainda, risco de perecimento de prova indispensável e insubstituível para a elucidação do crime.

6. CONCLUSÃO

O controle de legalidade sobre a atuação policial é imprescindível para a adequada consolidação de garantias fundamentais em um Estado

Democrático de Direito. Trata-se, com efeito, de agregar esforços na tentativa de controle constitucional da intervenção do Estado no contexto social, com vistas a compatibilizar o direito de privacidade com a necessária tutela repressiva penal.

A análise judicial dessa celeuma nos Tribunais Superiores brasileiros tem demonstrado oscilação entre o entendimento consolidado no STF e no STJ. No entanto, considerados os pronunciamentos mais recentes, é possível que haja modificação da jurisprudência do Supremo, no sentido da necessidade de expedição de mandado judicial prévio, o que se aproximaria da perspectiva mais garantista apresentada pelo STJ e pelo julgado *Riley v. California*.

O acesso sem autorização ao conteúdo dos *smartphones*, portanto, acarreta a ilicitude das provas obtidas, razão pela qual é primordial que haja a pacificação quanto à matéria nas Cortes, máxime tendo em vista as novas disposições do Marco Civil da Internet e da LGPD.

A ressignificação do direito de privacidade estimula novas perspectivas no tratamento das informações pessoais, o que demanda cautela também por parte da administração pública, seja no tratamento judicial, seja na fase de investigação criminal.

Desse modo, tendo em vista a compreensão acerca da inviolabilidade de domicílio, interceptação telemática e custódia de dados armazenados, entende-se que a regra geral é a impossibilidade de acesso ao conteúdo dos aparelhos celulares na ocasião da prisão em flagrante, sem prévio mandado judicial, restringindo-se tal possibilidade, tão somente, à situação em que verificadas as hipóteses de absoluta imprescindibilidade, como risco à vida ou à incolumidade física, ou, ainda, risco de perecimento de prova indispensável e insubstituível para a elucidação do crime.

Outrossim, em tais situações, é necessário que haja observância aos pilares de licitude da prisão, à necessidade, adequação e proporcionalidade em sentido estrito, limitação temporal, pertinência temática e relato detalhado do procedimento pela autoridade policial. Propugna-

-se, nesse sentido, pela consolidação da legalidade constitucional que proporcione o respeito aos direitos fundamentais, à democracia e ao Estado de Direito, assegurando a adequada tutela penal sem sacrifícios exacerbados de garantias.

REFERÊNCIAS

ALEXY, Robert. *Teoria dos direitos fundamentais*. 2. ed. São Paulo: Malheiros, 2015.

ÁVILA, Humberto Bergmann. A distinção entre princípios e regras e a redefinição do dever de proporcionalidade. *Revista de Direito Administrativo*, Rio de Janeiro, n. 215, 1999.

BRASIL. Superior Tribunal de Justiça. *RHC n. 51.531/RO*. Rel. min. Nefi Cordeiro, Sexta Turma, julgado em 19-4-2016, *DJe* de 9-5-2016.

BRASIL. Supremo Tribunal Federal. *HC n. 91.867/PA*. Rel. min. Gilmar Mendes, Segunda Turma, julgado em 24-4-2012, *DJe* 185, de 20-9-2012.

BRASIL. Supremo Tribunal Federal. *HC n. 124.322/RS AgR*. Rel. min. Roberto Barroso, Primeira Turma, julgado em 9-12-2016, *DJe* 268, de 19-12-2016.

BRASIL. Supremo Tribunal Federal. *Informativo n. 944*. Brasília, 10 a 14 jun. 2019. Disponível em: http://www.stf.jus.br/arquivo/informativo/documento/informativo944.htm. Acesso em: 15 out. 2020.

CAMBI, Eduardo. *Direito constitucional à prova no processo civil*. Coleção Temas Atuais de Direito Processual Civil. São Paulo: Revista dos Tribunais, 2001. v. 3.

DEZEM, Guilherme Madeira. A busca e apreensão em celulares: algumas ponderações em torno da proteção de dados, da privacidade e da eficiência do processo. *Cadernos Jurídicos*, São Paulo, ano 21, n. 53, jan.-mar. 2020, p. 35-48.

ESTADOS UNIDOS DA AMÉRICA. Suprema Corte dos Estados Unidos da América. *RILEY v. CALIFORNIA*. Disponível em: https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf. Acesso em: 15 out. 2020.

FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito*. Universidade de São Paulo, n. 88, p. 440. Disponível em: http://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 13 out. 2020.

GIMENEZ, Luiz Victor Rós. *Direito probatório de terceira geração*: os aspectos jurídicos que envolvem a obtenção de provas extraídas de *smartphones* no ato da prisão em flagrante. Monografia (Bacharel em Direito) – Centro Universitário "Antônio Eufrásio de Toledo" de Presidente Prudente. São Paulo, p. 86. 2018.

LIMA, Renato Brasileiro de. *Manual de processo penal*: volume único. 5. ed. Salvador: Editora JusPodivm, 2017.

MAGALHÃES, Vlamir Costa. Ilicitude probatória em processo penal e regra de exclusão (*exclusionary rule*): comentários sobre a legitimidade do acesso a aparelhos eletrônicos apreendidos em situação flagrancial. *Direito Federal: Revista da AJUFE*. São Paulo, v. 31, n. 97, jan./jun. 2019.

MAGRANI, Eduardo. *Entre dados e robôs*: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MARANHÃO, Juliano. O que é dado não comunicado? *In*: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (Eds.). *Direitos funda-*

mentais e processo penal na era digital: doutrina e prática em debate. São Paulo: InternetLab, 2018. v. 1.

RODOTÀ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SCAFF, Fernando Facury. *A responsabilidade civil do Estado intervencionista*. 2. ed. Rio de Janeiro: Renovar, 2001. p. 236-237.

SILVA, César Dario Mariano da. *Provas ilícitas*: princípio da proporcionalidade, interceptação e gravação telefônica, busca e apreensão, sigilo e segredo, confissão, comissão parlamentar de inquérito (CPI) e sigilo. 6. ed. São Paulo: Atlas, 2010.

SILVA, De Plácido e. *Vocabulário jurídico*. 2. ed. Rio de Janeiro/São Paulo: Forense, 1967. v. 3.

WARREN, Samuel D.; BRANDEIS, Louis D. *The right to privacy*. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acesso em: 15 out. 2020.

ZILLI, Marcos. A prisão em flagrante e o acesso de dados em dispositivos móveis. Nem utopia, nem distopia. Apenas a racionalidade. *In*: ABREU, Jacqueline de Souza; ANTONIALLI, Dennys (Eds.). *Direitos fundamentais e processo penal na era digital*: doutrina e prática em debate. São Paulo: InternetLab, 2018. v. 1.

A IMPORTÂNCIA DO COMPARTILHAMENTO DE DADOS PESSOAIS PARA FINS DE INVESTIGAÇÃO CRIMINAL E OS POSSÍVEIS REFLEXOS DA LGPD

Luiz Fernando Rodrigues[1]

RESUMO

Este artigo analisa a importância do compartilhamento de dados pessoais para fins de investigação criminal, mediante convênios e acordos de cooperação técnica, tomando-se por base o ordenamento jurídico previsto na Lei n. 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). O tema mostra-se relevante, pois, o art. 4º, § 1º, dessa norma estabelece que o tratamento de dados pessoais para fins de segurança pública, defesa nacional, segurança do Estado, atividades de investigação e repressão de infrações penais será objeto de legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público.

---

1 Mestre em Ciências Contábeis pela Universidade de Brasília. Especialista em auditoria e perícia contábil. Pós-graduando em Direito do Uso e Proteção de Dados pela PUC-Minas. Graduando em Direito pela Universidade Católica de Brasília. Analista de contabilidade/perito do MPU e professor da pós-graduação na Universidade Católica de Brasília.

Nesse sentido, foi criada uma comissão de juristas na Câmara dos Deputados com o objetivo de estudos sobre a norma prevista no art. 4º, em especial no que se refere ao tratamento de informações pessoais no âmbito da segurança pública, investigações penais e repressão de infrações penais. O diploma legal ainda não foi editado até a conclusão deste trabalho. Diante do contexto atual, entende-se que ele levará em consideração a importância do compartilhamento de dados entre os órgãos da administração pública para fins de investigação e as repercussões da LGPD nesse processo. Isso é fundamental para ensejar maior segurança jurídica e melhor governança dos dados sob responsabilidade desses órgãos, bem como diminuir as incertezas na aplicação e interpretação dos dispositivos relacionados ao compartilhamento de dados dentro do governo.

Palavras-chave: Lei Geral de Proteção de Dados. Dados pessoais. Investigação. Compartilhamento.

ABSTRACT

Taking as a base the legal order established in the General Data Protection Law (GDPL), this article analyzes the importance of sharing personal data shared for criminal investigation purposes, through technical cooperation agreements and agreements. The theme is relevant because, although art. 4, III, of Law N. 13,709/2018 exclude from its scope of application several activities, including those of investigation and repression of crimes, provides that the processing of personal data provided for in item III will be governed by specific legislation, which shall provide for proportional and strictly necessary measures to serve the public interest, subject to due legal process. In this sense, a commission of lawyers was created in the Chamber of Deputies to prepare studies on the specific law provided for in art. 4th. The said law has not yet been edited until the conclusion of this work. Thus, it is understood

that the forthcoming law must consider the importance of data sharing between public administration bodies for research purposes and the repercussions of GDPL in this process. This is essential to provide greater legal certainty and better governance of data under the responsibility of these bodies, as well as to reduce uncertainties in the application and interpretation of rules related to data sharing within the government.

Keywords: General Data Protection Law. Personal data. Investigation. Sharing.

1. INTRODUÇÃO

A Lei n. 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) visa proteger informações sensíveis de pessoas físicas e apresenta caráter de norma geral, a ser observado por órgãos da União, dos Estados, do Distrito Federal e dos Municípios.

Em seu art. 4º, III, a LGPD afasta sua incidência sobre o tratamento de dados pessoais realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais.

Já o § 1º do art. 4º estabelece que o tratamento de dados pessoais inscritos no inciso III será objeto de legislação específica, a qual versará medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos na lei.

Diante dessa prerrogativa, em 26 de novembro de 2019, foi criada uma comissão de juristas pelo presidente da Câmara dos Deputados, Rodrigo Maia (DEM-RJ), a fim de elaborar anteprojeto de legislação específica ao tratamento de dados pessoais no âmbito da segurança pública, investigação penal e repressão de crimes. Vale destacar, no entanto, que, até a conclusão deste trabalho, a edição não foi finalizada.

A despeito da ausência de normativo específico, a LGPD já prevê que as organizações públicas e privadas só poderão coletar dados pessoais se tiverem o consentimento do titular. Além disso, precisam deixar claro para ele o que será coletado, para quais fins e se haverá compartilhamento. Esse é o ponto fundamental em análise aqui; pois, na maioria das bases de dados compartilhadas para fins de investigação, quando o cidadão disponibiliza informações pessoais, não o faz com esse intuito, ou seja, ele as apresenta à Receita Federal, ao INSS, à Justiça Eleitoral, por motivos outros. Todavia, todos os dados podem ser compartilhados com órgãos de investigação por meio de convênios ou acordos de cooperação, constituindo, portanto, uma importante base de investigação.

Daí o desafio da lei vindoura: assegurar a preservação dos direitos dos cidadãos resguardados pela LGPD, mas também observar o papel dos órgãos de investigação e os interesses públicos envolvidos.

2. LEI GERAL DE PROTEÇÃO DE DADOS E REGULAMENTO GERAL SOBRE PROTEÇÃO DE DADOS

Apesar de atualmente o tema fomentar diversas discussões nos meios acadêmicos, jurídicos e de tecnologia, tanto no âmbito público quanto privado, não se pode afirmar que a preocupação com dados pessoais seja muito recente, pois, no Brasil, outras leis já tratavam de forma direta ou indireta do uso desses dados.

Influenciado pelo Regulamento Geral sobre a Proteção de Dados – ou *General Data Protection Regulation* (GDPR), em inglês –, da União Europeia, o Brasil sancionou, em 14 de agosto de 2018, a LGPD – Lei n. 13.709/2018 –, com vistas a estabelecer um prazo para adequação. Após idas e vindas, ela finalmente entrou em vigor no dia 18 de setembro de 2020, porém sem a formalização das sanções administrativas, adiada para agosto de 2021, e da Autoridade Nacional de Proteção de Dados.

A LGPD é bastante abrangente no que se refere às informações protegidas, basta analisar os fundamentos previstos em seu art. 2º:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I – o respeito à privacidade;
>
> II – a autodeterminação informativa;
>
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV – a inviolabilidade da intimidade, da honra e da imagem;
>
> V – o desenvolvimento econômico e tecnológico e a inovação;
>
> VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Com a entrada em vigor da LGPD, entende-se que, além dos órgãos públicos, todas as pessoas e qualquer empresa ou grupo de empresas que incluir em suas bases de dados informações de clientes ou não, sendo para fins econômicos, devem seguir os procedimentos previstos na lei.

3. DADOS PESSOAIS E DIREITOS E GARANTIAS FUNDAMENTAIS PREVISTOS NA CONSTITUIÇÃO

De acordo com Rangel (2016, p. 16), a definição de direitos e garantias fundamentais é oscilante de Estado para Estado e, consequentemente, de autor para autor. Qualquer conceito pode resultar insatisfatório para o leitor, face à ausência de conteúdo próprio ou, ainda, inexatidão quanto a delimitação e abrangência. Até porque há no Direito uma síncope entre os juristas, o que significa dizer: usam frequentemente palavras diversas para se referirem ao mesmo conceito e, muitas vezes,

por meio das mesmas palavras, acreditam estarem abordando conceitos diferentes. Não são poucos aqueles que se propõem a estudar direitos e garantias fundamentais sem sequer defini-los.

Ainda segundo Rangel (2016, p. 18), os direitos e garantias fundamentais são aqueles que têm como escopo respeitar a dignidade da pessoa humana, protegendo-a do arbítrio estatal, criando, assim, condições necessárias para uma vida em sociedade livre de preconceitos e visando ao desenvolvimento do ser humano. Trata-se de situações jurídicas de natureza constitucional fundamentadas no princípio da soberania popular, as quais, portanto, podem e devem ser exigidas do Estado através do exercício do direito subjetivo público de ação.

Com relação ao sigilo de dados, Ferraz Júnior (1993, p. 439) entende que a inviolabilidade do sigilo de dados (art. 5º, XII, CF/1988) é correlata ao direito fundamental à privacidade (art. 5º, X, CF/1988) e que em questão está o direito de o indivíduo excluir do conhecimento de terceiros aquilo que a ele só é pertinente e que diz respeito ao seu modo de ser exclusivo no âmbito de sua vida privada.

Nesse sentido, é relevante analisar o julgamento de liminar em sede da Ação Direta de Inconstitucionalidade (ADI) n. 6.387, na qual a Ordem dos Advogados do Brasil (OAB) questionou a constitucionalidade da Medida Provisória (MP) n. 954, de 17 de abril de 2020, que dispunha sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de serviço telefônico fixo comutado e de serviço móvel pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE). Buscava-se, com a edição da medida, dar suporte à produção estatística oficial durante a situação de emergência de saúde pública internacional decorrente do novo coronavírus, nos termos da Lei n. 13.979, de 6 de fevereiro de 2020.

No caso concreto, assim entendeu a ministra Rosa Weber, do STF:

> A Constituição da República confere especial proteção à intimidade,

> à vida privada, à honra e à imagem das pessoas ao qualificá-las como invioláveis, enquanto direitos fundamentais da personalidade, assegurando indenização pelo dano material ou moral decorrente de sua violação (art. 5º, X). O assim chamado direito à privacidade (*right to privacy*) e os seus consectários direitos à intimidade, à honra e à imagem emanam do reconhecimento de que a personalidade individual merece ser protegida em todas as suas manifestações. A fim de instrumentalizar tais direitos, a Constituição prevê, no art. 5º, XII, a inviolabilidade do "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução penal. (BRASIL, STF, 2020)

Note-se o destaque dado pela ministra quanto às informações relacionadas à identificação – efetiva ou potencial – de pessoa natural a configurarem dados pessoais e integrarem, nessa medida, o âmbito de proteção das cláusulas constitucionais assecuratórias da liberdade individual (art. 5º, *caput*), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII). A manipulação e o tratamento, desse modo, hão de observar, sob pena de lesão a esses direitos, os limites delineados pela proteção constitucional.

A ministra asseverou ainda que, em decorrência dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da LGPD, como fundamentos específicos da disciplina da proteção de dados pessoais.

Apesar do citado entendimento, seguido por outros nove ministros, há de se destacar o questionamento de Doneda (2019, p. 261): "Possuindo a privacidade tutela constitucional, poderíamos afirmar que igualmente a proteção de dados pessoais estaria tutelada constitucionalmente?" Para o autor, se derivarmos a proteção de dados pessoais diretamente da privacidade, tal qual espécie e subespécie, poderíamos

sustentar existir uma extensão da tutela da privacidade à proteção de dados pessoais, sendo essa última mão longa da primeira.

Segundo Doneda (2019, p. 262), se, por um lado, a privacidade é encarada como direito fundamental, as informações pessoais em si parecem, a uma parte da doutrina, protegidas somente em relação a sua "comunicação", conforme art. 5º, XII, que trata da inviolabilidade da comunicação de dados.

Como não há na Constituição Federal de 1988 (CF/1988), de forma expressa, essa proteção, observa-se que a tutela do direito fundamental à proteção de dados pessoais tem sido buscada a partir do art. 5º, XII, da CF/1988, que assegura a inviolabilidade do sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas.

Nesse sentido, Ferraz Júnior (1993, p. 447 *apud* DONEDA, 2019, p. 262-263), aponta que

> o sigilo, no inciso XII do art. 5º, está referido à comunicação, no interesse da defesa da privacidade. Isto é feito, no texto, em dois blocos: a Constituição fala em sigilo "da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas".

Para o autor, o que se regula, portanto, é a comunicação por correspondência e telegrafia, comunicação de dados e telefonia. Desse modo, ressalta que o objeto protegido no direito à inviolabilidade do sigilo não são os dados em si, mas a sua comunicação restringida (liberdade de negação). A troca de informações privativa é que não pode ser violada por sujeito estranho à comunicação.

Doneda (2019, p. 262) destaca ainda decisão do STF relatada pelo ministro Sepúlveda Pertence, que reconheceu expressamente a inexistência da garantia de inviolabilidade sobre dados armazenados em computador com fulcro em garantias constitucionais, endossando, portanto, a tese de Ferraz Júnior.

Tanto é assim que tramita na Câmara dos Deputados a Proposta de Emenda à Constituição n. 17-A, de 2019, do Senado Federal. Pretende-se com ela alterar a Constituição Federal justamente para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

Como se observa, apesar de decisões judiciais em sentido diverso, é natural que a proteção aos dados pessoais, por não estar expressa no texto constitucional, enseje discussões acerca da tutela protetora para impedir intervenções. Ou seja, em última instância, o Estado não pode violar qualquer direito fundamental, exceto em hipóteses legais, que representam a exceção.

Daí a importância de se entender o alcance da LGPD e as repercussões no compartilhamento de dados pessoais para fins de investigação criminal.

4. COMPARTILHAMENTO E USO DE DADOS PARA FINS DE INVESTIGAÇÃO CRIMINAL

Diante da conjuntura apresentada, faz-se necessário avaliar a estratégia regulatória para a própria compreensão do conteúdo informacional. É imprescindível, nesse caso, evidenciarem-se possíveis problemáticas em torno de uma estratégia de investigação e governança de dados dogmática e anacrônica pensada em anos anteriores. Deve-se verificar, inclusive, o descompasso entre soluções governamentais que visam ao interesse público e o empoderamento do titular dos dados pessoais, o qual tem o direito de consentir com o uso dos próprios dados e cientificar-se quanto à destinação da coleta.

Mendroni (2013, p. 353) afirma que o promotor e a autoridade policial podem e devem levar a cabo investigação – através da requisição de documentos a órgãos públicos e particulares, com vistas a posterior

análise, confrontação com outras provas etc. Para tanto, sugere a possibilidade de requisitarem dados aos seguintes órgãos:

a) DVC, Prodesp;
b) Receita Federal (mediante aut. judicial);
c) Bancos (extratos mediante aut. judicial);
d) Secretarias das Fazendas Estaduais;
e) Cartórios: Registro de Imóveis e Títulos e Documentos;
f) Detran: pesquisa: placa, proprietário, histórico, endereço, multas;
g) Juntas Comerciais;
h) Telefônica (mediante aut. judicial);
i) Companhias de seguros;
j) Companhias de assistência médica;
k) Companhias aéreas;
l) BOs – do bairro onde o investigado morou;
m) Polícia Federal.

Conforme mencionado, na maioria dessas bases, quando o cidadão disponibiliza seus dados, não o faz para fins de investigação, mas eles podem ser compartilhados para tal finalidade.

Marat (2008, p. 181 *apud* KHALED, 2013, p. 177-118) salienta ser essencial que a instrução do processo esteja sujeita a formas fixas, precisas, regulares, para que não se conduza de maneira arbitrária à coisa mais grave do mundo. Por conseguinte, essa parte da legislação criminal exige muita atenção não somente por ser indispensável regulamentar todos os seus atos e a forma de cada um deles em especial, mas também para assegurar o cumprimento dessas regras, redundando nulo aquilo que for contrário a elas.

Segundo Santin (2001, p. 2), a atividade de investigação criminal destina-se ao fornecimento de elementos mínimos sobre a autoria e materialidade do delito, para a formação da *opinio delicti* do Minis-

tério Público, o desencadeamento ou não da ação penal pública e o embasamento para o recebimento da denúncia e concessão de medidas cautelares pelo juiz. Também serve para embasar a queixa-crime da vítima nos crimes de ação privada ou ação penal subsidiária. A atribuição para a realização de investigação criminal é das polícias, especialmente a federal, as civis e as militares, por crimes federais, estaduais e militares, respectivamente.

Nesse diapasão, a Lei n. 12.850, de 2 de agosto de 2013, que define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, as infrações penais correlatas e o procedimento criminal, prevê em seu art. 3º:

> Art. 3º Em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção da prova:
>
> I – colaboração premiada;
>
> II – captação ambiental de sinais eletromagnéticos, ópticos ou acústicos;
>
> III – ação controlada;
>
> IV – acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais;
>
> V – interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica;
>
> VI – afastamento dos sigilos financeiro, bancário e fiscal, nos termos da legislação específica;
>
> VII – infiltração, por policiais, em atividade de investigação, na forma do art. 11;
>
> VIII – cooperação entre instituições e órgãos federais, distritais, estaduais e municipais na busca de provas e informações de interesse da investigação ou da instrução criminal.

De acordo com Bitencourt (2014, p. 108), a própria previsão legal de cooperação entre órgãos públicos consiste em uma expressa confissão de incapacidade de realização do controle social penal pelo Estado. Não é concebível que seja necessário constar de disposição legal tamanha obviedade. Aliás, a obstrução de investigação criminal, seja por agente público, seja por particular, constitui crime previsto no Código Penal (CP) desde 1940, pois resulta necessariamente em um favorecimento real ou pessoal (arts. 348 e 349). Assim, a colaboração entre os órgãos públicos para fins de investigação criminal é medida de rigor e – ao menos deveria ser – a regra em tais casos. Trata-se, por conseguinte, de mera previsão programática, que corresponde quase perfeitamente à redação do art. 7º, *b*, da Convenção de Palermo, o que serve para revelar, também, o quanto a legislação interna brasileira absorve de influência internacional.

Na lição de Bitencourt (2014, p. 108), a troca de informações, na era da comunicação, é medida essencial de inteligência para o controle social da atividade criminosa. Todas as instituições oficiais deveriam imediatamente convergir para um sistema de dados unificado, que permitisse a múltipla alimentação e o acesso desde as agências oficiais a todos os dados, indistintamente, sempre que envolvidas questões criminais. Afinal, as informações públicas pertencem ao Estado como um todo e não podem ser consideradas "particularizadas" ou "inacessíveis" entre os distintos órgãos estatais. Muito diferente, entretanto, é permitir-se sua publicidade. O acesso à informação pública, pelo agente público, há de ser indiscriminado. Mas o seu uso há de ser restrito às hipóteses de ausência de violação da intimidade daqueles a quem as informações se refiram; quando não, deve ser submetido a rigoroso controle judicial.

Nesse sentido, Mendroni (2013, p. 354) enfatiza lógico que a investigação criminal seja realizada, no âmbito de obtenção de dados e informações sobre os fatos, o mais rápido possível, antes que o suspeito tenha conhecimento da investigação. Caso contrário, agirá rapidamente

para ocultar e apagar provas e evidências. Em outros países, isso não seria possível, uma vez que configuraria outro delito, o de "obstrução da justiça", não contemplado no direito positivo penal brasileiro.

Observe-se, portanto, a importância do compartilhamento de dados para fins de investigação nos mais diversos contextos. Por exemplo, ante suspeita de que determinada pessoa seja proprietária de empresa investigada por fraudar licitações, é justificável o acesso a bases de dados compartilhadas para que tal informação seja confirmada ou mesmo refutada. Tal procedimento garante a celeridade nas investigações e a segurança nas demais ações. Essa medida também poderá ser adotada para garantir a instauração de inquérito ou outro procedimento investigatório que dependa dos dados obtidos preliminarmente para ser realizado.

Destaque-se, por relevante, a natureza relativa da proteção ao sigilo, assim como de outros direitos consagrados, inclusive na Constituição Federal. Sua garantia cede espaço ao interesse público maior consubstanciado na apuração de crimes.

5. SUPREMACIA DO INTERESSE PÚBLICO EM RELAÇÃO AO PRIVADO

Quando o assunto é acesso de dados pessoais e compartilhamento para fins de investigação, não há dúvidas de que a celeuma gira em torno do confronto entre o direito de o Estado proceder à investigação com base no interesse público e o direito fundamental à privacidade e intimidade dos cidadãos.

Não obstante, conforme estudado anteriormente, o próprio STF reconhece que o direito à intimidade e privacidade no sentido dessas medidas não é absoluto, comportando exceções, observados os termos e as exigências da legislação específica.

Ao tratar do afastamento de sigilos bancários e fiscais para fins de investigação, a partir de decisão judicial fundamentada, Bitencourt

(2014, p. 107) cita Ferraz Júnior quando este afirma que: "em questão está o direito de o indivíduo excluir do conhecimento de terceiros aquilo que a ele só é pertinente e que diz respeito ao seu modo de ser exclusivo no âmbito de sua vida privada".

Nesse sentido, Bitencourt (2014, p. 107) conclui que a questão de conflito entre princípios, quais sejam, o interesse público na persecução criminal e a preservação da intimidade individual, deve ser ponderada para filtrar a correta hermenêutica a respeito da regra. A regra resulta aplicável, desde que ajustada aos princípios sobre ela incidentes.

Bitencourt (2014, p. 107) cita, ainda, dois aspectos considerados cruciais: a necessidade de a autoridade pública que investiga a persecução de um crime ter acesso aos dados, porque essencial para o deslinde da investigação; e de as informações oferecidas serem mantidas sob sigilo da autoridade que as recebe, bem como de sua consecução submeter-se ao controle judicial, na forma expressa no art. 23 da Lei n. 12.850/2013.

Nessa linha, a Diretiva n. 2016/680 da União Europeia (UE) determina que o exercício das funções de prevenção, investigação, detecção ou repressão de infrações penais conferidas institucionalmente por lei às autoridades competentes permite-lhes exigir às pessoas singulares o cumprimento do que lhes é solicitado. Nesse caso, o consentimento do titular, na acepção do Regulamento n. 2016/679, também da EU, não deverá constituir o fundamento jurídico do tratamento de dados pessoais pelas autoridades competentes. Caso seja impingido a cumprir uma obrigação legal, o titular não tem verdadeira liberdade de escolha, pelo que sua reação não poderá ser considerada livre manifestação da vontade.

5.1 GARANTISMO PENAL EM RELAÇÃO A DADOS PESSOAIS

Considerando o escopo do trabalho, ou seja, o compartilhamento de dados pessoais para fins de investigação criminal, não se poderia

deixar de mencionar o chamado garantismo penal. Segundo Ferrajoli (1998 *apud* RANGEL, 2016, p. 20):

> (...) designa um modelo normativo de direito: precisamente, no que diz respeito ao direito penal, o modelo de estrita legalidade SG, próprio do Estado de direito, que se caracteriza como um sistema cognitivo ou de poder mínimo, sob o plano jurídico, como um sistema de vínculos impostos à função punitiva do Estado em garantia dos direitos dos cidadãos. É consequentemente, garantista todo sistema penal que se conforma normativamente com tal modelo e que o satisfaz efetivamente.

No entender de Rangel (2016, p. 30), ele visa à utilização de um sistema normativo constitucional por meio da construção de barreiras limitadoras e punitivas dos abusos aos direitos fundamentais e do exercício arbitrário do poder, estabelecendo um âmbito dentro do qual as liberdades públicas do indivíduo, enquanto ser livre, possam ser tuteladas eficazmente. O fundamento e o fim do garantismo penal é a tutela da liberdade do indivíduo frente às várias formas de exercício arbitrário do poder político. É a efetividade dos preceitos constitucionais.

Para o autor, há perfeita simbiose entre o Estado Constitucional Democrático de Direito e a Teoria do Garantismo Penal. Somente no respeito ao princípio da legalidade, com a submissão do poder público – representado pelo Legislativo, Executivo e Judiciário – ao império da Constituição e seu efetivo compromisso com as garantias dos direitos fundamentais dos cidadãos, são criadas as condições para que o texto constitucional se irradie no cotidiano da sociedade. Não há espaço, assim, em um Estado de Direito, enquanto democrático for, para exercício de poder sem limite e ato de poder que não seja objeto de controle jurisdicional.

Rangel ressalta ainda que o garantismo é uma forma de se dar ao cidadão mecanismos para pleno exercício de direitos fundamentais vio-

lados por meio de atos de império, a fim de que se possa restabelecer a ordem jurídica violada. O princípio da legalidade exige que o exercício de qualquer poder tenha na lei justa (entenda-se lei submetida aos ditames constitucionais) sua fonte formal de legitimidade.

Em sentido diverso, Lopes e Gloeckner (2014, p. 48) advertem que o termo "garantismo", no atual contexto, em especial em *terrae brasilis*, padece de compreensão mais alargada e menos preconceituosa. Costumeiramente, como faz o senso comum jurídico, desvirtuou-se o conceito para, de forma maniqueísta, se construir uma verdadeira dicotomia (falsa) entre garantistas e não garantistas. Como se alguém pudesse racionalmente advogar em prol da inaplicabilidade da Constituição da República. Para todos aqueles que desejarem uma compreensão despida de falsos imbróglios e de premissas destituídas de rigor científico, o garantismo pode ser orquestrado através de uma teoria do Direito e de uma teoria da democracia. Esta, aliás, a última construção de Ferrajoli.

Lopes e Gloeckner (2014, p. 48) asseveram que se deve buscar o significado jurídico da expressão "garantismo" antes de tudo. Inegável é, para Ferrajoli, que a palavra "garantia" adquiriu, de súbito, nos anos recentes, uma ampliação de significado que culminou com sua utilização em campos os mais diversos do Direito. Tal resultado não deixou indene o direito penal e o processual penal.

No artigo *The Right to Privacy*, os juízes da Suprema Corte dos Estados Unidos Samuel D. Warren e Louis D. Brandeis afirmam que o indivíduo deve ter proteção total em relação à pessoa e à propriedade, mas, de tempos em tempos, tem sido necessário definir novamente a natureza exata e a extensão dessa proteção. As mudanças políticas, sociais e econômicas envolvem o reconhecimento de novos direitos, e o direito comum, em sua eterna juventude, cresce para atender às demandas da sociedade (WARREN; BRANDEIS, 1890).

6. COMPARTILHAMENTO DE DADOS ENTRE ÓRGÃOS PÚBLICOS

No que se refere ao compartilhamento de dados, foi publicado o Decreto n. 10.406/2019, que trata do assunto no âmbito da administração pública federal. O diploma refere-se à disponibilização de dados pelo gestor a um determinado receptor.

Observe-se que, ao excluir as atividades da abrangência da LGPD e regulamentar o compartilhamento de dados com base na legislação supra, o legislador criou uma celeuma. Questiona-se se os órgãos que exercem as atividades descritas no inciso III do art. 4º da Lei n. 13.709/2018 estariam sujeitos ao cumprimento dos requisitos previstos no Decreto n. 10.046/2019, conforme será visto a seguir.

O Decreto n. 10.046/2019 dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. O art. 3º detalha as diretrizes que devem nortear a ação:

> Art. 3º O compartilhamento de dados pelos órgãos e entidades de que trata o art. 1º observará as seguintes diretrizes:
>
> I – a informação do Estado será compartilhada da forma mais ampla possível, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na Lei n. 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais;
>
> II – o compartilhamento de dados sujeitos a sigilo implica a assunção, pelo recebedor de dados, dos deveres de sigilo e auditabilidade impostos ao custodiante dos dados;
>
> III – os mecanismos de compartilhamento, interoperabilidade e auditabilidade devem ser desenvolvidos de forma a atender às necessidades de negócio dos órgãos e entidades de que trata o art. 1º, para facilitar a execução de políticas públicas orientadas por dados;
>
> IV – os órgãos e entidades de que trata o art. 1º colaborarão para

a redução dos custos de acesso a dados no âmbito da administração pública, inclusive, mediante o reaproveitamento de recursos de infraestrutura por múltiplos órgãos e entidades;

V – nas hipóteses em que se configure tratamento de dados pessoais, serão observados o direito à preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação; e

VI – a coleta, o tratamento e o compartilhamento de dados por cada órgão serão realizados nos termos do disposto no art. 23 da Lei nº 13.709, de 2018.

Nesse ponto, importante relembrar o citado art. 23:

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

I – sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para *a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;*

II – (VETADO); e

III – seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei n. 13.853, de 2019)

IV – (VETADO). (Incluído pela Lei n. 13.853, de 2019) Vigência

§ 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

§ 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no *caput* deste artigo de instituir as autoridades de que trata a Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei n. 9.507, de 12 de novembro de 1997 (Lei do *Habeas Data*), da Lei n. 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo), e da Lei n. 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

§ 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no *caput* deste artigo, nos termos desta Lei.

§ 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o *caput* deste artigo.

Segundo consta da Resolução n. 2/2020 do Ministério da Economia, as diretrizes para categorização de compartilhamento de dados foram elaboradas pelo Comitê Central de Governança de Dados, de acordo com os arts. 21 e 31 do Decreto n. 10.046/2019. As orientações presentes são válidas para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União.

O objetivo é facilitar o compartilhamento de dados dentro do governo, esclarecendo conceitos e procedimentos operacionais básicos para cumprimento do referido decreto.

Nessa fase, três frentes estão sendo abordadas: a) redução da ambiguidade das normas legais existentes; b) categorização de dados para facilitar o compartilhamento de dados; e c) adequação dos requisitos de segurança para o compartilhamento de dados.

A análise da Resolução n. 2/2020 evidencia que a intenção do legis-

lador foi permitir o compartilhamento de dados em geral entre órgãos da administração pública, sem se ater à finalidade específica de cada órgão, ou seja, ela prevê uma categorização dos dados, porém a finalidade vai depender do gestor que os receber:

> A categorização visa separar os compartilhamentos em três grandes grupos: amplo, restrito e específico. Na verdade, isso já é uma prática em muitos órgãos, mesmo que com outros nomes.
>
> Amplo são os dados que deveriam estar em transparência ativa, ou que são cedidos sempre que solicitados pelo Serviço de Informações ao Cidadão (SIC). Trocá-los entre órgãos não é um problema, geralmente.
>
> Os demais tipos são dados que possuem normas afirmando que são protegidos de ampla divulgação ou sigilosos, que não podem ser publicados. Mas isso não implica, ou proíbe, que sejam compartilhados dentro do governo. Os órgãos geralmente separam esses dados em dois grupos. O primeiro é o que habitualmente é cedido aos órgãos públicos, sem uma análise profunda de seu uso. Isso se deve, geralmente, ao baixo risco associado a essas informações. O segundo é um grupo de informações críticas, capazes de trazer problemas graves para seus titulares ou para o órgão. Até hoje, esses dois grupos estavam sob as mesmas regras. A categorização pretende separá-los.
>
> O gestor de dados irá decidir quais informações estão em cada grupo, usando as orientações desse documento e da aplicação das normas legais.

Importante destacar que, em seu item 5.1.9, a resolução prevê que os dados recebidos por compartilhamento restrito poderão ser retransmitidos ou compartilhados com outros órgãos ou entidades que comprovem a necessidade de acesso, exceto se proibido expressamente na autorização concedida pelo gestor de dados ou se houver posterior revogação da permissão, mediante fundamentação, nas duas hipóteses (art. 12, § 4º, do Decreto n. 10.046/2019). O item 5.1.10 estabelece que qualquer re-

transmissão e compartilhamento de dados continuam sujeitos aos termos do decreto, inclusive entre as instituições abrangidas: órgãos e entidades da administração pública federal direta, autárquica e fundacional.

Mesmo analisando detidamente as normas de compartilhamento de dados até aqui, em conjunto com o art. 4º, III, da Lei n. 13.709/2018, restam dúvidas quanto aos órgãos de investigação poderem ter acesso a dados pessoais de bases mantidas por outras instituições públicas, independentemente das regras previstas na LGPD, no Decreto n. 10.046/2019 e na Resolução n. 2/2020.

Considerando que o GDPR é inspiração para a LGPD, é relevante analisar de que forma os países da Europa lidam com a temática relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, conforme é descrito nessa diretiva.

Segundo disposto na Diretiva (UE) n. 2016/680:

> É crucial assegurar um nível elevado e coerente de proteção dos dados pessoais das pessoas singulares e facilitar o intercâmbio de dados pessoais entre as autoridades competentes dos Estados-Membros, a fim de assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial. Para tal, o nível de proteção dos direitos e liberdades individuais no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais – incluindo a salvaguarda e a prevenção de ameaças à segurança pública – deverá ser equivalente em todos os Estados-Membros. A proteção eficaz dos dados pessoais na União exige não só que sejam reforçados os direitos dos titulares dos dados e as obrigações de quem trata dados pessoais, mas também que haja reforço dos poderes

> equivalentes para controlar e assegurar a conformidade com as regras de proteção dos dados pessoais nos Estados-Membros.
>
> Para efeitos de prevenção, investigação ou repressão de infrações penais, é necessário que as autoridades competentes tratem os dados pessoais, recolhidos no contexto da prevenção, investigação, detecção ou repressão de infrações penais específicas para além desse contexto, a fim de obter uma melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detectadas.

Ao longo de todo o texto, estabelecem-se critérios diferenciados para o tratamento de dados com fins de prevenção, investigação, detecção ou repressão a infrações penais. Nesse sentido, espera-se que, assim como na Europa, a legislação específica brasileira, prevista no art. 4º da Lei n. 13.709/2018, leve em consideração as peculiaridades do tratamento de dados para fins de investigação.

Em um cenário de constante evolução tecnológica, o tempo, por exemplo, é fator fundamental para o sucesso das investigações. Percebe-se, nesse contexto, que a natureza acelerada das mudanças torna cada vez mais difícil se avançar sem cooperação entre órgãos de investigação e demais da administração pública responsáveis por realizar o tratamento de dados para finalidades diversas.

7. CONCLUSÃO

No compartilhamento de dados pessoais entre órgãos públicos de variadas finalidades com órgãos e autoridades que atuam na investigação, há fundamentos suficientes a justificar a adoção dessas medidas excepcionais, ante as evidências de autoria e/ou participação dos investigados nos mais diversos crimes em apuração. Prevalece, nesse caso, o interesse público na efetiva persecução penal dos fatos em questão.

Do estudo realizado, conclui-se que, não exorbitados os limites traçados pela Constituição ao versar a disponibilização e o compartilhamento dos dados pessoais, os órgãos de investigação poderão ter acesso a dados pessoais de bases mantidas por outros públicos, independentemente do consentimento e da ciência do titular.

Da mesma forma, uma vez que os órgãos de persecução penal observem a proporcionalidade nos critérios a embasar a intervenção estatal na coleta, no compartilhamento e no uso dos dados pessoais, se houver mudança de finalidade ou repasse de dados a terceiros, não haveria necessidade de se obter um novo consentimento do titular. Uma vez em posse dessa base de dados, não seria crível supor que o titular poderia, quando for de seu desejo, revogar a autorização ou pedir acesso, exclusão, portabilidade, complementação ou correção das informações.

Tal entendimento, considerado todo o exposto, não violaria o sigilo, tampouco invadiria a privacidade, uma vez que a troca de informações entre órgãos de investigação e demais órgãos públicos se mostra extremamente necessária ao equilíbrio de forças – ou desequilíbrio em prol da justiça – no combate ao crime, sobretudo em uma época em que este se dissemina de forma rápida e organizada.

Nesse sentido, em linha com o direito internacional, os dados pessoais obtidos pelas autoridades brasileiras competentes em situações de investigação criminal não podem ser tratados para outros fins. Se assim o for, a não ser que esse tratamento seja autorizado por norma específica ou decisão judicial, será aplicável a LGPD em sua integralidade.

Entende-se que a lei específica prevista no art. 4º, III, da LGPD deve levar em conta a realidade dos órgãos de investigação, o interesse público e o esforço despendido pelo Estado para investigar e processar o suposto autor de uma infração. Caso a nova lei traga restrições exageradas, é possível que isso dificulte, sobremaneira, a persecução criminal que engloba tanto a fase pré-processual quanto a da ação penal. Por

exemplo, atender aos requisitos do art. 18, II e III, da LGPD[2] para que o suspeito de um crime possa acessar seus dados, mesmo que para fins de correção de informações incompletas, inexatas ou desatualizadas, não nos parece razoável em uma fase preliminar de investigação.

Assim, havendo evidências de delito, com circunstâncias pendentes de elucidação, mostra-se imprescindível, para o prosseguimento das investigações e, até mesmo, para o esclarecimento dos fatos, que os órgãos e as autoridades responsáveis pela persecução penal tenham acesso a dados relevantes, que, muitas vezes, originalmente não estão sob controle de outros órgãos públicos.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. *Comentários à Lei de Organização Criminosa*: Lei 12.850/2013. São Paulo: Saraiva, 2014.

BRASIL. Constituição (1988). *Constituição da República Federativa do Brasil*: promulgada em 5 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 5 out. 2020.

BRASIL. Decreto n. 10.046, de 9 de outubro de 2019. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central

2 "Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I – confirmação da existência de tratamento; II – acesso aos dados; III – correção de dados incompletos, inexatos ou desatualizados; IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;"

de Governança de Dados. *Diário Oficial da União*, Brasília, DF, seção 198º, 9 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D10046.htm. Acesso em: 5 mar. 2020.

BRASIL. Lei n. 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei n. 9.034, de 3 de maio de 1995; e dá outras providências. *Diário Oficial da União*, Brasília, DF, 2 ago. 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 8 maio 2020.

BRASIL. Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*, Brasília, DF, seção 197º, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 8 set. 2019.

BRASIL. Resolução n. 2/2020 do Ministério da Economia. Diretrizes para categorização de compartilhamento de dados. *Diário Oficial da União*, Brasília, DF, seção 1, 20 mar. 2020. Disponível em: http://www.in.gov.br/en/web/dou/-/resolucao-n-2-de-16-de-marco-de-2020-249025238. Acesso em: 16 maio 2020.

DIRETIVA (UE) 2016/680 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. *Jornal Oficial da União Europeia*. Dispo-

nível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=PT. Acesso em: 18 set. 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

FERRAZ JR., T. S. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito*, Universidade de São Paulo, n. 88, p. 439-459. Disponível em: http://www.revistas.usp.br/rfdusp/article/view/67231. Acesso em: 5 out. 2020.

KHALED JR., Salah H. *A busca da verdade no processo penal*: para além da ambição inquisitorial. São Paulo: Atlas, 2013.

LOPES JR., Aury; GLOECKNER, Ricardo Jacobsen. *Investigação preliminar no processo penal*. 6. ed. rev., atual. e ampl. São Paulo: Saraiva, 2014.

MENDRONI, Marcelo Batlouni. *Curso de investigação criminal*. 3. ed. rev. e amp. São Paulo: Atlas, 2013.

RANGEL, Paulo. *Investigação criminal direta pelo Ministério Público*: visão crítica. 5. ed. rev. e atual. São Paulo: Atlas, 2016.

SANTIN, Valter Foleto. *A investigação criminal e o acesso à justiça*. 2001. Disponível em: https://www.apmp.com.br/. Acesso em: 25 maio 2020.

WARREN, S.; BRANDEIS, L. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220. doi:10.2307/1321160. Disponível em: https://www.jstor.org/stable/1321160?seq=1#metadata_info_tab_contents. Acesso em: 9 maio 2020.

QUEBRA DE SIGILO EM MASSA E PROTEÇÃO DE DADOS DE TERCEIROS: COMO MINIMIZAR O IMPACTO DA MEDIDA SEM PREJUDICAR A AMPLA DEFESA

Maria Thereza Rocha de Assis Moura[1]
Daniel Marchionatti[2]

RESUMO

A quebra de sigilo de dados em massa obtém dados de pessoas não envolvidas no evento criminoso. Após a identificação do suspeito, apenas uma fração dessas informações será de interesse imediato à persecução penal. Este artigo discute a possibilidade de proteger os dados de terceiros, deixando de dá-los ao conhecimento dos sujeitos do processo. Considera a necessidade de compatibilizar-se o interesse da defesa em explorar o conteúdo da base de dados com a proteção à privacidade dos terceiros. Conclui que devem ser automaticamente incorporados aos autos a cadeia de custódia da prova digital, os dados

1 Ministra do Superior Tribunal de Justiça. Corregedora Nacional de Justiça. Mestre e doutora em Direito Processual Penal pela Faculdade de Direito da USP. Professora doutora de Direito Processual Penal da USP.

2 Juiz federal. Doutorando pela USP. Mestre pela UFRGS. Professor do IDP.

dos imputados e os anonimizados. Ademais, para proteger os dados pessoais de terceiros, o acesso à base só deve ser assegurado aos sujeitos processuais mediante autorização judicial específica. Além disso, a base de dados deve ser eliminada o mais breve possível.

Palavras-chave: Quebra de sigilo em massa. Dados pessoais. Anonimização.

ABSTRACT

Mass surveillance obtains personal data from a set of people. After identifying a suspect, only a fraction of this information will be of immediate interest to the prosecution. This article discusses the protection of bystanders. The need to reconcile the defense's interest in exploring the content of the database with the protection of the privacy of third parties is taken into account. We conclude that the chain of custody, the personal data of the accused and the anonymized data should be automatically incorporated into the case file. On the other hand, in order to protect the personal data of third parties, access to the database should only be guaranteed to counselors after a specific judicial order. In addition, the database should be deleted as soon as possible.

Keywords: Mass surveillance. Personal data. Anonimization.

1. INTRODUÇÃO

No processo penal, a privacidade é um direito fundamental muito caro à defesa. Serve como barreira à "entrada" de informações no processo, ao impedir medidas investigativas invasivas desproporcionais e a exposição de informações, ao limitar o acesso de terceiros a dados sigilosos.

No entanto, vez por outra, esse direito entra em conflito com interesses defensivos. Neste artigo, discutiremos especificamente a limitação de acesso dos sujeitos do processo, em particular a defesa, a elementos de prova – dados pessoais – resultantes da quebra de sigilo, por dizerem respeito a terceiros.

Um caso ocorrido recentemente no Brasil ilustra a dificuldade de viabilizar uma persecução penal que, simultaneamente, proteja dados pessoais e assegure à defesa o acesso às mesmas informações de que a acusação faz uso. Em 26 de agosto de 2020, o Superior Tribunal de Justiça (STJ) confirmou três decisões judiciais que determinavam a provedor de aplicações de internet o fornecimento de dados pessoais em massa, no interesse de investigação de crime grave.

Os primeiros dois recursos analisados pelo Tribunal tratavam da requisição de informações sobre usuários que transitaram por perímetros especificados em determinado momento[3], técnica de investigação conhecida como *reverse location search* – busca por localização reversa[4]. Tal busca consiste em requisitar a provedor os dados de todos os usuários que realizaram conexão ou acesso em determinado lugar e hora. Conhecendo-se o local e o momento em que ocorrido o crime, identificam-se aqueles que estavam na região para, por eliminação, chegar-se ao perpetrador.

Um terceiro recurso julgado pela Corte tratava da requisição de informações sobre usuários que pesquisaram certas palavras em ferramenta de busca[5]. O objetivo era identificar todos que tivessem procurado

---

3 RMS n. 61.302 (2019/0199132-0) e RMS n. 62.143 (2019/0318252-3), rel. min. Rogério Schietti, Terceira Seção, julgado em 26-8-2020.

4 Analisamos essa e outras técnicas de investigação em Moura e Marchionatti (2020, p. 477-502).

5 RMS n. 60.698 (2019/0119654-6), rel. min. Rogério Schietti Cruz, Terceira Seção, julgado em 26-8-2020.

informações sobre a vítima ou sobre o modo de perpetração do delito. Por eliminação, tentava-se chegar ao perpetrador.

A inevitável invasão à privacidade de pessoas completamente alheias ao delito anima severas críticas a essas medidas investigativas[6]. Este artigo, entretanto, não pretende acirrar o debate acerca da admissibilidade da quebra de sigilo de dados em massa. Seu propósito é discutir um conflito de direitos autônomo, que decorre da quebra de sigilo de dados em massa, mas com ela não se confunde.

O sucesso da investigação ocorre quando, a partir da análise do conjunto de dados obtido, consegue-se identificar o provável autor do crime, contra o qual a persecução penal será direcionada. Como assegurar a ampla defesa daquele que vier a ser acusado e, ao mesmo tempo, proteger os dados pessoais dos titulares inocentes obtidos com a diligência?

Esse dilema é sério e importante. A defesa tem o direito de receber as informações que levaram ao estabelecimento da imputação, para poder contestar a tese acusatória. No entanto, a persecução penal tem o dever de proteger dados privados, em especial quando relativos a terceiros.

Essas questões serão debatidas neste artigo.

2. DEVER DE PROTEÇÃO AOS DADOS PESSOAIS

Informações pessoais adquiridas pela investigação e pelo processo penal devem ser protegidas. Trata-se de uma decorrência do direito à proteção à intimidade e à privacidade.

O direito à privacidade ou à vida privada está contemplado em várias declarações de direito, como o art. 17, 1, do Pacto Internacional

6 Ver Estellita e Gleizer (2018).

sobre Direitos Civis e Políticos; o art. 11, 2, do Pacto de São José da Costa Rica; o art. 8º da Convenção Europeia de Direitos Humanos; e o art. XXII da Declaração Islâmica Universal dos Direitos Humanos.

No Brasil, o texto constitucional traçou uma distinção de difícil entendimento, ao consagrar a inviolabilidade da intimidade e da vida privada (art. 5º, X). De acordo com Ferraz Júnior (1993, p. 441-442), há um "diferente grau de exclusividade" entre intimidade e privacidade. A primeira seria "o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada que, por mais isolada que seja, é sempre um viver entre os outros (na família, no trabalho, no lazer em comum)". O autor dá os seguintes exemplos: "o diário íntimo, o segredo sob juramento, as próprias convicções, as situações indevassáveis de pudor pessoal, o segredo íntimo cuja mínima publicidade constrange". Por sua vez, a segunda envolveria "a proteção de formas exclusivas de convivência", ou seja, situações em que há comunicação entre sujeitos, da qual estão excluídos terceiros. Portanto, de acordo com essa definição, a intimidade diz respeito a informações que não são comunicadas, ao passo que a privacidade se refere à comunicação restrita de informações.

Dados íntimos ou privados armazenados são invioláveis por força da própria Constituição. A proteção é aplicável independentemente do local em que estejam guardados. Mesmo após incorporados a uma investigação, eles seguem protegidos. Trata-se de decorrência do princípio da proporcionalidade, pois as limitações ao direito à vida privada devem ocorrer apenas no quanto adequado e necessário à persecução penal[7].

O juízo de proporcionalidade não se limita apenas à extensão da quebra de sigilo de dados, atinge também o uso dos dados captados

7 Para uma análise da solução de conflitos entre direitos fundamentais, ver Alexy (2008).

pela persecução penal, em todos os seus momentos. Assim, qualquer tratamento dos dados obtidos pela investigação ou persecução penal deve ser limitado ao indispensável a seus propósitos.

Algumas das consequências da limitação ao indispensável são bem conhecidas dos estudiosos e operadores do processo penal. A principal é a manutenção do segredo externo das informações sigilosas incorporadas ao processo. Dar as informações ao conhecimento de terceiros não é adequado ao interesse da persecução penal, o qual resta satisfeito pelo acesso da prova apenas aos sujeitos do processo. Daí por que, em uma restrição à regra da publicidade dos autos (art. 189 do CPC), apenas o Ministério Público, a defesa, o juízo e seus auxiliares têm acesso às informações sigilosas obtidas pelo processo. Com isso, dados bancários, fiscais e outros pessoais seguem protegidos. Trata-se da aplicação da vinculação à finalidade (*Zweckbindung*), um dos aspectos da autodeterminação informativa (*informationelle Selbstbestimmung*)[8]. Como assevera Shafers (2018), "por meio da vinculação à finalidade, assegura-se que os dados só serão tratados para a finalidade para a qual foram coletados".

Aqui, pretendemos discutir um passo além. Tendo em vista que a adoção do segredo externo permite que a defesa, o Ministério Público e o juízo tenham acesso ilimitado aos dados de terceiros obtidos pela quebra de sigilo, surge a indagação: Em que medida é possível que os próprios sujeitos do processo tenham limitado o acesso a dados pessoais de terceiros?

8 Esse aspecto da autodeterminação informativa ganhou notoriedade a partir da decisão do Tribunal Constitucional Alemão no Caso do Censo (*Volkszählungsurteil* – 1 BvR 209/83, de 15-2-1983).

3. SEGREDO EXTERNO E SUA INSUFICIÊNCIA PARA A PROTEÇÃO DE DADOS DE TERCEIROS

O resultado da quebra de sigilo em massa é um conjunto de informações contendo dados pessoais de todas as pessoas que estavam na situação objeto da requisição. Chamaremos esse conjunto de informações de "base de dados". No exemplo mencionado na introdução deste artigo, essa base será composta pelos dados pessoais de todos os usuários que acessaram o serviço em determinado local e hora e de todos que pesquisaram determinadas palavras.

Analisando a base de dados, os investigadores passam a realizar o cruzamento de informações, montando e testando hipóteses, com o intuito de direcionar a suspeita a pessoa determinada. Concretizada a suspeita, a persecução se volta para um sujeito, e os dados a ele relativos tornam-se de grande relevância para a acusação. O restante da base de dados, no entanto, não revelará informações de interesse para a tese acusatória.

A questão que propomos está em como gerir essas informações, garantindo-se o máximo de acesso aos sujeitos processuais – em especial à defesa –, mas também assegurando ao máximo a vida privada dos terceiros.

A solução tradicional do direito processual brasileiro para a proteção de dados pessoais é o segredo externo. Este, contudo, não é suficiente quando se trata de salvaguardar dados de terceiros.

O segredo externo consiste em limitar o acesso dos documentos sigilosos às partes e aos interessados legalmente habilitados. Ao receber dados bancários requisitados, incumbe ao Poder Judiciário preservar "o seu caráter sigiloso mediante acesso restrito às partes, que delas não poderão servir-se para fins estranhos à lide" (art. 3º da Lei Complementar n. 105/2001). O magistrado que requisita registros de conexão ou de acesso a aplicações de internet deve "tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça" (art. 23 do Marco Civil da Internet).

Essas normas, entretanto, não tratam da questão central que aqui nos preocupa, uma vez que o segredo externo é desenhado para proteger o próprio acusado ou, eventualmente, a vítima ou outros envolvidos no delito, da divulgação de dados pessoais. O foco de nossa atenção está na proteção a dados de terceiros, que não apresentam qualquer relação com o fato criminoso, mas que tiveram o sigilo de suas informações pessoais atingido em razão da quebra de sigilo em massa.

A quebra de sigilo de dados em massa, alcançando terceiros não envolvidos, é medida excepcionalíssima, que exige cautelas igualmente excepcionais, não apenas para sua decretação, mas também no tratamento dos dados obtidos. Essa situação recomenda um cuidado extremo no tratamento dos dados pessoais, inclusive com o impedimento de acesso a todos os que não estejam envolvidos em sua análise. Mas como fazer?

Alguns ordenamentos jurídicos adotam por padrão a limitação de acesso às informações sigilosas obtidas pela investigação, incorporando ao processo apenas aqueles elementos cujo valor probatório é percebido pelos investigadores. Com isso, restringem a invasão da privacidade representada pela quebra de sigilo apenas ao adequado às necessidades da persecução penal. Os interesses da defesa são, ao menos em tese, protegidos pelo dever dos agentes públicos de incorporar aos autos não apenas informações incriminatórias mas também dados favoráveis à defesa.

No direito francês, são incorporadas aos autos do processo somente as informações tidas por relevantes, permanecendo a base de dados lacrada (*sous scellés fermés*). As informações obtidas mediante quebra de sigilo ou de outras técnicas especiais de investigação são analisadas pelo investigador. Este, "agindo sob sua responsabilidade, descreve ou transcreve" os dados "úteis à manifestação da verdade" no processo[9].

9 Arts. 100-5 (interceptação de comunicações eletrônicas), 230-38 (geolocalização), 706-95-18 (técnicas especiais de investigação) do *Code de Procédure Pénale*.

A proteção à privacidade de terceiros é cuidada mediante a vedação de transcrição de dados não interessantes ao processo – "nenhum trecho relativo à vida privada estranha às infrações pode ser conservado no caderno da ação"[10]. A base de dados é destruída ao final do prazo prescricional para a persecução penal[11].

O direito alemão adota a mesma lógica. O resultado do uso de técnicas especiais de investigação é apreciado pelos investigadores. Elementos de interesse são incorporados aos autos. Outras informações são destruídas sem demora[12].

Em ambos os casos, a legislação expressamente assinala aos magistrados que conduzem as investigações o dever de produzir provas de encargo e desencargo. Ou seja, a investigação oficial também tem o compromisso de produzir provas de interesse da defesa[13].

No direito brasileiro, a tradição é completamente diferente. Impedir os sujeitos do processo de acessar os elementos probatórios não é algo corriqueiro em nosso processo penal. As normas brasileiras sobre organização da informação dentro do processo determinam simplesmente sua justaposição sequencial. Nesse sentido, o art. 9º do CPP prevê que "todas as peças do inquérito policial serão, num só processado, reunidas". Da mesma forma, o Código de Processo Civil (CPC) prevê a encadernação de todos os atos e elementos em autos, com todas as folhas numeradas e rubricadas (art. 207 do CPC). Existem algumas previsões

---

10 Art. 706-95-18 do *Code de Procédure Pénale*.

11 Arts. 100-6 (interceptação de comunicações), 230-43 (geolocalização), 706-91-19.

12 Parágrafos 81 (análise de DNA em massa), 98a e 98b (investigação por perfil), 100e (interceptação de telecomunicações, busca e apreensão de dados e captação ambiental), 100g (captação de dados de conexão), (técnicas ocultas de investigação) 100i (investigação de terminais móveis) e 100d (medidas que afetam o núcleo essencial da privacidade) do StPO.

13 Arts. 39-3 e 81 do *Code de Procédure Pénale*; § 160, (2), do StPO.

de autuação em separado para a manutenção do segredo externo de algumas peças, mas inexiste norma que permita sonegar aos sujeitos do processo[14] elemento de prova já incorporado aos autos.

Quanto à defesa, o acesso amplo do imputado aos elementos de prova coligidos em seu desfavor é um pilar do processo penal. Discorrer sobre a importância disso seria supérfluo. Mencionado no enunciado n. 14 da Súmula Vinculante[15], no Estatuto da Ordem dos Advogados do Brasil (art. 7º, XIV, da Lei n. 8.906/1994), na Lei das Organizações Criminosas (art. 7º, § 2º, da Lei n. 12.850/2013) e no Código de Processo Penal (art. 3º-B, XV, e art. 3º-C, § 4º), o amplo acesso da defesa aos elementos de prova já documentados em procedimento investigatório é um marco do processo penal brasileiro.

Entre nós, mesmo o resultado de meios de obtenção de prova invasivos, como a interceptação telefônica, é integralmente compartilhado com todos os suspeitos (art. 8º da Lei n. 9.296/1996). Os imputados têm acesso inclusive ao registro de comunicações que não estão sendo usadas como prova e das quais não tomaram parte. O incidente de inutilização das gravações sem interesse para a persecução penal (art. 9º da Lei n. 9.296/1996) depende de iniciativa das partes e só ocorre depois do acesso das defesas ao material[16].

A jurisprudência afirma um duplo requisito para assegurar o acesso aos elementos de prova. O primeiro, positivo: o elemento "deve apontar

---

14 A previsão legal mais próxima no direito brasileiro é da impossibilidade de traslado do inquérito para o juiz de julgamento, na forma do art. 3º-C, § 3º, do CPP, introduzido pela Lei n. 13.594/2019. Os propósitos, no entanto, são completamente diversos.

15 "É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa."

16 Uma vez que todas as defesas copiaram as gravações, a destruição do banco de dados judicial passa a ter pouco ou nenhum efeito para a defesa da privacidade. São raros os requerimentos de inutilização.

a responsabilidade criminal" daquele que pede acesso. O segundo, negativo: ele "não deve referir-se à diligência em andamento". Com base nessa compreensão, é possível, em tese, limitar o acesso da defesa a elementos que não apontam a responsabilidade criminal do imputado[17].

Cumpre destacar, no entanto, que, na quebra de sigilo de dados em massa, o elemento de prova produzido é também do interesse da defesa, porque uma fração desses dados leva à condição de suspeito.

Embora o segredo externo seja medida adequada e importante à proteção da vida privada daqueles que tenham interesse no processo, sua eficácia é limitada. Dentro do círculo de participantes do processo, não há segredos – todos têm acesso a todas as provas. Por exemplo, numa ação penal instruída pela interceptação de conversas telefônicas de um dos réus, os demais acusados poderão acessar esse material, ainda que não tenham tomado parte nas conversas.

Dessa forma, o segredo externo é insuficiente para cuidar da proteção de dados de terceiros. Ainda que estes sejam, em princípio (e apenas em princípio), irrelevantes para o processo, todos estiveram acessíveis para as partes. Depois que a acusação teve a oportunidade de extrair aquilo que entendeu importante, não servem ao juízo, pois não precisará deles para formar sua convicção, nem à defesa, para a qual o acesso a dados sobre os quais não têm conhecimento ou domínio traria qualquer benefício. Sua juntada aos autos desde logo, ainda que sob segredo externo,

17 É até aqui dominante a jurisprudência no sentido de impedir o acesso de acusados delatados a atos de colaboração produzidos pelo delator que não digam respeito ao delito em questão. O *leading case* para essa negativa é o Inq n. 3.983, rel. min. Teori Zavascki, STF, Pleno, julgado em 3-3-2016. O STJ vem adotando entendimento semelhante, ainda que a questão não esteja integralmente pacificada: REsp AgRg n. 1.587.239, rel. min. Maria Thereza de Assis Moura, Sexta Turma, julgado em 14-8-2018; RHC n. 67.493, rel. min. Felix Fischer, Quinta Turma, julgado em 19-4-2016.

seria medida que invadiria a privacidade dos titulares dos dados além do adequado aos interesses da persecução penal.

A despeito dessa irrelevância *prima facie*, é possível que discussões se instaurem em torno do acesso à base de dados. E, muito provavelmente, será da defesa o legítimo interesse de acesso, para montar suas próprias apurações, ou para demonstrar inconsistência na tese acusatória. Nesse caso, passa a existir conflito entre a privacidade de terceiros e o interesse da defesa.

Para proteger o direito à vida privada dos terceiros, mesmo contra os sujeitos do processo, é preciso construir, pela via interpretativa, mecanismos de salvaguarda à privacidade, os quais devem ser diferentes das ferramentas conhecidas pelo direito brasileiro até o momento. Não há uma normatização imediata dessa questão, e o segredo externo revela-se insuficiente.

O principal mecanismo de salvaguarda parece ser a segregação da base de dados, fora dos autos do processo. O acesso dos sujeitos processuais à base de dados deve ser fundado em um posterior juízo de proporcionalidade, diverso daquele que amparou a quebra de sigilo de dados. A decisão de quebrar o sigilo opõe os interesses da persecução penal à vida privada dos potenciais atingidos. Nessa segunda decisão, a privacidade dos titulares dos dados atingidos é ponderada contra os interesses da defesa. Trata-se de uma segunda quebra de sigilo, ainda que em ambiente mais controlado.

A melhor forma de encaminhar a solução do problema parece ser a incorporação direta aos autos apenas de informações sem maior potencial de atingir a privacidade de terceiros. Assim, alguns resultados da quebra de sigilo de dados devem ser incorporados diretamente ao processo criminal. Muitas informações são de evidente interesse probatório e atingem pouco ou nada a privacidade de outros que não integram a ação.

No entanto, as informações que envolvem de forma importante a privacidade de terceiros, para que sejam dadas a conhecer, devem de-

pender de uma nova autorização judicial. A base de dados recebida, ou mesmo frações dela que não digam respeito aos imputados, só devem ser dadas a conhecer mediante um novo juízo de adequação, necessidade e proporcionalidade.

Para avaliação da extensão em que o acesso aos dados deve ser garantido, é possível separar as informações em quatro conjuntos: (i) cadeia de custódia; (ii) informações pessoais dos acusados; (iii) informações anonimizadas; e (iv) informações pessoais de terceiros. Os três primeiros podem ser incorporados diretamente ao processo. O quarto deve depender de autorização judicial específica.

4. DADOS RESULTANTES DA QUEBRA DE SIGILO EM MASSA INCORPORADOS DIRETAMENTE AO PROCESSO

Alguns dados serão de valor probatório claro e não representarão um custo adicional a terceiros se incorporados diretamente aos autos do processo. Os resultados da quebra de sigilo em massa que indiquem a contribuição dos imputados para os fatos ou que revelem o número de pessoas na mesma situação não afetam a privacidade de terceiros e devem, desde logo, aportar aos autos, ficando acessíveis para todos os sujeitos processuais. Estão nessa situação (i) a cadeia de custódia; (ii) as informações pessoais dos acusados; e (iii) as informações anonimizadas.

4.1 CADEIA DE CUSTÓDIA

O direito dos sujeitos do processo ao acesso à cadeia de custódia da prova é indubitável. A quebra de sigilo em massa envolve coleta, receptação, análise e armazenamento de informações. Não é impossível que essas informações sejam fornecidas em suporte analógico – em

papel, por exemplo –, o mais comum, no entanto, é que sua obtenção ocorra em meio digital.

A cadeia de custódia dos elementos obtidos deve ser documentada, especialmente se o forem de forma digital. Muito embora o Código de Processo Penal não faça menção à cadeia de custódia de provas imateriais, parece indubitável a conveniência de assegurar a mesmidade de qualquer elemento de prova, inclusive os digitais (BADARÓ, 2017, p. 522).

Dado o contexto, acusação, defesa e juízo têm interesse em tomar contato com a documentação da cadeia de custódia, como forma de conferir a integridade do elemento.

Neste ponto, não parece haver sequer espaço para controvérsia.

4.2 INFORMAÇÕES RELATIVAS AOS IMPUTADOS

O direito ao acesso a informações relativas aos imputados tampouco merece discussão, dado que elas estabelecem ou reforçam a suspeita ou a justa causa para a ação penal. Nos casos de quebra de sigilo em massa, costumam ser os elementos que levam ao direcionamento de uma investigação a pessoas determinadas.

Retomando o exemplo concreto mencionado na introdução, a acusação terá interesse em colacionar aos autos os dados que demonstram que o celular do imputado transitou pela região determinada ou que consultou as palavras dadas no mecanismo de pesquisa.

De seu lado, a defesa terá interesse em conhecer dos detalhes desses dados, para poder a eles se contrapor. No exemplo, uma pequena diferença no horário ou na trajetória pode ser decisiva para a demonstração de que o imputado não perpetrou o delito.

Esses elementos são incorporados aos autos e devem passar pela devida valoração.

4.3 DADOS ANONIMIZADOS

As partes também têm potencial interesse em fazer constar dos autos dados anonimizados, que reflitam a prevalência da ocorrência na população ou outros detalhes potencialmente reveladores.

O meio para dar conhecimento das informações, sem identificar os titulares, é a juntada aos autos do dado anonimizado, que é definido como o "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art. 5º, III, da Lei Geral de Proteção de Dados Pessoais – LGPD). Ainda de acordo com o inciso XI do mesmo artigo, a anonimização "é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

Dados anonimizados podem ser juntados ao processo sem representar uma vulneração adicional à privacidade. Eles não são em regra sequer considerados dados pessoais, na forma do art. 12 da LGPD.

O conhecimento de quantas pessoas estavam na mesma situação é fundamental para avaliar a relevância do indício. A ocorrência terá muito mais impacto demonstrativo se for incomum. No exemplo mencionado na introdução, se o aparelho do acusado fosse o único conectado próximo ao local do crime em determinado momento, a suspeita será muito mais forte do que se houvesse centenas de outros aparelhos na mesma situação. A mesma lógica é aplicável ao mecanismo de pesquisa. Se a pesquisa ao termo é recorrente, a relevância do indício fica enfraquecida.

Além da quantidade de pessoas na mesma situação, outros detalhes podem ser elucidativos. Por exemplo, se o imputado apontar que um aparelho, que não o seu, consultou a palavra no mecanismo de pesquisa e estava no local do crime, poderá fazer surgir dúvida sobre a própria responsabilidade.

A anonimização consistirá na supressão das informações que possam

ligar o dado ao usuário. A extensão dessa supressão pode ser objeto de controvérsia. No exemplo, a supressão da localização geográfica completa dos usuários que fizeram a pesquisa por determinados termos é um fator importante para a anonimização. No entanto, a preservação de uma informação geográfica mais geral pode ser útil ao processo. Poder-se-ia pensar em suprimir as coordenadas geográficas, mantendo-se a informação da unidade política em que ela foi executada, com maior ou menor precisão – bairro, município, estado etc.

As controvérsias sobre a extensão da supressão podem ser levadas ao juízo, que deverá realizar o devido arbitramento do conflito.

O procedimento de anonimização (art. 5º, XI, da LGPD) deve ser devidamente documentado e dado a conhecer nos autos. De posse dos dados anonimizados, a parte terá a oportunidade de checar o total de incidência da ocorrência, além de aferir quaisquer outros pontos que entenda relevantes.

Com isso, fica preservada a privacidade dos terceiros, mas garantido o acesso da informação relevante à defesa.

5. BASE DE DADOS

A base de dados contém informações de terceiros e, portanto, não deve ser confiada aos sujeitos do processo, sem a demonstração de justa causa para tanto.

A acusação tem a oportunidade de extrair as informações que entender relevantes para instruir a persecução penal. Portanto, a questão sobre a limitação de acesso ao membro do Ministério Público que oficia durante a persecução penal não parece levantar maiores problemas.

Para a defesa, no entanto, essa limitação é bastante problemática. Como afirmado, o amplo acesso da defesa aos elementos de prova é um dos pilares do processo penal. Sua limitação precisa ser proporcional,

para satisfazer um fim específico – tutela da vida privada de terceiros –, com o mínimo sacrifício ao interesse defensivo.

Para compatibilizar esses dois pontos, o acesso da defesa à base de dados não deve ser automático. Ao contrário dos demais dados que são juntados a investigações e processos criminais, pensamos que esse acesso deve ser autorizado judicialmente. Assim, a base de dados deve ser mantida segregada dos autos, até ordem judicial em contrário.

A fim de obter acesso à base de dados, a defesa precisa apontar a relevância que o resultado pode ter em seu favor, ou demonstrar a seriedade do propósito de instaurar sua própria apuração, em cima dos dados pessoais dos terceiros. A autorização para isso deve levar em conta a relevância potencial do exame. Um acusado que confessa o delito não teria, em princípio, interesse em perscrutar a base de dados para enfraquecer a suspeita que sobre si paira.

Ao apreciar o requerimento, o magistrado deve levar em conta o quão sensíveis as informações são e o quão relevantes elas podem ser para a demonstração daquilo a que a defesa se propõe. Deve, além do mais, levar em conta que a defesa precisará da informação para construir suas apurações. Logo, o juízo não pode exigir uma demonstração exauriente de que a prova servirá ao propósito exoneratório. Eventuais dúvidas pendem em favor do requerente.

É impossível prever com precisão as necessidades da defesa em todos os casos. Não se descarta a possibilidade de o magistrado adotar cautelas, minimizando o impacto do acesso a informações. Assim, é possível cogitar, eventualmente e em tese, do acesso em condições controladas, voltadas a evitar a divulgação do conteúdo das informações.

Portanto, o acesso da defesa à base de informações de pessoas não envolvidas no delito não deve ser automático. A proteção aos dados pessoais de terceiros exige que a autorização de acesso à defesa seja avaliada pelo juiz, que deverá assegurar o exercício da ampla defesa, mas adotar as cautelas necessárias para minimizar o impacto da violação de privacidade.

6. ELIMINAÇÃO, ARMAZENAMENTO E ARQUIVAMENTO DA BASE DE DADOS

A eliminação das informações de terceiros que não dizem respeito ao processo, resultantes da quebra de sigilo em massa, deve ocorrer o mais cedo possível. O caminho natural da prova produzida mediante quebra de sigilo em massa é que a acusação extraia as informações que indicam a responsabilidade do imputado e perca o interesse no restante da base de dados.

A partir de então, deve ser adotada uma política de limitação de tratamento dos dados que compõem a base. Essa é a medida recomendada pelo art. 16º, 3, *b*, da Diretiva n. 2016/680 do Parlamento Europeu e do Conselho,

> relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

Nesse caso, a limitação de tratamento significa que a base de dados deve ser armazenada com segurança, de forma a impedir qualquer outro tratamento[18] não autorizado. Se possível, o armazenamento deve ocorrer em dispositivo sem acesso à rede e protegido por lacre físico e criptografia.

Essas cautelas são fundamentais, mas não esgotam a preocupação. Trata-se de dados pessoais que estão sob o controle do Estado. Essa

18 O art. 5º, X, da LGPD define tratamento como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

situação é excepcional e deve cessar o quanto antes, com o descarte dos dados, para assim restabelecer a confiança na inviolabilidade da vida privada (art. 5º, X, da CF).

Portanto, a questão do acesso da defesa aos dados deve ser resolvida o quanto antes. A tendência natural da gestão de provas no Brasil é a guarda indefinida do vestígio. Porém, o arquivamento da base de dados em arquivos judiciais, policiais ou de custódia, indefinidamente, gera insegurança e restringe desnecessariamente o direito à privacidade.

A legislação brasileira não prevê um incidente para decisão sobre o interesse defensivo no acesso aos dados. A solução, a nosso ver, é construir, com as ferramentas processuais que se possui, uma solução que contemple os interesses da defesa e da privacidade de terceiros.

Na falta de previsão específica, o último momento para a defesa manifestar o interesse no acesso à base de dados deve ser o momento da resposta à acusação (arts. 396-A e 406, § 3º, do CPP). Essa é a oportunidade para a defesa especificar as provas que pretende produzir.

Na ausência de requerimento de acesso à base de dados na resposta à acusação, deve-se determinar sua eliminação. Requerido o acesso, cabe ao magistrado deliberar o quanto antes. A depender da complexidade, o requerimento pode demandar uma instrução específica.

Sendo a decisão pela eliminação, sua execução deve ocorrer apenas após a preclusão. A reconstrução da base de dados pode ser difícil ou impossível. Assim, por cautela, é importante manter o armazenamento na pendência dos recursos.

Caso a decisão sobre o acesso à prova ocorra de forma interlocutória, surge o problema da via impugnatória. Numa primeira análise, cremos que o recurso cabível será a apelação contra a posterior sentença. O CPP não prevê claramente um recurso imediato. Qualquer construção por aproximação seria insatisfatória. Pode-se argumentar em prol da apelação imediata, por ser uma decisão com força de definitiva, na medida em que ordenada a eliminação da base de dados (art. 593, II,

do CPP). No entanto, estar-se-á no início da instrução e, em última análise, o que se tem é o indeferimento de prova. Pode-se defender o cabimento do recurso em sentido estrito, mas não há previsão no rol do art. 581 do CPP. Dado o contexto, a impugnação imediata parece ser cabível apenas pela via do *habeas corpus*.

Dessa forma, o requerimento deve ocorrer na primeira oportunidade possível, o mais tardar por ocasião da resposta à acusação, e a decisão também deve ocorrer o tão pronto quanto viável, realizando-se a instrução necessária à apreciação do requerimento. A eliminação da base de dados deve aguardar a preclusão.

7. CONCLUSÃO

A quebra de sigilo de dados em massa é medida excepcionalíssima e, como tal, deve ater-se ao indispensável à instrução da causa penal.

O acesso à defesa da base de dados pessoais de terceiros nem sempre é necessária e, portanto, não deve ser automática. Muito embora o acesso da defesa a todos os elementos de prova esteja no alicerce do processo penal, essa limitação precisa ser observada, tendo em vista a vulneração da vida privada de terceiros não envolvidos no delito.

Para garantir a ampla defesa, é importante que sejam automaticamente incorporados aos autos a cadeia de custódia da prova digital, os dados pessoais dos imputados e os dados anonimizados.

Para proteger os dados pessoais de terceiros, o acesso à base de dados apenas será assegurado à defesa mediante autorização judicial específica. A defesa precisa demonstrar a relevância potencial dessas informações a sua estratégia. No entanto, o juízo não pode exigir daquela uma demonstração exauriente de que a prova servirá ao propósito exoneratório. Eventuais dúvidas pendem em favor do requerente.

O requerimento de acesso à base de dados terá de ser resolvido o quanto antes. A legislação brasileira não prevê um incidente próprio para tanto. Na falta de uma previsão específica, o último momento para a defesa manifestar o interesse no acesso à base de dados será o da resposta à acusação (arts. 396-A e 406, § 3º, do CPP).

Requerido o acesso, caberá ao magistrado deliberar o quanto antes. A depender da complexidade, o requerimento poderá demandar uma instrução específica.

Na falta de requerimento de acesso, ou preclusa a decisão que o indefere, deve-se proceder à eliminação dos dados, independentemente do trânsito em julgado da ação penal.

Com essas cautelas, maximiza-se a proteção à inviolabilidade da vida privada, já tão combalida com a admissão da quebra de sigilo de dados em massa.

REFERÊNCIAS

ALEXY, Robert. *Teoria dos direitos fundamentais*. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

BADARÓ, Gustavo. A cadeia de custódia e sua relevância para a prova penal. *In*: SIDI, Ricardo; LOPES, Anderson Bezerra (Orgs). *Temas atuais da investigação preliminar no processo penal*. Belo Horizonte: D'Plácido, 2017. p. 522.

ESTELLITA, Heloísa; GLEIZER, Orlandino. A investigação penal de insuspeitos: STJ fere direitos ao exigir coleta massiva de dados. *Folha de S.Paulo*, São Paulo, 20 jun. 2018. Disponível em: https://www1.folha.uol.com.br/opiniao/2020/09/a-investigacao-penal-de-insuspeitos.shtml. Acesso em: 7 out. 2020.

FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito*, Universidade de São Paulo, v. 88, 1993, p. 441-442.

MOURA, Maria Thereza de Assis; MARCHIONATTI, Daniel. Dados digitais: interceptação, busca e apreensão e requisição. *In*: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos (Orgs.). *Direito, processo e tecnologia*. 1. ed. São Paulo: RT, 2020. v. 1, p. 477-502.

SHAFERS, Tim Philipp, Die Datenschutz-Grundverordnung (DSGBO). *Eine Neue Zeitrechnung im Bereich des Datenschutzes*, FREILAW: FREIBURG L. Students J. 16, 2018.

UTILIZAÇÃO DE DADOS DE APLICATIVOS DE *CONTACT TRACING* EM INVESTIGAÇÃO CRIMINAL À LUZ DA LGPD

Thiago Augusto Bueno[1]

RESUMO

Cuida-se de trabalho no qual se analisa, à luz da Lei Geral de Proteção de Dados (Lei n. 13.709/2018), a possibilidade de compartilhamento e utilização em investigações criminais de dados coletados, originariamente, em aplicações de *contact tracing*, desenvolvidas com vistas ao enfrentamento da pandemia de covid-19. Para tanto, a partir do estudo dos conceitos jurídicos de privacidade, consentimento e finalidade, foi feita uma análise do objetivo dos aplicativos que se utilizam da tecnologia de *contact tracing*, de modo a se perquirir acerca da viabilidade da transferência dos dados dessas aplicações para fins de investigação criminal. Durante o estudo, utilizou-se de comparação com o sistema

1 Procurador da República em Manaus. Pós-graduado no curso de especialização em Direito Público com em ênfase em Direito Constitucional pela Universidade Potiguar e no curso de especialização em Direito Aplicado ao Ministério Público Federal pela Escola Superior do Ministério Público Federal. Mestre em Direito pela Universidade Católica de Brasília. Pós-graduando em Direito Digital pelo ITS/UERJ.

comunitário europeu, inspirador da legislação brasileira de proteção de dados, em especial do guia elaborado pelo Parlamento Europeu que, especificamente, trata da matéria. Além disso, no plano interior, o aplicativo "Coronavírus SUS", desenvolvido pelo Ministério da Saúde em parceria com a *Apple* e o *Google*, foi objeto de estudo.

Palavras-chave: Pandemia. *Contact tracing*. Investigação criminal.

ABSTRACT

This paper analyses the possibility of sharing the data collected by contact tracing apps that were designed in the context of the pandemic of covid-19, with criminal investigation, according to the Brazilian Law of Data Protection (Lei nº 13.709/2018). It was developed by studying the law concepts of privacy, consent and the purposes of data processing, particularly the aim of these apps, in order to clarify if it is possible to use this data in criminal investigations. Throughout the writing process, the European Union system was the comparison base because the General Data Protection Regulation inspired the Brazilian Data Protection Law. Thus, the "Guidance on Apps supporting the fight against Covid 19 pandemic in relation to data protection", released by European Commission was studied. Besides that, the app "Coronavírus SUS" offered by the Brazilian Health Ministry and produced by Apple and Google was analyzed.

Keywords: Pandemic. Contact tracing. Criminal investigation.

1. INTRODUÇÃO

A pandemia de covid-19 mudou em muito, de forma abrupta, o modo como nos relacionamos socialmente. Apesar de a taxa de mortalidade

decorrente da nova doença ser menor do que outras síndromes respiratórias também transmitidas por vírus, como a *sars* e o *mers*, o número absoluto de vítimas fatais de covid-19 é maior em decorrência do alto índice de transmissibilidade (MAHASE, 2020).

A constatação científica de que o novo coronavírus se espalha a partir do contato próximo entre as pessoas e de que muitos infectados são assintomáticos, o que propicia maior transmissão, criou um cenário no qual, ausente a vacina, as autoridades sanitárias têm de se valer de medidas não farmacológicas para o enfrentamento da pandemia (AQUINO, 2020). Entre as principais estratégias empregadas para o combate está o isolamento social, a testagem da população, a quarentena dos diagnosticados com a nova doença e o controle de comunicantes (SILVA, 2020). Essa última objetiva identificar pessoas que tenham tido contato com o vírus e que, de algum modo, possam ser vetores de transmissão da doença mesmo sem desenvolverem sintomas.

Essa modalidade de enfrentamento de doenças epidêmicas não é nova, constando inclusive do *Guia de vigilância epidemiológica do Ministério da Saúde* editado em 2009 (BRASIL, 2009). Normalmente o controle é realizado manualmente, a partir da identificação e pesquisa dos diagnosticados. Em uma das etapas, é realizada entrevista com os portadores do vírus com o objetivo de identificar todos aqueles que tiveram contato próximo com o infectado durante o período de transmissão da doença. Pretende-se, com isso, evitar a disseminação do agente transmissor da moléstia.

Diante dessa demanda, a evolução tecnológica permitiu a elaboração de um novo instrumento de controle dos comunicantes, a versão eletrônica do procedimento, conhecida pelo nome inglês *contact tracing*, expressão livremente traduzida para o português como "rastreamento de contatos". Trata-se de medida não farmacológica empregada no enfrentamento da pandemia de covid-19 que busca fornecer um mapa da disseminação do coronavírus a partir da utilização de aplicativos que

funcionam em *smartphones*. As aplicações de *contact tracing* pretendem identificar pessoas que tiveram algum tipo de contato com alguém diagnosticado com a doença no período de contágio do vírus, de modo que possam ser adotadas medidas de testagem e quarentena, com o objetivo de interromper o processo de transmissão da doença.

Dada a novidade da tecnologia e a sensibilidade das informações envolvidas, já que se referem à saúde das pessoas, muitas são as questões surgidas a partir da adoção dessas ferramentas de controle epidemiológico, especialmente quanto à coleta, ao tratamento e ao uso dos dados. Nesse contexto, discute-se acerca da possibilidade do uso dos dados coletados nessas aplicações para fins de investigação criminal, propondo-se a tanto o presente estudo. Antes, porém, faz-se necessário entender como funcionam as aplicações de *contact tracing*.

2. FUNCIONAMENTO DAS APLICAÇÕES DE *CONTACT TRACING*

A partir de um *smartphone*, utilizado como representação do usuário, o aplicativo de *contact tracing* mensura a distância e o tempo de contato mantido com outro aparelho celular que tenha o mesmo sistema instalado (ADA LOVELACE INSTITUTE, 2020). A proximidade permite a troca de registros entre os dispositivos móveis, normalmente por meio da tecnologia *bluetooth*. Assim, os dados são coletados e tratados a partir de parâmetros estabelecidos por algoritmo, e, caso um dos envolvidos seja diagnosticado como portador do novo coronavírus, são identificadas as interações com potencialidade para disseminar a doença.

Exemplificando, se dois indivíduos "A" e "B" instalam o aplicativo em seus *smartphones* e, em determinado momento, ambos se encontram e mantêm contato a uma distância menor que dois metros, por quinze minutos, a interação é registrada nos dois aparelhos. Três dias após o evento, "A" é diagnosticado com covid-19 e reporta essa informação

à aplicação. Com esse registro, o aplicativo, a partir da definição do algoritmo, rastreia contatos ocorridos nos últimos catorze dias, a menos de três metros de distância, por mais de cinco minutos. Dessa forma, é apurado o registro do encontro entre "A" e "B", o qual se encaixa nos parâmetros definidos. Em seguida, o usuário "B" recebe uma mensagem em seu *smartphone* noticiando a ocorrência de um potencial contato com alguém que tenha sido diagnosticado com covid-19 e orientando-o a fazer um teste para aferição da doença e a se colocar em quarentena enquanto não for divulgado o resultado do seu exame.

Dessa forma, a efetividade da medida depende da colaboração ativa dos usuários em dois momentos distintos. Primeiramente eles terão de baixar, instalar e permitir o funcionamento contínuo do aplicativo. Depois terão de informar, prontamente, eventual diagnóstico positivo para o vírus.

O tratamento dos dados colhidos por esse método traz uma série de implicações que repercutem diretamente nos dados pessoais sensíveis dos respectivos titulares. Além dos registros referentes à saúde, são objeto de coleta e análise informações que dizem respeito à localização e às interações sociais dos usuários, com dados precisos de onde, por quanto tempo e a que distância uma pessoa esteve com outra. Tal procedimento requer, portanto, especial atenção de modo a se evitar a prática de atos ilícitos, já que, a depender de como sejam tratados, os dados podem ser utilizados para comportamento discriminatório e perseguição de minorias étnicas ou de movimentos sociais, o que fere de morte os direitos inerentes à personalidade.

Entendido o funcionamento das aplicações de *contact tracing*, é preciso fazer breves apontamentos sobre os conceitos de privacidade, consentimento e finalidade, à luz da Lei Geral de Proteção de Dados (LGPD).

3. PRIVACIDADE, CONSENTIMENTO E FINALIDADE

Quanto à privacidade, faz-se necessário apontar a evolução do conceito. Antes visto como o direito de ser deixado só (*right to be left alone*), tal como trazido por Warren e Brandeis no século XIX (TEFFÉ; TEPEDINO, 2020), atualmente a privacidade é tratada como o direito de ter conhecimento acerca do fluxo informacional de si próprio, sobre o conteúdo das informações coletadas, registradas e tratadas, de modo que seja assegurado ao titular dos dados o acesso e o manejo de medidas de proteção, retificação e exclusão (CARNEIRO; MAGRANI; SOUZA, 2020). Em uma abordagem mais sintética e pragmática, o conceito de privacidade na atual sociedade da informação, afetada pelo capitalismo de vigilância[2], implica a apuração da extensão dos dados coletados e a forma de tratamento e registro adotados por agentes de organizações privadas ou do Estado.

Conforme lição de Pasquale (2015), os dados pessoais têm sido coletados e tratados pelo Estado e pelas grandes corporações atuantes no meio digital para a formação do que ele chamou de *one-way mirror* (espelho de sentido único, em tradução livre), de modo que esses organismos possam ter conhecimento sobre quase tudo a respeito do titular dos dados, enquanto este, em contrapartida, não conhece a extensão das informações que lhe são extraídas, em clara situação de desigualdade.

Nesse contexto, especialmente os grandes atores privados do mundo digital, a partir do oferecimento de serviços, em tese, gratuitos, coletam

2 Zuboff (2018) define capitalismo de vigilância (*surveilance captialism*), entre outros sentidos, como sendo a ordem econômica que se vale de experiências humanas como fonte para atividades comerciais escondidas de extração, predição e venda de produtos e serviços. Como apontado por Frazão (2020), o capitalismo de vigilância se utiliza de experiências humanas como matéria-prima para a produção de dados comportamentais.

toda sorte de dados pessoais que, devidamente tratados, formam um verdadeiro espectro digital do titular. Assim, o usuário dos serviços digitais, a partir da adoção das mais diversas ferramentas de vigilância tecnológica, tais como os *cookies*[3], tem seu comportamento monitorado o tempo todo, de modo que lhe são extraídos dados comportamentais que, tratados pelos grandes atores do meio digital, são aplicados para a personalização de mensagens publicitárias (BIONI, 2020).

A coleta maciça de dados pessoais aliada ao tratamento com emprego de ferramentas de *big data*, a partir da utilização de algoritmos cujos mecanismos de funcionamento não são transparentes, levou Cathy O'Neil a se referir aos algoritmos como armas matemáticas de destruição[4], em razão dos resultados nefastos que podem decorrer do uso, aparentemente legítimo e objetivo, dessas tecnologias, tais como reforço de preconceitos em desfavor de minorias étnicas (O'NEIL, 2016).

Nesse sentido, o recém-lançado documentário *O dilema das redes* pôs em debate as consequências de grandes corporações usarem redes sociais para avolumarem seu poder econômico mediante a coleta desmensurada de dados e seu tratamento, com o emprego de ferramentas de *big data*, tais como algoritmos que funcionam de forma enviesada e não transparente, para fins nem sempre tão legítimos e muitas vezes desconhecidos dos seus titulares, com implicações de gigantesca magnitude no arranjo social e democrático atual.

---

3 *Cookies* são aplicações desenvolvidas para funcionamento nos navegadores de internet (tais como *Google Chrome*, *Internet Explorer*, *Mozila* e Brave) que têm por finalidade a coleta de dados referentes às preferências dos usuários quando estão em ambiente da internet. Sua utilização permite que a navegação pelas páginas da *web* seja mais rápida. No entanto, oferecem informações sobre os hábitos comportamentais do usuário na rede.

4 *Weapons of math destruction*, em alusão à expressão em língua inglesa que se refere às armas de destruição em massa – *weapons of mass destruction*.

No plano jurídico interno, a LGPD, inspirada no *General Data Protection Regulation* (GDPR), do sistema comunitário europeu, pressupõe que todo dado pessoal tem relevância e valor e que o consentimento é o elemento principal e o fundamento para a autodeterminação informativa do indivíduo, de modo que ele possa ter efetivo controle das informações acerca da sua pessoa (FRAJHOF; MANGETH, 2020). Nos termos de seu art. 5º, XII, o consentimento deve ser livre, informado e inequívoco, além de se voltar a uma finalidade determinada. Esses são os quatro requisitos para a garantia da validade do consentimento.

Quanto ao primeiro deles, entende-se por livre o consentimento tomado sem os vícios previstos no Código Civil, tal como determina o art. 8º, § 3º, da LGPD[5], em clara situação de determinação de diálogo das fontes (BIONI, 2020). Sendo assim, não são admitidas intervenções que maculem a expressão da vontade do titular dos dados (TEPEDINO; TEFFÉ, 2020).

Por sua vez, o acesso à informação é requisito determinante para permitir que o titular tenha aptidão para dispor de seus dados. Segundo Bioni (2020), a informação se sustenta em dois elementos, (1) ser perceptível e (2) ser útil. Logo, o cidadão precisa ter a consciência de que está sendo informado, de modo que o ato de informar não pode ser implícito, o que demonstra a relevância da forma pela qual se transmite a informação. Além disso, esta precisa ser útil no sentido de acrescer conhecimento ao titular, de modo a lhe conferir ganho informacional que lhe permita validamente decidir pela outorga do consentimento. Essas informações precisam ser adequadas e claras, em atenção aos princípios da transparência e boa-fé objetiva (FRAJHOF; MANGETH,

5 "Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. (...) § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento."

2020), de modo a reduzir a assimetria técnica e informacional entre as partes (TEPEDINO; TEFFÉ, 2020).

De sua parte, inequívoca é a característica que determina ter sido o consentimento tomado de forma clara, sem interpretações ambíguas, não se exigindo que decorra de uma ação afirmativa da qual não se tenha dúvida da intenção do titular, já que pode ser extraída implicitamente. No entanto, exige uma conduta positiva do seu titular, não sendo admitida sua extração a partir de posturas omissivas do cidadão (FRAJHOF; MANGETH, 2020).

O último elemento relacionado ao consentimento na LGPD é a finalidade específica, ponto determinante para se aferir a legitimidade do tratamento de dados. O art. 6º, I, do aludido diploma define o conteúdo do princípio da finalidade como sendo a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Dessa forma, há uma obrigação legal de correlação entre o tratamento dos dados e a finalidade informada (OLIVEIRA; LOPES, 2020), em razão da vinculação do consentimento outorgado a um objetivo específico, previamente conhecido, previsto e aceito pelo titular. Como decorrência, é vedado o uso de dados para fins genéricos (FRAJHOF; MANGETH, 2020).

Assentadas as interações entre privacidade, consentimento e finalidade, passemos a analisar as características dos dados pessoais sensíveis, categoria objeto de tratamento das aplicações de *contact tracing*.

4. DADOS SENSÍVEIS

Os dados pessoais objeto das aplicações de *contact tracing* são classificados como sensíveis pelo ordenamento jurídico pátrio, já que se ligam a informações referentes à saúde do seu titular, conforme dispõe o art. 5º, II, da LGPD:

> Art. 5º Para os fins desta Lei, considera-se:
>
> (...)
>
> II – **dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, *dado referente à saúde* ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (Grifo nosso)

Em razão dessa disciplina específica, o tratamento dos dados se ampara no art. 11 e não no art. 7º da LGPD, como ocorre com os pessoais ordinários. Desse modo, a base legal para seu tratamento é diversa, adstrita às hipóteses taxativas trazidas no referido excerto normativo.

A elaboração da LGPD teve nítida inspiração no sistema normativo da União Europeia, no qual o GDPR, ao dispor acerca da disciplina do tratamento de dados pessoais sensíveis (*sensitive personal data*), em seu o art. 9º, item 1, trouxe previsões mais rigorosas se comparadas aos de natureza ordinária. Nesse sentido, os dados referentes à saúde são considerados sensíveis, de modo que seu tratamento, via de regra, é proibido, sendo admitido somente nas hipóteses do item 2 do mesmo artigo:

> 1. O processamento de dados pessoais que revelem dados de raça, origem étnica, opiniões políticas, crenças religiosas ou filosóficas ou sindicais e o processamento de dados genéticos e biométricos para o propósito de unicamente identificar uma pessoa natural, *dados referentes à saúde* ou à vida sexual ou orientação sexual pessoal são proibidos.[6] (Tradução livre – grifo nosso)

---

6 "*1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person,* ***data concerning health*** *or data concerning a natural person's sex life or sexual orientation shall be prohibited*." (Grifo nosso)

Essa distinção aplicável aos dados sensíveis se dá por dois motivos principais: em razão de revelarem atributos ainda mais profundos da privacidade, veiculando informações da intimidade de seus titulares, e em razão da potencial discriminação decorrente da sua utilização (COTS; OLIVEIRA, 2019), sendo que essa disciplina específica se aplica a dados sensíveis tratados por entidade pública ou privada (MULHOLLAND, 2020). A potencialidade de discriminação em decorrência do acesso a dados pessoais sensíveis é o traço distinto do tratamento aplicável pela LGPD, já que seu uso pode ser abusivo, implicando tratamento não igualitário ao titular. O tratamento legislativo diferenciado conferido aos dados pessoais sensíveis se legitima, assim, para afastar possibilidades de ameaças à liberdade e autonomia dos indivíduos (TEFFÉ, 2020).

Como exemplo de revelação de dados pessoais sensíveis que resultou em tratamento discriminatório, podemos citar a veiculação na mídia e na internet, por autoridades sul-coreanas, de informações colhidas por meio de aplicações de *contact tracing*, a indicarem idade, sexo e lugares visitados por pessoas diagnosticadas com covid-19 (CHA; SMITH, 2020). A partir da divulgação desses dados, alguns indivíduos se tornaram vítimas de *fake news* envolvendo prolação de falsos casos de adultério e até mesmo inexistentes participações em seitas ocultas (SANG-HUN, 2020). Situações como essas demonstram quão discriminatória pode ser a divulgação de dados sensíveis.

A redação do art. 11, I, da LGPD denota que o consentimento, como base legal para o tratamento de dados pessoais sensíveis, exige requisitos mais severos quando comparado aos dados pessoais não sensíveis. Com efeito, o dispositivo permite o tratamento de dados sensíveis "*quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas*".

De plano, destaca-se que o excerto legal supraindicado exige que o consentimento seja mais qualificado. Não bastasse ser livre, informado, inequívoco e para finalidade determinada (art. 5º, XII, da LGPD), é

necessário que tenha sido manifestado de *forma específica e destacada*, de modo que o aspecto da forma da manifestação ganha destaque (KONDER, 2020), sendo imprescindível que haja algum tipo de visibilidade na manifestação de aquiescência do titular dos dados. Além disso, Mulholland (2020, n.p.) aponta que a especificidade deve ser entendida como delimitação do objeto ou da finalidade do tratamento:

> Por exemplo, deve-se especificar que a coleta por uma seguradora de saúde de dados sobre doenças preexistentes só estará legitimada se restrita a estas informações – doenças preexistentes –, estando excluídas de tratamento todas as demais informações sobre a situação de saúde do contratante. Em outras palavras, o tratamento de dados fica restrito àqueles que se referem a doenças preexistentes, devendo o consentimento, de forma expressa e específica, indicar esse objetivo.

Como decorrência da especificidade do consentimento no caso dos dados sensíveis, tem-se que o emprego de fórmulas genéricas para coleta, tratamento e uso de dados sensíveis é ilícito, uma vez que impede a verificação da vinculação da atividade exercida pelo controlador ou operador de dados.

Ademais, especificamente quanto a dados sensíveis que se refiram a serviços de saúde, o art. 11, § 4º, da LGPD[7] traz restrições a seu

7 "§ 4º É vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º deste artigo, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir: I – a portabilidade de dados quando solicitada pelo titular; ou II – as transações financeiras e administrativas resultantes do uso e da prestação dos serviços de que trata este parágrafo."

uso para fins de exploração econômica, em uma demonstração de que carecem de maior grau de proteção, dada a repercussão na esfera da personalidade de seu titular.

5. *CONTACT TRACING* NO SISTEMA COMUNITÁRIO EUROPEU

Como se percebe, o arcabouço normativo e principiológico da LGPD traz toda uma carga de proteção aos dados pessoais como expressão de direito da personalidade. Esse arranjo foi desenvolvido de modo a permitir que o cidadão tenha o conhecimento prévio e necessário para decidir pela anuência dos processos de coleta, tratamento e uso de seus dados por serviços oferecidos por instituições privadas e pelo Poder Público. As aplicações de *contact tracing*, além de trabalharem com dados referentes a aspectos da saúde de seu titular, acessam outros relativos a contatos, interações sociais, rotinas e lugares frequentados, de modo que o tratamento dessas informações merece especial tutela do Estado.

Considerando que a legislação pátria foi inspirada no sistema comunitário europeu, é interessante verificar as soluções encontradas pela União Europeia quanto ao uso das aplicações de *contact tracing*. Nesse sentido, a Comissão Europeia elaborou um guia voltado à matéria de proteção de dados – *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*, no qual são elencados elementos a serem privilegiados tendo-se em vista o enaltecimento da confiança dessas aplicações. Pretende-se, com isso, ampliar o uso desses sistemas pela população, de modo que eles se tornem ferramentas efetivas para o enfrentamento da pandemia.

Um dos pontos destacados no documento é a necessidade de indicação do embasamento legal para o processamento dos dados (*legal basis for processing*), de modo que sejam observadas as normas legais referentes ao consentimento para acesso dos dados e seu respectivo tratamento. Desse

modo, o GDPR ressalta que o consentimento deve ser livre, específico, explícito e informado (*freely given, specific, explicit and informed*). Além disso, deve ser expresso por meio de uma ação afirmativa, excluindo-se, assim, comportamentos omissivos, o que vai ao encontro do consentimento qualificado por finalidade específica e destacada, previsto na LGPD, relativamente aos dados pessoais sensíveis (art. 11, I).

Ainda, ante a natureza dos dados pessoais coletados e as circunstâncias da pandemia, o documento indica que os Estados devem (1) descrever em detalhes o processamento dos dados e especificar os propósitos para os quais serão utilizados; (2) identificar claramente quem será o controlador dos dados e quem mais terá acesso a eles; (3) excluir a possibilidade de processamento para outros propósitos que não os previstos na legislação; (4) prever medidas específicas que assegurem instrumentos de garantia em favor dos titulares[8].

O guia volta suas atenções à coleta mínima dos dados necessários às aplicações, de modo a garantir a privacidade dos titulares. No Brasil, tal medida encontra guarida no princípio da necessidade, previsto no art. 6º, III, da LGPD[9], cuja aplicação busca determinar a restrição na coleta e

---

8 "*Given the nature of the personal data concerned (in particular health data as special categories of personal data) as well as the circumstances of the current COVID-19 pandemic, relying on the law as the legal basis would contribute to legal certainty, since it would (i) prescribe in detail the processing of specific health data and clearly specify the purposes for the processing; (ii) spell out clearly who is the controller, i.e. the entity processing the data, and who, beside the controller, can have access to such data; (iii) exclude the possibility to process such data for different purposes than those listed in the legislation and (iv) provide for specific safeguards. In order not to undermine the public usefulness and acceptance of the apps the national legislator should pay particular attention that the solution chosen is as inclusive vis-a-vis citizens as possible*."

9 "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) III – necessidade: limitação do tratamento ao mínimo

no tratamento dos dados ao estritamente necessário para a consecução do fim ao qual aquiesceu o titular (LOPES; OLIVEIRA, 2020).

Veja-se que há clara preocupação quanto à transparência, vinculação e necessidade da coleta, do tratamento e do uso dos dados, para que os cidadãos sejam informados e estejam seguros de que suas informações serão utilizadas estritamente para o controle de comunicantes no âmbito da pandemia. Esse propósito se justifica na medida em que o que se busca é criar um ambiente propício à difusão do uso dessas aplicações, de modo que ocorra o efetivo rastreamento da transmissão do vírus. Assim, a Comissão Europeia percebeu que a larga adoção dos aplicativos de *contact tracing* passa, indispensavelmente, pelo estabelecimento de uma relação de confiança entre os usuários e a autoridade estatal controladora dos dados.

Vale lembrar que o documento da Comissão Europeia não traz qualquer orientação no sentido da vedação do compartilhamento dos dados coletados em aplicações de *contact tracing* para uso em investigações criminais, cabendo essa disciplina a cada um dos Estados-membros.

6. *CONTACT TRACING* NO BRASIL

Para fins deste estudo, será analisado o aplicativo "Coronavírus SUS" do Ministério da Saúde. Funcionando como aplicação de *contact tracing* desde 31 de julho de 2020, foi desenvolvido a partir de uma parceria com o *Google* e a *Apple*. De acordo com as Políticas de Privacidade e Termo de Consentimento para Tratamento de Dados, o sistema está em

---

necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados."

conformidade com a LGPD, sendo o Ministério da Saúde o controlador dos dados. Interessante notar, no entanto, que no documento consta que o usuário consente que a controladora (Ministério da Saúde):

> tome decisões referentes ao tratamento de seus dados pessoais, notoriamente sem identificações pessoais, sendo tratados apenas por chave vinculada ao aparelho celular e sua mobilidade, sem, contudo, ter acesso a dados pessoais de propriedade, *razão pela qual tais informações não são tratadas como sensíveis para o âmbito da Lei Geral de Proteção de Dados Pessoais*. (Grifo nosso)

Nesse ponto cabe destacar que, conforme analisado, os dados coletados, tratados e utilizados pelas aplicações de *contact tracing* têm natureza sensível, já que são diretamente ligados a informações inerentes à saúde do titular, de modo que a utilização de mecanismo tecnológico de não identificação pessoal do proprietário do dispositivo móvel não desnatura essa característica dos dados. Inclusive a própria LGPD traz disciplina acerca daqueles que tenham passado por procedimento de ocultação da identidade de seus titulares, definindo em seu art. 5º, III, como *dado anonimizado o relativo a titular que não possa ser identificado, considerando-se a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento*. No caso dos dados anonimizados, não há aplicação da LGPD, tal como previsto expressamente no seu art. 12[10], já que eles não têm valor algum, ficando fora do âmbito de proteção legal. Como trazido por Mulholland (2020, n.p.):

---

10 "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. § 1º A determinação do que seja razoável deve

> Essa exclusão de tutela se deve ao fato de que a proteção de dados pessoais está justificada como forma de abrigar a privacidade, a identidade e a liberdade dos titulares de dados. Em não sendo possível realizar-se a identificação desse titular, a tutela dos dados não se mostra necessária, haja vista que o próprio objetivo da Lei deixa de estar legitimado.

No entanto, deve ser ressaltado que, havendo a possibilidade de reversão do processo de anonimização, o próprio art. 12 da LGPD ressalva o retorno da incidência da aplicação da Lei, uma vez que ressurgem as repercussões dos dados com os objetos jurídicos privacidade, identidade e liberdade de seus titulares.

A questão discutida neste trabalho resta prejudicada caso não haja reversão da anonimização dos dados coletados no aplicativo de *contact tracing*, uma vez que não será possível identificar os titulares e, a partir daí, suas interações sociais e movimentações espaciais, informações de grande relevância para investigações criminais. Dessa forma, restaria afastada a aplicação da LGPD por absoluta ausência de valor dos dados que justifiquem sua proteção.

No entanto, uma vez exitosa a reversão do processo de anonimização e, por conseguinte, sendo possível identificar os cidadãos que utilizaram o aplicativo de *contact tracing*, há clara incidência da LGPD para proteção dos dados objeto de tratamento. Nessa situação, é importante ressaltar a

---

levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. § 3º A autoridade nacional poderá dispor sobre padrões e técnicas utilizados em processos de anonimização e realizar verificações acerca de sua segurança, ouvido o Conselho Nacional de Proteção de Dados Pessoais."

natureza sensível desses dados, por conta das consequências decorrentes da finalidade do consentimento outorgado pelo titular, à luz da LGPD.

Ocorre que uma das bases legais de tratamento de dados previsto no art. 7º da LGPD é o legítimo interesse do controlador, previsto no inciso IX,[11] o qual, na prática, permite que o tratamento seja feito com um objetivo diferente daquele com o qual consentiu seu titular. Há uma autorização legal para a alteração da finalidade do uso dos dados pelo controlador, legitimando-se seu emprego em finalidade diversa daquela abarcada pelo consentimento originariamente conferido pelo cidadão, de modo a amparar interesse legítimo do controlador dos dados.

Acontece que tal previsão é exclusiva para dados pessoais não sensíveis. Quanto aos sensíveis, o art. 11 da LGPD, que traz o rol das hipóteses de embasamento legal para o tratamento, não elenca circunstância que o autorize sem o consentimento do titular para tutela do legítimo interesse do controlador. As disposições das alíneas *e, f* e *g* do inciso II do art. 11 da LGPD[12] se referem a circunstâncias nas quais há o legítimo

---

11 "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: (...) IX – quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;"

12 "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: (...) e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais."

interesse do titular, e não do controlador, o que legitima o tratamento sem a necessidade de outorga de consentimento pelo cidadão. São situações que se referem à tutela da vida, incolumidade física, saúde e segurança do próprio titular, não tendo sido trazida qualquer previsão que abarque o legítimo interesse de terceiro.

Dessa forma, não se mostra cabível que o controlador do aplicativo "Coronavírus SUS", o Ministério da Saúde, se fundamente em alegação de seu legítimo interesse, ou de terceiro, para alteração da finalidade do uso dos dados da referida aplicação, uma vez que se trata de dados sensíveis e não há amparo legal em tal pretensão.

No caso das aplicações de *data tracing*, a finalidade é a identificação e o rastreamento de potenciais situações de transmissão do vírus. No caso do aplicativo "Coronavírus SUS", constam como finalidades, de forma destacada, com fonte em tamanho maior e em negrito, em cumprimento à determinação do art. 11, I, da LGPD, nos Termos de Uso:

> Possibilitar que a Controladora identifique e entre em contato com o Titular para fins de relacionamento podendo informar que esteve em contato com o usuário que descobriu estar infectado.
>
> Possibilitar que a Controladora contate com usuários que estiveram em contato com o titular do dado, em face de descoberta que o mesmo identificou estar infectado com o coronavírus.

Assim, pelo princípio da finalidade, o uso dos dados coletados pelo referido aplicativo deve limitar-se ao propósito de identificação de usuários que possam ter sido contaminados em decorrência de interações pessoais potencialmente transmissoras da doença. Via de consequência, todo e qualquer uso dos dados com outro propósito será ilícito.

Quanto ao compartilhamento de dados, o aplicativo "Coronavírus SUS" informa que:

> não realizará compartilhamento dos dados com nenhuma outra instituição, quer pública ou privada, acerca das chaves identificadoras dos equipamentos móveis cujo autorizado o tratamento de dado do Titular, em estrita obediência à política de prevenção a vida e a saúde, observados os princípios e as garantias estabelecidas na Lei nº 13.709.

Diante disso, em prestígio ao consentimento manifestado pelos usuários, bem como em razão do princípio da finalidade e da natureza sensível dos dados, não será possível o compartilhamento dos dados coletados pelo aplicativo "Coronavírus SUS" para utilização em investigações criminais.

Por fim, pondera-se que, por expressa disposição do art. 4º, III, *d*, da LGPD[13], o aludido diploma legislativo não abarca questões atinentes ao tratamento de dados para investigação e repressão de infrações criminais. Nesse particular, deverá ser editada uma versão criminal da LGPD a disciplinar especificamente esse procedimento, conforme previsto no art. 4º, § 1º, da Lei[14]. O mesmo excerto normativo prevê, no entanto, desde já, a aplicação dos princípios gerais de proteção de dados, bem como os direitos de titular à matéria, de modo que os princípios da finalidade, adequação, necessidade, transparência e não discriminação são aplicáveis ao tratamento de dados que envolvam investigação criminal (MENEZES; COLAÇO, 2020).

---

13 "Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: (...) III – realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais;"

14 "Art. 4º (...) § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei."

7. CONCLUSÃO

A pandemia gerada pelo novo coronavírus trouxe um cenário de mobilização das instituições públicas e privadas em escala global para a tutela da saúde nunca visto. A velocidade do alastramento da doença e o número de vítimas exigiram profundas mudanças nos meios de organização social que acabaram por trazer implicações na privacidade dos cidadãos.

Os aplicativos de *contact tracing* são uma poderosa ferramenta tecnológica para controle de comunicantes, e a difusão de seu uso pode contribuir decisivamente para o enfrentamento do coronavírus. No entanto, é preciso refletir sobre a possível exposição da privacidade dos usuários mediante divulgação dos dados colhidos por esse tipo de tecnologia, já que, além de informações relativas à saúde, revelam interações sociais e deslocamentos geográficos.

A partir do uso de ferramentas de *big data*, como análise por algoritmos, é possível desenvolver um verdadeiro espectro digital do cidadão. Em razão disso, exige-se dos desenvolvedores dessas aplicações e dos controladores e operadores dos dados coletados e objeto de tratamento a observância estrita dos princípios que norteiam a legislação de proteção de dados pessoais, especialmente do consentimento, da finalidade e da necessidade.

A falta de legislação nacional acerca da proteção de dados relacionados à investigação criminal não pode dar azo à instalação de uma verdadeira sociedade de vigilância em matéria de segurança pública, com o desmensurado acesso a dados e informações pessoais dos cidadãos.

Particularmente, no que se refere ao aplicativo "Coronavírus SUS", não parece acertado eventual compartilhamento dos dados para fins de investigação criminal. Um dos motivos para esse posicionamento seria o registro apresentado nos Termos de Serviço do aplicativo, no qual o assunto não é tratado, uma vez que a finalidade à qual aquiesceu

o usuário não pode ser alterada unilateralmente pelo controlador sob fundamento de tutela de seu legítimo interesse, por falta de amparo legal. Além disso, nos Termos de Uso, há previsão expressa de que os dados não serão compartilhados com nenhuma outra entidade, seja pública ou privada.

REFERÊNCIAS

AQUINO, Estela M. L. *et al*. Medidas de distanciamento social no controle da pandemia de COVID-19: potenciais impactos e desafios no Brasil. *Ciência & Saúde Coletiva*, Rio de Janeiro, v. 25, supl. 1, p. 2423-2446, jun. 2020. Disponível em: http://dx.doi.org/10.1590/1413-81232020256.1.10502020. Acesso em: 7 set. 2020.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. *Lei n. 13.709/2018.* Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 7 set. 2020.

BRASIL. Ministério da Saúde. Secretaria de Vigilância em Saúde. Departamento de Vigilância Epidemiológica. *Guia de vigilância epidemiológica*. 7. ed. Brasília: Ministério da Saúde, 2009. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/guia_vigilancia_epidemiologica_7ed.pdf. Acesso em: 7 set. 2020.

CARNEIRO, Giovana; MAGRANI, Eduardo; SOUZA, Carlos Affonso. *Lei Geral de Proteção de Dados*: uma transformação na tutela dos dados pessoais. A LGPD e o novo marco normativo no Brasil. Caitlin Mulholland, 2020. Versão eletrônica.

CHA, Sangmi; SMITH, Josh. South Korea promises more privacy as it tracks contacts of new coronavirus cases. *Global News*, 14 maio 2020. Disponível em: https://globalnews.ca/news/6942244/south-korea-coronavirus-tracing-routes/. Acesso em: 7 set. 2020.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada*. 3. ed. rev., atual. e ampl., São Paulo: Thomson Reuters, 2019.

FRAJHOF, Isabella Z; MANGETH, Ana Lara. *As bases legais para o tratamento de dados pessoais*. A LGPD e o novo marco normativo no Brasil. Caitlin Mulholland, 2020. Versão eletrônica.

FRAZÃO, Ana. *Fundamentos da proteção dos dados pessoais – Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados*. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

KONDER, Carlos Nelson. *O tratamento de dados sensíveis à luz da Lei 13.709/2018*. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

LOPES, Isabela Maria Pereira; OLIVEIRA, Marco Aurélio Bellizze. *Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018*. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Revista dos Tribunais, 2020.

MAHASE, Elisabeth. *Coronavirus*: covid-19 has killed more people than SARS and MERS combined, despite lower case fatality rate. https://pubmed.ncbi.nlm.nih.gov/32071063/. Acesso em: 7 set. 2020.

MULHOLLAND, Catlin. *O tratamento de dados pessoais sensíveis*. A LGPD e o novo marco normativo no Brasil. Caitlin Mulholland, 2020. Versão eletrônica.

O DILEMA das redes. Direção de Jeff Orlowski. Estados Unidos. 2020.

O'NEIL, Cathy. *Weapons of math destruction*: how big data increases inequality and threatens democracy. Nova Iorque, 2016. Versão eletrônica.

PASQUALE, Frank. *The black box society*: the secret algorithms that control money and information. President and Fellows of Harvard College. 2015. Versão eletrônica.

SANG-HUN. Choe. In South Korea, Covid-19 comes with another risk: online bullies. *The New York Times*, Nova Iorque, 19 set. 2020. Disponível em: https://www.nytimes.com/2020/09/19/world/asia/south-korea-covid-19-online-bullying.html?utm_campaign=newsletter_-_23-09-2020&utm_medium=email&utm_source=RD+Station. Acesso em: 7 set. 2020.

SILVA, Antonio Augusto Moura. *Sobre a importância da ampliação da capacidade de testagem dos sintomáticos para a contenção da epidemia pela COVID-19 no Brasil*. 20 mar. 2020. Disponível em: https://abori.com.br/artigos/sobre-a-importancia-da-ampliacao-da-capacidade-de-testagem-dos-sintomaticos-para-a-contencao-da-epidemia-pela-covid-19-no-brasil/. Acesso em: 7 set. 2020.

TEFFÉ, Chiara Spadaccini. *Tratamento de dados pessoais de crianças e adolescentes*: considerações sobre o art. 14 da LGPD. A LGPD e o novo marco normativo no Brasil. Caitlin Mulholland, 2020. Versão eletrônica.

TEFFÉ, Chiara Spadaccini; TEPEDINO, Gustavo. *Consentimento e proteção de dados na LGPD*. Lei Geral de Proteção de Dados Pessoais

e suas repercussões no Direito Brasileiro. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

TRINDADE, Rodrigo. App Coronavírus SUS agora vai avisar quando usuário foi exposto: entenda. *UOL*, 31 jul. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/07/31/app-coronavirus---sus-adiciona-rastreamento-de-contatos-entenda.htm. Acesso em: 7 set. 2020.

UNIÃO EUROPEIA. Comissão Europeia. *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*. 17 abr. 2020. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020XC0417%2808%29. Acesso em: 7 set. 2020.

UNIÃO EUROPEIA. Parlamento Europeu. *Tracking mobile devices to fight coronavirus*, abr. 2020. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649384/EPRS_BRI(2020)649384_EN.pdf. Acesso em: 7 set. 2020.

INTERNET E REGULAÇÃO: O MARCO CIVIL DA INTERNET COMO ESTRATÉGIA (NECESSÁRIA) DE GOVERNANÇA NACIONAL

Pablo Coutinho Barreto[1]

RESUMO

A internet é um fenômeno tecnológico que impacta de forma ímpar a vida da sociedade contemporânea em todas as suas múltiplas dimensões. Sua importância impõe a discussão sobre as formas de regulação necessárias ao bom uso. O modelo brasileiro de governança merece destaque, dada sua perspectiva democrática, colaborativa e multissetorial. Dentro deste ecossistema de governança plural, foi gestado o Marco Civil da Internet, que estabelece princípios, fundamentos, objetivos, garantias, direitos e deveres dos múltiplos atores da rede. O diploma se mostra estratégia válida e necessária de governança nacional da internet, estando perfeitamente alinhada com as estratégias em âmbito global.

Palavras-chave: Internet. Regulação. Governança. Modelo. Marco Civil da Internet.

---

1 Mestre em Desenvolvimento e Meio Ambiente pela Universidade Federal de Sergipe. Especialista em Direito Civil pela Fundação Faculdade de Direito da Bahia. Procurador da República.

ABSTRACT

The Internet is a technological phenomenon that uniquely impacts the life of contemporary society in all its multiple dimensions. The importance of the Internet in society requires that we discuss what forms of regulation are necessary for its proper use, and that the Brazilian governance model deserves to be highlighted given its democratic, collaborative and multisectoral perspective. Within this ecosystem of plural governance, the Brazilian Civil Internet Framework was established, establishing principles, foundations, objectives, guarantees, rights and duties of the network's multiple actors. The Civil Internet Framework is a valid and necessary strategy for national internet governance and is perfectly aligned with global strategies.

Keywords: Internet. Regulation. Governance. Model. Brazilian Civil Framework of the Internet.

1. INTRODUÇÃO

Atualmente, vive-se em uma sociedade em rede; todos estão conectados entre si e dependentes da internet. Esse fenômeno tem impactado a sociedade contemporânea de forma considerável, influenciando os rumos da atividade econômica, da política nacional e internacional, modificando as formas de expressão cultural e de provimento de serviços de educação e saúde.

Amizades, informações, relacionamentos amorosos, negócios e outras inúmeras atividades de nossa vida cotidiana perpassam, necessariamente, pela rede mundial de computadores. Não é por outra razão que uma pesquisa realizada por *BBC World Service* (2010) demonstrou que, ao menos, quatro em cada cinco pessoas consideram o acesso à internet um direito fundamental.

Esse cenário, completamente distinto há poucas décadas, é reconhecido por todos que se predispõem a estudar o fenômeno da internet. A essencialidade do funcionamento da rede é inquestionável, por isso muito se debate, nos governos, na academia, na indústria tecnológica e na sociedade civil, acerca da necessidade e forma de sua regulação.

A regulação da internet, sua governança, abrange múltiplas facetas, atores e interesses – públicos, privados, políticos, econômicos e culturais. Uma das questões mais importantes postas em debate é o âmbito da governança da rede, se global, nacional, multilateral, multissetorial, e a capacidade de diversas estratégias de regulação conviverem.

Nessa linha, discute-se a eficácia e a relevância da adoção de estratégias normativas nacionais, ante a ausência de um marco normativo internacional que regule o uso e o desenvolvimento da internet.

O presente artigo busca, dentro desse contexto, analisar a importância do Marco Civil da Internet, Lei n. 12.965, de 23 de abril de 2014, enquanto estratégia nacional de governança da internet. Adota-se uma abordagem qualitativa, amparada em pesquisa bibliográfica, buscando-se subsídios críticos acerca da relevância da legislação brasileira, que estabelece princípios, garantias, direitos e deveres para o uso da internet no País.

De início, são apresentados conceitos e marcos históricos relacionados à internet e sua governança, de forma a introduzir o tema a ser abordado. Em seguida, passa-se a descrever a estrutura e o funcionamento da governança da internet no Brasil, conferindo-se o merecido destaque ao modelo inovador aqui adotado. Após, entra-se, propriamente, no âmago da discussão da hipótese formulada, aferindo-se a importância do Marco Civil da Internet como estratégia de governança nacional.

2. A INTERNET E SUA GOVERNANÇA: CONCEITOS E MARCOS HISTÓRICOS

A internet, em definição constante em verbete da *Wikipédia*, é um sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos (*Internet Protocol Suite* ou TCP/IP), com o propósito de servir progressivamente usuários no mundo inteiro.

Em linhas gerais, existem três camadas que compõem a internet: a infraestrutura física (cabeamento telefônico, cabo, satélite), a estrutura de padrões lógicos (TCP/IP e outros protocolos) e os conteúdos. Uma de suas ideias fundamentais é propiciar a comunicação ponta a ponta entre os participantes da rede. Isso significa que quaisquer dispositivos a ela conectados podem comunicar-se livremente, lembrando-se que, atrás deles estão pessoas, que utilizam essa capacidade de comunicação para as mais diversas finalidades (GATTO *et al.*, 2009).

Como se vê, não há como limitar a definição de internet apenas a aspectos técnicos de infraestrutura. Sua estrutura complexa envolve também o processo de interação da tecnologia com a sociedade, em seus aspectos legais, regulatórios, econômicos, de desenvolvimento social e cultural (LUCERO, 2004; GATTO *et al.*, 2009).

Embora, desde seu nascedouro, parte da cultura da internet seja inspirada por correntes fortes de anarquismo e pensamento libertário, que rejeita a intervenção estatal e qualquer possibilidade de controle ou regulação (SILVA, 2015), um fenômeno tecnológico de tal porte demanda, necessariamente, a existência de alguma regulação pública e/ou privada, sob pena de virar uma verdadeira "terra sem lei". Assim, o desenvolvimento da internet precisa se fazer acompanhado, sempre de perto, pela discussão acerca das dimensões e formas de sua governança.

Os especialistas da telecomunicação veem a governança da internet com foco no desenvolvimento de determinada infraestrutura técnica. Os especialistas da computação se concentram no desenvolvimento de diferentes padrões e aplicações. Já os da comunicação priorizam a faci-

lidade nessa área. Por sua vez, os ativistas dos direitos humanos miram questões relacionadas à liberdade de expressão, à privacidade e a outros direitos humanos básicos. Os advogados se detêm aos detalhes relativos à jurisdição e resolução de controvérsias. Os políticos geralmente priorizam questões que causem impacto na seara eleitoral, enquanto os diplomatas se preocupam com o desenvolvimento dos interesses nacionais e sua proteção (KURBALIJA, 2016). Todas essas perspectivas, entretanto, entrelaçam-se na definição atual de governança da internet.

A governança da internet foi conceituada pela Cúpula Mundial sobre a Sociedade da Informação (2003) como o desenvolvimento e a aplicação pelos governos, pelo setor privado e pela sociedade civil, em seus respectivos papéis, de princípios, normas, regras, procedimentos de tomadas de decisão e programas em comum que definem a evolução e o uso da internet. Definição semelhante é defendida por Kurbalija (2016), para quem a governança da internet pode ser vista como o conjunto de atividades desenvolvidas por uma complexa teia de agentes (privados e públicos, nacionais e internacionais) de gerência e coordenação de recursos, processos, conteúdos, aplicativos e sistemas relacionados.

A evolução da governança da internet no mundo pode ser analisada a partir de diversos marcos históricos, merecendo um destaque por seu relevo, a fase que vai do início do desenvolvimento da rede até o fim da década de 1990, a que se inicia com a criação da *Internet Corporation for Assigned Names and Numbers* (Icann) e a deflagrada a partir das escandalosas revelações de Edward Snowden e o início da vigência do Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR, na sigla em inglês).

Até o fim da década de 1990, as questões relacionadas a esse tema se restringiam às eminentemente técnicas e eram desenvolvidas por universidades americanas, por delegação do governo dos Estados Unidos, berço do experimento denominado *Advanced Research Projects Agency Network* (Arpanet), que veio a originar a internet como a conhecemos hoje.

Em virtude da comercialização do acesso à internet, a sua consequente popularização e seu espraiamento pelo mundo, a governança da internet mereceu um processo de institucionalização mais robusto, surgindo, em 1998, a Icann, organização privada, sediada sob as leis do estado da Califórnia, aberta à participação internacional, pluriparticipativa, sem preponderância de atores governamentais, que passou a funcionar como ponto focal da governança (CANABARRO, 2014).

Outro marco histórico a merecer destaque ocorreu, em 2013, com a revelação pelo analista de sistemas da *National Security Agency* (NSA) Edward Snowden, a jornalistas do *The Guardian* e *Washington Post*, de mecanismos e infraestrutura de espionagem utilizados pelos Estados Unidos em cooperação com, ao menos, Reino Unido, Austrália, Nova Zelândia e Canadá.

As revelações de Snowden não só fizeram com que o público global se interessasse em saber como é a governança da internet, especialmente em relação às questões relacionadas à proteção de dados e aos direitos de privacidade (KURBALIJA, 2016), como provocou reações de diversos países, a exemplo daquelas protagonizadas por Brasil e Alemanha, inclusive com a proposição pelo governo brasileiro, em discurso proferido pela presidente Dilma Rousseff na 68ª Assembleia Geral das Nações Unidas, de cinco princípios que deveriam orientar a constituição de um marco civil multilateral, conforme nos recordam Canabarro e Gonzales (2018).

Esse episódio deflagrou um debate amplo sobre o tema, resultando, inclusive, na realização do Encontro Multissetorial Global sobre o Futuro da Governança da Internet – NETmundial, ocorrido em abril de 2014, na cidade de São Paulo. O evento teve por agenda de trabalho a definição de princípios para a condução da governança global da internet e a criação de um roteiro para a evolução da rede mundial.

Por fim, uma explanação sobre o desenvolvimento da governança da internet em âmbito mundial, que buscasse pontuar marcos históricos desde sua origem até os dias atuais, não seria satisfatória caso não fosse

mencionado o impacto da nova regulamentação europeia de proteção de dados da União Europeia, a *General Data Protection Regulation* (GDPR), em vigência desde o dia 25 de maio de 2018.

O GDPR, apesar de ser uma lei da União Europeia (UE), por diversos fatores, possui eficácia e aplicação extraterritorial, além dos seus limites geográficos. Como bem apontam Cordeiro e Gouveia (2018), a norma europeia tornou-se o novo parâmetro do fluxo relacional entre organizações e pessoas, baseando-se em pilares estruturais que determinam o tratamento lícito e transparente dos dados, a minimização dos dados e a coleta reservada, apenas, a fins e prazos determinados e estritamente necessários, com direito ao esquecimento, entre outros.

Não é por outra razão que diversas legislações nacionais foram influenciadas pelo GDPR, inclusive a Lei Geral de Proteção de Dados (LGPD) brasileira, que entrou em vigência em setembro de 2020.

3. O MODELO BRASILEIRO DE GOVERNANÇA DA INTERNET

O Brasil idealizou e implantou um modelo institucionalizado de governança da internet de forma inédita, em âmbito mundial. Não somente o pioneirismo dessa iniciativa merece destaque, mas também sua forma de condução, calcada, desde o nascedouro, em uma perspectiva colaborativa e multissetorial.

A internet deve sua inserção no território brasileiro às iniciativas da área acadêmica na década de 1980. Em razão disso, tanto o registro de nomes sob o .br quanto a distribuição de nomes IP (*Internet Protocol*) foram alocados no meio acadêmico até o amadurecimento da rede despertar o interesse em setores da iniciativa privada e do governo (GATTO *et al.*, 2009).

Em 1995, o Ministério das Comunicações e o Ministério da Ciência, Tecnologia e Inovação divulgaram nota afirmando a importância de

se constituir um comitê para gerir a internet no Brasil. Essa proposta veio a se tornar realidade, em pouco tempo, com a edição da Portaria Interministerial n. 147, de 31 de maio de 1995, que criou, de forma inovadora, o Comitê Gestor da Internet no Brasil (CGI.br).

Originalmente composto por 9 membros, atualmente o CGI.br constitui-se de 21 representantes escolhidos dentre prepostos do próprio governo, da área acadêmica, de operadoras de telecomunicações e de provedores de acesso. Além desses, há um representante dos usuários, eleito para exercer um mandato de três anos.

Embora não exista previsão para a sociedade participar diretamente das decisões do Comitê Gestor da Internet no Brasil, Gatto *et al.* (2009) esclarecem que a representatividade dos principais setores envolvidos está plenamente assegurada em sua composição. Isso porque, além dos representantes do governo, as entidades do terceiro setor elegem quatro conselheiros, as associações de empresas – provedores, telecomunicações etc. – selecionam outros quatro, as associações acadêmicas nomeiam três e o colegiado consensualmente designam um conselheiro que apresente notório saber no campo.

O modelo multissetorial e colaborativo de governança instituído pelo CGI.br fica ainda mais fortalecido ao tempo em que a participação de qualquer indivíduo interessado em questões mais técnicas é assegurada por meio de grupos de trabalho e fóruns de discussão que funcionam como espaços de diálogo e de troca de informação dentro da comunidade técnica da internet no Brasil (GATTO *et al.*, 2009).

As atuais atribuições do Comitê Gestor da Internet no Brasil estão disciplinadas no Decreto n. 4.829, de 3 de setembro de 2003, cabendo-lhe: i) estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil; ii) estabelecer diretrizes para a organização das relações entre o governo e a sociedade, na execução do registro de nomes de domínio, na alocação de endereço IP e na administração pertinente ao domínio de primeiro nível (ccTLD – *country*

code Top Level Domain), ".br", no interesse do desenvolvimento da internet no país; iii) propor programas de pesquisa e desenvolvimento relacionados à internet, que permitam a manutenção do nível de qualidade técnica e inovação no uso, bem como estimular sua disseminação em todo o território nacional, buscando oportunidades constantes de agregação de valor aos bens e serviços a ela vinculados; iv) promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de internet, bem assim para a sua crescente e adequada utilização pela sociedade; v) articular as ações relativas à proposição de normas e procedimentos referentes à regulamentação das atividades inerentes à internet; vi) garantir sua representatividade em fóruns técnicos nacionais e internacionais sobre internet; vii) adotar os procedimentos administrativos e operacionais necessários para que a gestão da internet no Brasil se dê segundo os padrões internacionais aceitos pelos órgãos de cúpula da internet, podendo, para tanto, celebrar acordo, convênio, ajuste ou instrumento congênere; viii) deliberar sobre quaisquer questões a ele encaminhadas quanto aos serviços de internet no país; e ix) aprovar seu regimento interno.

O Comitê Gestor da Internet não se constitui em órgão governamental. Somente adquiriu personalidade jurídica em 2005, quando foi criada uma sociedade civil sem fins lucrativos, sob a supervisão do CGI.br, chamada Núcleo de Informação e Coordenação do .br (NIC.br). O grupo passou a ser o braço executivo do Comitê para várias de suas atribuições (GATTO *et al.*, 2009).

O NIC.br é dividido em vários núcleos: o Registro.br, responsável pelos nomes ".br", pela distribuição dos endereços IP, no País, e por cuidar dos servidores raiz do DNS aqui presentes. As questões de segurança são atribuição do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). Cabe ao Centro de Estudos sobre as Tecnologias da Informação e da Comunicação (CETIC.br) a produção de indicadores e estatísticas, responsáveis pela divulgação

de informações periódicas sobre o crescimento da rede, fundamentais ao monitoramento e à avaliação do impacto socioeconômico das novas tecnologias. A atuação em relação a questões de infraestrutura e qualidade técnica da internet fica reservada ao Centro de Estudos e Pesquisas em Tecnologia de Redes e Operações (CEPTRO.br).

A estrutura da governança brasileira da internet, centrada no CGI.br, consolida um modelo pluriparticipativo e horizontalizado que opera a partir do consenso de seus conselheiros representantes do poder público, do setor privado, do terceiro setor e da academia, servindo de inspiração para o futuro da governança global da internet (CANABARRO, 2014).

Destaca-se, na abordagem brasileira, sua gestão pluralista de bens da comunidade. Embora o CGI.br não abarque todos os temas da governança da internet, atualmente objeto de discussão mundial através do Fórum de Governança da Internet da ONU (IGF), por meio de comissões de trabalho voluntárias, busca acompanhá-los (conteúdo, acesso, inclusão digital, privacidade, regulação, uso indevido, entre outros), participando de forma destacada nos principais fóruns, conferências, organismos e eventos internacionais relacionados ao desenvolvimento e governança da Internet, entre os quais as reuniões da Icann e do IGF (AFONSO, 2005).

Credita-se, ainda, como vantagem do modelo de governança brasileiro, o fato de o CGI.br se guiar por um conjunto de princípios para a governança e uso da internet no Brasil, o denominado "Decálogo do CGI.br", aprovado pela Resolução CGI.br/RES/2009/003/P. Segundo esse decálogo, trata-se de princípios que devem embasar e orientar as ações e decisões do CGI: i) liberdade, privacidade e direitos humanos; ii) governança democrática e colaborativa; iii) universalidade; iv) diversidade; v) inovação; vi) neutralidade da rede; vii) inimputabilidade da rede; viii) funcionalidade, segurança e estabilidade; ix) padronização e interoperabilidade; e x) ambiente legal e regulatório (CANABARRO, 2014).

O processo de institucionalização da governança da internet no Brasil deu outro passo importante e inovador com a elaboração de uma norma

que estabelece princípios, garantias, direitos e deveres para o uso da internet no País.

Iniciado no ano de 2009, o debate público que precedeu a elaboração do Marco Civil da Internet ocorreu de forma dialógica e colaborativa, sendo promovido pelo Ministério da Justiça, em parceria com o Centro de Tecnologia e Sociedade, da Fundação Getúlio Vargas, por meio da plataforma CulturaDigital.br. No curso desse processo, os mais diversos setores da sociedade participaram vivamente das discussões que resultaram em um texto cujas balizas foram dadas pelos já mencionados princípios para a governança e uso da internet no Brasil (Decálogo do CGI.br).

Após essa ampla discussão, o Projeto de Lei do Marco Civil da Internet, enviado pelo Poder Executivo ao Congresso no ano de 2011, foi aprovado e sancionado durante o Encontro NETmundial, realizado na cidade de São Paulo. A novel legislação (Lei n. 12.965, de 23 de abril de 2014), construída de forma aberta e colaborativa, estabeleceu em seus 32 artigos, de forma detalhada, fundamentos, princípios, objetivos, regras de interpretação, garantias, direitos e deveres para o uso da internet no Brasil.

4. O MARCO CIVIL DA INTERNET COMO ESTRATÉGIA (NECESSÁRIA) DE GOVERNANÇA NACIONAL

O Marco Civil da Internet surge como um dos mais importantes instrumentos legislativos domésticos a consagrar princípios e direitos de usuários de internet, estruturando, igualmente, os contornos legais das responsabilidades, da liberdade de expressão e acessos no ambiente digital, encarando-os como vetores da cidadania global. Foram considerados no processo dialógico de construção da norma os interesses de governos, organizações da sociedade civil, empresas, representantes do Poder Judiciário, especialistas em políticas públicas e membros da

academia. O amplo envolvimento dos vários setores da sociedade resultou no exemplo mais bem delineado de participação multissetorial na elaboração e no monitoramento da lei (POLIDO; ANJOS, 2016).

Para o criador da *World Wide Web*, Tim Berners-Lee, com a aprovação do texto do Marco Civil da Internet, o Brasil consolidou sua reputação como líder da democracia e contribuiu para a inauguração de uma nova era, na qual os direitos dos cidadãos do mundo serão protegidos por Constituições digitais (LIMA, 2014).

A partir da vigência do diploma, a disciplina do uso da internet no Brasil teve como fundamentos: respeito à liberdade de expressão; reconhecimento da escala mundial da rede; garantia dos direitos humanos; desenvolvimento da personalidade e exercício da cidadania em meios digitais; pluralidade e diversidade; abertura e colaboração; livre iniciativa, livre concorrência e defesa do consumidor; e finalidade social da rede.

Os princípios fixados foram a garantia da liberdade de expressão, comunicação e manifestação de pensamento; proteção da privacidade; proteção dos dados pessoais; preservação e garantia da neutralidade de rede; preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; responsabilização dos agentes de acordo com suas atividades; preservação da natureza participativa da rede; e liberdade dos modelos de negócios promovidos na internet.

Alguns pilares do Marco Civil da Internet alteraram as normas vigentes e definiram de forma clara as relações entre usuários e destes com empresas do setor, a exemplo da garantia da liberdade de expressão, privacidade, intimidade dos usuários e inviolabilidade das comunicações, a necessidade de consentimento prévio do usuário para a coleta de dados, o respeito à finalidade da coleta, o tempo de guarda de registros de conexão e de navegação do usuário, a retirada de conteúdos infringentes e a neutralidade da rede (BRASIL, 2015).

Outro aspecto que merece destaque, especialmente no que se refere

à solução de conflitos entre usuários de empresas, é quanto à incidência da lei brasileira a provedores de aplicações e conexão sediados em país estrangeiros. De acordo com o disposto no art. 11, em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que, pelo menos, um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Os §§ 2º e 3º ressaltam, ainda, que a norma de extraterritorialidade se aplica aos dados coletados em território nacional e ao conteúdo das comunicações, desde que, pelo menos, um dos terminais esteja localizado no Brasil, mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou, pelo menos, uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

É necessário destacar, entretanto, haver autores que formulam críticas duras à regulamentação de princípios, garantias, direitos e deveres para o uso da internet no Brasil, por meio do Marco Civil da Internet. Tomasevicius Filho (2016), por exemplo, sustenta que, embora o diploma tenha sido bastante festejado por ser a primeira lei do mundo a disciplinar os direitos e deveres dos usuários da rede, mudanças substanciais não ocorrerão, uma vez que a legislação não teria acrescentado praticamente nada à legislação vigente e seria ingenuidade do legislador brasileiro manter a pretensão de solução de problema de escala mundial, com efeitos extraterritoriais, por meio de uma lei nacional. Diante disso, a solução para a governança da internet exigiria a elaboração de uma lei uniforme ou convenção internacional sobre o uso da internet a instituir um marco civil internacional.

Há fortes argumentos, no entanto, que parecem afastar as principais críticas lançadas em relação ao caráter inovador do Marco Civil da Inter-

net e à possibilidade de bem regular comportamentos de usuários, provedores de conteúdo, provedores de aplicação e do próprio Poder Público.

De início, é preciso destacar que, se o Direito brasileiro preenchia as lacunas existentes até então, interpretando e adaptando as normas existentes à nova realidade tecnológica, pautando-se em princípios dispostos na Constituição Federal de 1988 e em regras especificadas no Código Civil, no Código de Defesa do Consumidor, na Lei do *Habeas Data* e, mais recentemente, na Lei de Acesso à Informação, com a aprovação do Marco Civil da Internet, a proteção à privacidade foi alçada a princípio, de forma a orientar e disciplinar o uso da internet no país (MENESES; ASSUNÇÃO, 2016). Ou seja, para além de inovar o ordenamento jurídico, estabelecendo regras específicas, construídas a partir de terminologia e conceitos adequados à nova tecnologia, o normativo incorporou à legislação ordinária brasileira princípios de governança e uso da internet, antes dispostos apenas em documentos elaborados pelo CGI.br, de forma a lhes conferir maior estatura normativa, orientando a interpretação e aplicação do direito na regulação das condutas humanas em suas relações virtuais.

Sobre o outro aspecto criticado, é verdade que o caráter transnacional da internet não foi acompanhado por uma lei internacional, prevalecendo ainda hoje a influência norte-americana, por razões que se prendem, sobretudo, à própria gênese da internet, à localização da entidade privada que gere os nomes de domínio e os endereços de IP (Icann), em Los Angeles, e à grande concentração de *data centers* instalados nos Estados Unidos (SILVA, 2015).

Como destacado por Gatto *et al.* (2009), talvez os mecanismos de governança hoje existentes não sejam suficientemente adequados para assegurar o equilíbrio entre os múltiplos interesses dos diversos atores envolvidos, bem como a continuidade e crescimento dos benefícios trazidos pela internet à sociedade em geral e aos indivíduos. O caminho a ser trilhado para a evolução do modelo atual de governança da internet, todavia, não pode estar atrelado ao abandono de estratégias

nacionais, em favor de uma suposta incapacidade da legislação interna para produzir efeitos extraterritoriais significativos. Ao contrário, o modelo de governança global da internet é pluralista (*multistakeholder*), com a participação de atores governamentais e privados, da academia, do terceiro setor, em um processo dinâmico de construção colaborativa que abarca a possibilidade de convivência pacífica de normas internacionais, regionais e nacionais, com seus objetivos perfeitamente alinhados.

Canabarro (2014) adverte parecer improvável alcançar o consenso em torno da ideia da governança da internet desnacionalizada e universal, desvinculada da competição interestatal no sistema internacional e da possibilidade de captura da estrutura institucional existente no plano sistêmico, bem como do recurso às alianças entre a agência estatal e a agência não estatal, formadas de maneira dinâmica em prol de interesses nacionais bem definidos.

A governança da internet traz em si um grau de reciprocidade entre atores e regiões que mescla os efeitos locais e globais das suas decisões. Com isso, novas formas de regulação e deliberação multilateral e multissetorial se consolidam (ANASTÁCIO, 2016). Canabarro e Gonzales (2018) ressaltam, acertadamente, haver uma convergência possível que envolva multilateralismo e multissetorialismo, capaz de garantir uma coexistência pacífica e oferecer uma alternativa de democratização da política internacional por meio da abertura à participação nos processos de formulação e tomada de decisão.

A adoção de uma estratégia nacional, inclusive normativa, ao revés de se mostrar incompatível com a existência de uma governança global e a adoção de um marco civil internacional, alinha-se ao disposto no item 38 da Agenda de Túnis para a Sociedade da Informação, aprovada pela Cúpula Mundial sobre a Sociedade da Informação, em 2005, que clama pelo fortalecimento das instituições regionais de gestão dos recursos da internet, para garantir os interesses nacionais e os direitos desses países de geri-los, ao mesmo tempo que mantém a coordenação global.

Nessa linha, andou muito bem o Brasil ao adotar o Marco Civil da Internet como estratégia nacional de governança da internet, consolidando um modelo de regulação democrático, aberto, colaborativo e multissetorial. O diploma aqui vigente é a expressão de um modelo pluralista, que privilegia a participação de múltiplos atores no processo de construção da gestão, em contraposição ao modelo de regulação tradicionalmente adotado no cenário internacional. A norma brasileira que estabelece princípios, garantias, direitos e deveres para o uso da internet, além de se bem articular com as iniciativas globais de governança da rede, serve como paradigma de um caminho exitoso a ser trilhado na elaboração de um marco civil internacional.

5. CONCLUSÃO

O fenômeno tecnológico da internet não se limita a uma infraestrutura física e a padrões lógicos que permitem a comunicação entre seus participantes. É um processo dinâmico de interação da própria tecnologia com a sociedade contemporânea, como nenhuma outra na história, responsável por impactar a vida das pessoas de tal forma que se prospecta o acesso à internet como um novo direito fundamental.

Dada a relevância da internet para a vida cotidiana atual, muito se discute acerca da necessidade de alguma regulação pública e/ou privada incidir sobre sua estrutura, seu desenvolvimento e seus objetivos. Nesse contexto, um dos debates mais interessantes abrange saber as dimensões e formas de governança necessárias para o bom uso da rede.

A governança da internet pode ser definida como desenvolvimento e aplicação de princípios, regras, procedimentos e protocolos de tomada de decisão, por uma rede complexa de atores públicos, privados, nacionais e internacionais, que definem seu uso e evolução. O modelo brasileiro, pioneiro em âmbito mundial, merece destaque por sua pers-

pectiva colaborativa e multissetorial. O pluralismo na composição da entidade encarregada da governança da internet no Brasil (CGI.br) e a abertura do processo de formação e tomada de decisões, aliados à existência de um conjunto de princípios postos (Decálogo do CGI.br) que balizam eticamente as diretrizes adotadas na regulação da internet, são características positivas que merecem servir de exemplo para modelos de outros países.

O Marco Civil da Internet foi gestado neste ambiente democrático, colaborativo e multissetorial. A participação dos mais diversos setores da sociedade brasileira na elaboração da proposta que veio a ser aprovada pelo Congresso Nacional resultou em uma norma que estabelece, de forma detalhada, fundamentos, princípios, objetivos, regras de interpretação, garantias, direitos e deveres para o uso da internet no Brasil.

Entretanto, algumas críticas são lançadas quanto à relevância dessa lei para a regulação das condutas de usuários, provedores de conteúdo, provedores de aplicação e do próprio Poder Público, notadamente em relação a sua suposta incapacidade de conseguir produzir efeitos significativos, dado o caráter transnacional da rede.

Ocorre que a elaboração de uma legislação interna, para servir como alicerce de uma boa governança da internet, alinha-se ao disposto no item 38 da Agenda de Túnis para a Sociedade da Informação, que clama pelo fortalecimento das instituições regionais de gestão, para garantir os interesses nacionais e os direitos desses países a gerir os próprios recursos da internet, ao mesmo tempo que mantém a coordenação global.

Ao adotar o Marco Civil da Internet como uma estratégia nacional de governança da internet, o Brasil, além de consolidar um modelo de regulação democrático, aberto, colaborativo e multissetorial, mantém-se em consonância com as estratégias de governança global da internet, sendo perfeitamente compatível com um futuro marco civil internacional, servindo-lhe, inclusive, como exemplo.

REFERÊNCIAS

AFONSO, Carlos Alberto. *Governança da internet*: contexto, impasses e caminhos. São Paulo: RITS, 2005.

ANASTÁCIO, Kimberly de Aguiar. Transnacionalidade na rede: introdução à governança da internet e ao Netmundial. *In*: POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos (Orgs.). *Marco civil e governança da internet*: diálogos entre o doméstico e o global. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2016. p. 224-248.

BBC NEWS. *Internet access is "a fundamental right"*. 2010. Disponível em: http://news.bbc.co.uk/2/hi/8548190.stm. Acesso em: 24 jul. 2018.

BRASIL. *Lei n. 12.965, de 23 de abril de 2014*. Marco Civil da Internet [recurso eletrônico]: estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. 2. ed. Brasília: Edições Câmara, 2015.

CANABARRO, Diego Rafael. *Governança global da internet*: tecnologia, poder e desenvolvimento. Tese (Doutorado em Ciência Política). Instituto de Filosofia e Ciências Humanas, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014. 433 p.

CANABARRO, Diego Rafael; GONZALES, Alexandre Arns. Governança global da internet: um mapa da economia política internacional em torno dos identificadores alfanuméricos da rede. *Carta Internacional*, [S.l.], v. 13, n. 1, maio 2018. ISSN 2526-9038. Disponível em: https://cartainternacional.abri.org.br/Carta/article/view/748. Acesso em: 25 jul. 2018.

CORDEIRO, Silvério Brunhoso; GOUVEIA, Luis Borges. *Regulamento Geral de Proteção de Dados (RGPD)*: o novo pesadelo das empresas?,

maio 2018. Disponível em: https://bdigital.ufp.pt/bitstream/10284/6714/1/RI_trs_07_2018.pdf. Acesso em: 24 jul. 2018.

CÚPULA MUNDIAL SOBRE A SOCIEDADE DA INFORMAÇÃO, Genebra 2003-Túnis 2005. Tradução de Marcelo Amorim Guimarães, São Paulo: Comitê Gestor da Internet no Brasil, 2014.

GATTO, Raquel F.; MOREIRAS, Antonio M.; GETSCHKO, Demi. *Governança da internet*: conceitos, evolução e abrangência. 27º Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2009. Livro Texto dos Minicursos, p. 61-97.

INTERNET. *Wikipédia*: a enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Internet. Acesso em: 24 jul. 2018.

LIMA, Luiz. Dilma destaca defesa a Marco Civil feita por Berners-Lee. *Estadão Digital*. Disponível em: http://www.estadao.com.br/noticias/nacional,dilma-destaca-defesa-a-marco-civil-feitapor-berners-lee,1148991,0.htm. Acesso em: 24 jul. 2018.

MENESES, Rafael da Silva; ASSUNÇÃO, Linara Oueiras. Os contornos jurídicos da proteção à privacidade no Marco Civil da Internet. *In*: POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos (Orgs.) *Marco civil e governança da internet*: diálogos entre o doméstico e o global. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2016. p. 112-145.

MONTEIRO, Renato Leite. Lei Geral de Proteção de Dados do Brasil: análise contextual detalhada. *Jota*, Opinião & Análise, 14 jul. 2018. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/lgpd-analise-detalhada-14072018. Acesso em: 24 jul. 2018.

OLIVEIRA, Carlos Eduardo Elias de. *Aspectos principais da Lei n.*

12.965, de 2014, o Marco Civil da Internet: subsídios à comunidade jurídica. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/Senado, abr./2014 (Texto para Discussão n. 148). Disponível em: www.senado.leg.br/estudos. Acesso em: 24 jul. 2018.

POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos. Palavras inciais. *In*: POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos. *Marco civil e governança da internet*: diálogos entre o doméstico e o global. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2016, p. xi-xiv.

SILVA, Nuno Sousa. *A internet*: um objecto para o Direito Administrativo Global? 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2586194. Acesso em: 24 jul. 2018.

CRIMES INFORMÁTICOS DE LAVAGEM DE DINHEIRO: LEI PENAL NO ESPAÇO E O PROBLEMA DAS LITISPENDÊNCIAS INTERNACIONAIS

Fábio André Guaragni[1]
Felipe Américo Moraes[2]

RESUMO

O presente artigo tem como objetivo responder a seguinte pergunta: em que medida os crimes informáticos de lavagem de dinheiro tencionam o Princípio da Territorialidade em matéria penal? Para responder, serão abordados: a) o desenvolvimento da política internacional de combate à lavagem de dinheiro, em particular a adotada pelo Brasil; b) os novos riscos advindos da quarta revolução industrial, sobretudo o surgimento dos ativos virtuais e a possibilidade de novos métodos da prática de lavagem de dinheiro através da internet; c) o tratamento dispensado hoje a esses crimes, tangente à lei penal no espaço; e, por fim, d) sugestões para solução de conflitos positivos de competência internacional.

---

1 Doutor em Direito Penal (UFPR). Professor (UniCuritiba/PR). Procurador de Justiça (MP/PR).

2 Mestrando em Direito Econômico e Cidadania (UniCuritiba/PR). Especialista em Direito Penal Econômico e Empresarial (Positivo/PR). Advogado criminalista.

Palavras-chave: Crimes informáticos. Lavagem de dinheiro. Criptomoedas. Territorialidade. Litispendência.

ABSTRACT

This article aims to answer the following question: money laundering crimes practiced thru the internet makes the Territoriality Principle's application difficult in criminal matters? In order to respond, will be said about: a) the development of the international policy to combat money laundering, especially that adopted by Brazil; b) the new risks arising from the Industrial Revolution 4.0, especially the emergence of virtual assets and the possibility of new methods of the practice of money laundering through the internet; c) the territorial treatment of these crimes today will be addressed; and, finally, d) suggestions for resolving positive conflicts of international competence will be mentioned.

Keywords: Cybercrime. Money laundering. Cryptocurrencies. Territoriality.

1. INTRODUÇÃO

A Revolução Industrial 4.0, marcada pelo que se convencionou chamar de tecnologias disruptivas, promotoras da fusão plena dos meios físico e biológico com o digital (SCHWAB, 2016, p. 16), mudou radicalmente a organização social em diversas áreas, incrementando exponencialmente a globalização econômica e das comunicações, evento que, devido à velocidade em que ocorre, causa um inevitável atraso regulatório (GUARAGNI; RIOS, 2019).

O Direito tem tradicionalmente no mundo físico/real a única referência espacial. Entretanto, a integração dos dados digitais em rede, a

partir do avanço da internet, produziu uma nova dimensão ambiental. É possível reconhecer um *meio ambiente digital* (FIORILLO; CONTE, 2017, p. 17) contínuo, sem fronteiras, que serve como cenário para condutas humanas inéditas e complexas. Daí emergem novos meios de agressão aos bens jurídicos tradicionalmente protegidos pelo direito penal (FLORES PRADA, 2015, p. 2).

Nesse contexto, em oposição a crimes informáticos próprios, praticados *contra* o sistema de dados (de regra, violando conectividade, privacidade ou higidez de dados), ganham importância os chamados crimes informáticos impróprios. Ou seja, delitos tradicionais como estelionato, furto, crimes contra a honra e outros passam a ser cometidos também com uso de tecnologias de informática ou sistemas informáticos de dados. Não é preciso que se faça, necessariamente, uso da internet para a configuração desses delitos. Porém, é recorrente que os sujeitos ativos se valham da rede para práticas delitivas. Mais: a integração da rede aos objetos – IoT, ou internet das coisas – certamente fomentará a instrumentalização da transmissão de dados pela rede de computadores como parte integrante do *modus operandi* delitivo.

Esse fenômeno tem afetado em particular o crime de lavagem de dinheiro, diante do surgimento das criptomoedas. Elas possibilitaram a movimentação de valores econômicos de maneira instantânea ao redor do mundo, sem a dependência de instituições financeiras e à margem das agências estatais de controles voltados à preservação dos sistemas financeiros nacionais. Nessa quadra, as moedas digitais incrementaram o risco de o dinheiro proveniente de atividades criminosas ser ocultado, dissimulado e novamente injetado na economia. E, à toda evidência, colocaram em maus lençóis o modelo tradicional de exercício do poder punitivo estatal, já que apegado a uma zona delimitada de território físico (GUARAGNI; RIOS, 2019, p. 168-169). A agência de poder moldada como estado-nação vai, também quanto a essa conjuntura, mostrando-se superada.

A lavagem de dinheiro é crime internacional impróprio (ou em sentido amplo). Sabe-se que a respectiva tipificação depende dos Poderes Legislativos nacionais, como consequência da adoção disseminada do princípio da reserva legal. Também o exercício de jurisdição ocorre em nível nacional, autorizado, em regra, pela prática do delito no território do país (princípio da territorialidade) ou, excepcionalmente, por critérios de extraterritorialidade. Porém, os reflexos do delito de lavagem são percebidos em âmbito internacional, de modo que apenas será possível alcançar a efetiva repressão com a cooperação e uniformização legislativa, mediante parametrização internacional (LIMA, 2013).

A rigor, a lavagem é um autêntico símbolo do fenômeno da internacionalização do direito penal: diferentes nações criminalizaram e adotaram medidas processuais para prevenir e punir, de maneira símile, esse crime. Entretanto, ainda que a cooperação internacional tenha avançado no campo da assistência judiciária e policial, o delito, quando praticado de modo multilocal, carece de novas perspectivas de desenvolvimento normativo. Isso fica escancarado no marco temático da lei penal no espaço.

O assunto ganha relevância devido ao fato de essa prática delituosa prescindir da conversão dos ativos ilicitamente angariados em valores expressados pelas moedas circulantes, de curso forçado e legal, no marco de cada sistema financeiro nacional. Os branqueamentos de valores têm rumado para práticas consistentes no envio de dados criptografados, capazes de se comportar como moeda, emulando-as. Sistemas como o *Bitcoin*[3] ou outras criptomoedas que compartilham, ou não, do mesmo *blockchain* representam uma complexa tecnologia, carente de

3 Dá-se o nome de "*Bitcoin*", com a primeira letra maiúscula, a todo o sistema tecnológico que envolve tanto a criptomoeda, em si, também nominada "*bitcoin*", quanto seu *blockchain*, o qual permite que as transações ocorram de maneira segura.

regulação internacional uniforme pelos Estados para mitigar os riscos de lavagem de dinheiro.

Em julho de 2018, foi identificado um comércio de 1,8 mil criptomoedas, com uma capitalização de mais de 300 bilhões de dólares. Nele, 26% dos usuários estão associados a atividades ilegais, representando 45% de todas as atividades realizadas. Pontualmente, estima-se que 49% do mercado já passou por alguma operação ilícita, aproximadamente 37 milhões ao ano, totalizando 76 bilhões de dólares (FOLEY; KARLSEN; PUTNINŠ, 2019).

Em que pese expressivo o número de *bitcoins* associado a atividades ilícitas, ele está longe do montante que circula fora desse sistema, cerca de 800 bilhões a 2 trilhões de dólares americanos por ano (UNITED NATIONS, 2020). Além disso, é necessário destacar que outras criptomoedas dispõem de tecnologias superiores de acréscimo de anonimato, mostrando-se ainda mais eficientes que a *bitcoin* para realizar atos de lavagem de dinheiro. Mesmo assim, esta continua sendo predominante nas transações que envolvem atividades ilícitas, a revelar que, devido à complexidade da tecnologia, há espaço incremental para a movimentação de dinheiro ilícito. Mesmo os que o fazem não exploram os mais modernos instrumentos desse ambiente.

Percebe-se, portanto, existir uma tendência ascendente no cometimento de crimes informáticos impróprios de lavagem. Ante suas características, há possibilidade de organizações criminosas moverem dinheiro de maneira muito rápida, sem se submeterem aos controles das instituições financeiras, com auxílio de uma tecnologia que, pela velocidade de evolução, está passos à frente da regulação estatal de combate a esse delito. Tudo é uma imensa preocupação para o sistema penal.

Lado outro, abre-se um questionamento quanto aos limites do poder punitivo. Toda ação praticada na internet acaba por ser *omnilocalizada*, tanto quanto seu resultado. Se o meio ambiente digital é contínuo e sem fronteiras, o que se opera na rede repercute em todo esse ambiente. Qualquer ação na rede é localizada na ciberesfera, assim como todo resultado.

Não se trata de uma deslocalização, ou afastamento de um local preciso, mas o avesso: o crime, em vez de sem local, dá-se em todo lugar.

Tudo vai além do meio ambiente físico. E, sem embargo, também fisicamente existe uma multiplicidade topográfica. O delito ocorre perante diferentes jurisdições, por meio de servidores e provedores de serviços localizados em diferentes territórios.

Assim, há o risco de o agente ser processado criminalmente em todas as jurisdições. Atualmente é bastante difundido o critério da ubiquidade para se definir se um crime foi cometido ou não em dado território nacional. No Brasil, está no art. 6º, CP: "desde que o crime haja tocado o território nacional", considera-se praticado no país, na clássica lição de Hungria (2017, p. 110). Observada a múltipla utilização desse critério em ordenamentos jurídicos mundo afora, ainda que o toque em cada um dos territórios tenha sido de maneira extremamente superficial, pelo critério físico dos servidores e provedores, autoriza-se o acionamento da jurisdição do país. Se o meio ambiente adotado como referência para o critério da ubiquidade for o digital, o problema radicaliza-se: todo crime de lavagem no ciberambiente toca o território brasileiro (como já dito, o espaço digital é contínuo, uno, sem fronteiras) e todos os demais territórios nacionais. Isso permite projetar a proliferação de casos de litispendências internacionais, hipótese que pode configurar *bis in idem*.

Diante disso, o presente artigo tem como objetivo responder a seguinte pergunta: em que medida os crimes informáticos de lavagem de dinheiro tencionam o Princípio da Territorialidade em matéria penal? Responde-se abordando: a) o desenvolvimento da política internacional de combate à lavagem de dinheiro, em particular a adotada pelo Brasil; b) os novos riscos advindos da Quarta Revolução Industrial, sobretudo o surgimento dos ativos virtuais e a possibilidade de novos métodos da prática de lavagem de dinheiro através da internet; c) o tratamento dispensado hoje a esses crimes, tangente à lei penal no espaço; e, por fim, d) as sugestões para solução de conflitos positivos de competência internacional.

2. INTERNACIONALIZAÇÃO DA POLÍTICA ANTILAVAGEM DE DINHEIRO

O fenômeno da internacionalização do direito penal – de que é grandemente representativa a política internacional de combate à lavagem de dinheiro – deriva da última globalização (a primeira é a própria revelação geográfica do globo, bem representada pela expansão ultramarina e, nela, pela primeira circum-navegação, capitaneada por Fernão de Magalhães[4]), do final dos anos 1990 em diante.

O termo "globalização" explica a realidade social de um mundo sem fronteiras, cujos países, em que pese distantes fisicamente, são intercomunicados. Tudo ocorre no horizonte do uso intensivo de meios de transporte, que marcaram a história já no impulso à própria Primeira Revolução Industrial, destacando-se o ferroviário (conforme SCHWAB, 2016, p. 15; ALESSANDRI, 2010, p. 201) e as tecnologias da informação.

Nesse contexto, fala-se em *globalização econômica*, diante da troca mundial de bens ou serviços com pouco custo agregado, em mercados integrados, impulsionada por uma política neoliberal mundial sucessiva ao contexto de guerra fria – o modelo bipolarizado herdado do pós-guerra. Também se aborda a *globalização das comunicações*, pois as tecnologias da informação permitiram a troca de todos os tipos de dados em tempo real e em quantidade ilimitada (BORJA JIMÉNEZ, 2009, p. 6-8). O uso desses meios de comunicação em rede mundial de dados suscitou a *globalização financeira*, integrando as trocas financeiras no ambiente virtual e sugerindo um novo tipo de capitalismo, substitutivo do modelo industrial. Emerge um muito apropriadamente denominado "capitalismo financeiro-consumerista", com a "deslocalização de capitais

4 Recomenda-se o belo romance histórico sobre a jornada de Fernão de Magalhães: *Além do fim do mundo*, de Laurence Bergreen.

e empresas e a redução da taxa de sindicalização", numa *deregulation* guiada por americanos e ingleses (MAGATTI, 2017, p. 22).

Por outro lado, a globalização econômico-financeira produziu também a globalização do crime, afinal repercutiu nas práticas de criminalidade organizada. As antigas quadrilhas se converteram em associações estruturadas e sofisticadas, o que permitiu acúmulo de capital em locais variados, propícios ao delito. Organizações criminosas ganharam grande autonomia; assim, métodos tradicionais de repressão se tornaram obsoletos na medida em que, devido à fungibilidade dos membros da organização, a detenção em presídios passou a ser insuficiente.

Nesse contexto, percebeu-se que perseguir o dinheiro (*follow the money*) seria o método mais eficaz de combater esse modelo de criminalidade. Devido à ciência de que o volume de capital em posse das organizações criminosas precisa se submeter a processos de branqueamento, a persecução da lavagem de dinheiro passou a ser objeto das políticas de combate ao crime organizado desde o final do último século (BADARÓ, 2016, p. 30).

Para que isso seja realizado de maneira eficiente, é indispensável aos Estados agir em cooperação internacional, adotando instituições punitivas que transcendam as barreiras dos sistemas penais nacionais, voltando-se aos sistemas jurídicos supranacionais. Assim, torna-se premente a *globalização política*, na medida em que o processo de perda de soberania estatal, em sua concepção clássica, enseja frequentes e necessárias compensações mediante apoios de organizações supranacionais (BORJA JIMÉNEZ, 2009, p. 8).

Não foram somente essas características do crime organizado que fomentaram as atuais legislações internacionais sobre lavagem de dinheiro. Como ele produz concorrência desleal, torna-se desinteressante para uma política neoliberal globalizada, pois dificulta oportunidades de negócio e liquida uma saudável atuação, no mercado, de agentes interessados em fornecimento e distribuição de produtos e serviços.

Para se compreender melhor como o crime organizado se enquadra no atual contexto político-econômico, é preciso perceber como se delineou a relação entre as diferentes revoluções industriais e as ideologias políticas dominantes das respectivas épocas.

Na Primeira Revolução Industrial, na transição do século XVIII para o XIX, o alicerce da riqueza de um país era a liberdade de mercado, com mínima interferência do Estado. A este cabia cumprir exclusivamente a função de garantir os direitos de liberdade e livre competição, restringindo ao máximo o poder soberano.

Tal ideal político foi radicalmente contraposto na Segunda Revolução Industrial, ocorrida entre os séculos XIX e XX. Marcada pela organização do trabalho em série e forte capitalização das empresas, fez nascer a preocupação com direitos sociais e, por conta, modelos de Estados intervencionistas. O Estado liberal cedeu espaço ao intervencionista, que, em vez de figurar como espectador, passou a atuar como guardião da proteção formal dos direitos humanos e progresso da comunidade. Os efeitos colaterais disso – hão de ser mencionados – foram os regimes autoritários e totalitários (BORJA JIMÉNEZ, 2009, p. 10-12). O período pós-Segunda Guerra evidenciou o esforço de se compor o modelo interventivo com o asseguramento da livre iniciativa, ilustrada pela experiência europeia de bem-estar social (certamente inspirada no exemplo norte-americano do *new deal*, voltado à recuperação da grande quebra de 1929).

A Terceira Revolução Industrial, típica do fim do século XX, teve a *globalização* como pano de fundo. Com ela, um projeto ideológico de neoliberalismo foi marcado especialmente pelo desenvolvimento de novas tecnologias e processos econômicos. Surgiu, assim, um Estado que abria mão de projetos políticos tradicionais e se aproximava do centro: menos utópico, preocupado com controles concretos de marcadores macroeconômicos (taxas de juros, inflação) capazes de propiciar bom ambiente de mercado, com a busca de soluções rápidas, práticas e eficazes (BORJA JIMÉNEZ, 2009, p. 12).

É nesse cenário que avulta – como preocupação estatal – a deslealdade concorrencial. Entra em foco a mencionada característica das organizações criminosas que se revela tortuosa: a imensa capacidade de injetar recursos ilícitos em atividades lícitas. Isso produz forma evidente de concorrência desleal.

Para realizar os processos de mascaramento do capital ilícito, essas organizações constituem atividades empresariais com aparência e objeto legais, seja por meio de empresas de fachada, seja por efetiva atuação no mercado. Neste caso, ao realizarem o objeto empresarial, enquanto atores de um setor econômico qualquer, despontam com insuperável vantagem concorrencial em relação àqueles que não fazem uso da mesma fonte de investimento.

O incentivo para a atividade comercial não é somente a obtenção do lucro correlato mas também sua utilização como instrumento de transferência do dinheiro, antes ocultado e distanciado da verdadeira fonte ilícita. Mesmo um modelo de negócio com lucro negativo acaba se mantendo ativo, causando uma espécie de *dumping* em relação aos demais (STEINKO, 2012, p. 918).

O problema ocorre também na aquisição de bens passíveis de expressão econômica, como no mercado de imóveis. Ali é possível a elevação substancial dos preços, devido ao aumento artificioso da demanda (FERWERDA, 2013, p. 9), desequilibrando-se as relações de mercado e o acesso aos bens por quem só maneja ganhos lícitos.

É este contexto de globalização, de busca por soluções pragmáticas e pela garantia de lealdade concorrencial, que produz a internacionalização do direito penal e, especialmente, faz surgir uma política internacional de combate à lavagem de dinheiro. Diante do caráter globalizado do crime, percebeu-se a incapacidade dos Estados de satisfazer autonomamente a necessidade de combater a espécie delitiva. Daí o recurso à cooperação com outros, buscando, na sociedade internacional, soluções eficazes aos problemas comuns. Passou a ser necessário, portanto, um

regime internacional de prevenção e persecução do crime de lavagem de dinheiro (CORDERO, 2002, p. 96).

Nesse contexto, os regimes de combate aos crimes internacionais resultantes da globalização provocaram uma *desterritorialização* e *reterritorialização*. Os novos riscos derivados da macrocriminalidade implicaram o deslocamento da produção de regramentos dos centros de competência do Estado nacional para a sociedade internacional, de modo a promover medidas adequadas e uniformes de controle. O crime globalizado demanda soluções também globais, de modo que os tradicionais meios de exercer a política criminal de um país, isoladamente e para dentro de sua jurisdição, precisam ceder espaço à atuação conjunta (OLIVEIRA, 2018, p. 6).

Vale destacar que o Estado, nesse caso, não funciona como mero receptor de regras externas. Surge, a partir do diálogo com a sociedade internacional, uma negociação para busca conjunta de soluções de uma demanda externa, mas que precisa encaixar-se na política interna de cada Estado. Assim, a ideia de soberania nacional permanece presente no ponto em que nenhum Estado está obrigado a aderir a determinado projeto, incompatível com seu ordenamento jurídico (OLIVEIRA, 2018, p. 13). Há, entretanto, a evolução do conceito clássico de soberania[5], tensionado pela complexidade do mundo moderno, cujas decisões adotadas por um Estado acerca de sua política interna acabam sendo influenciadas pelos demais, os quais podem tanto endossá-las quanto a elas se opor (BAUMAN, 2011). Com isso, a autonomia do Estado para deliberar sobre seu ordenamento jurídico é diluída, e suas decisões influenciadas pela sociedade mundial. Percebe-se, diante disso,

5 No âmbito jurídico, trata-se da faculdade exclusiva do Estado para deliberar acerca de determinado tema social, em que haveria uma espécie de monopólio (OLIVEIRA, 2018, p. 11).

que o conceito clássico da soberania estatal passou por um processo de mutação irreversível, diante do fenômeno da internacionalização do Direito, por meio da absorção de modelos internacionais de combate à criminalidade (LIPINSKI; FERREIRA, 2019, p. 2-10).

3. A VIGÊNCIA DE UMA POLÍTICA INTERNACIONAL ANTILAVAGEM DE DINHEIRO

Por meio de reiteradas obrigações internacionais, os Estados assumiram gradualmente compromissos legislativos de promoção do adequado tratamento do crime de branqueamento de capitais, cuja persecução somente encontra eficácia acaso haja unidade de regulação sobre o tema. Em especial, identificaram-se carências de tipificação uniforme e previsão de meios adequados de persecução criminal e cooperação judicial internacional (OLIVEIRA, 2018, p. 5). Segundo Silva Sánchez (2013), a criminalidade da última globalização tornou imprescindível, em que pese sua dificuldade, a elaboração de respostas jurídico-penais uniformes a serem dadas pelas diferentes jurisdições.

3.1 TRATAMENTO MATERIAL DOS CRIMES INTERNACIONAIS DE LAVAGEM DE DINHEIRO

É nesse contexto que há a adesão, pelo Estado brasileiro, às convenções internacionais que tratam da lavagem de capital. A primeira foi a Convenção contra o Tráfico Ilícito de Entorpecentes e de Substâncias Psicotrópicas, de Viena, lavrada no ano de 1988 e ratificada pelo Brasil em 1991[6]. Ali foi reconhecido o caráter transnacional do delito, disparado o alerta quanto aos valores provenientes do tráfico de

6 Por meio do Decreto n. 154/1991.

entorpecentes e definidos os elementos típicos da lavagem de dinheiro, além de elaboradas medidas de confisco, abertura de sigilo bancário e cooperação entre seus integrantes. O evento coliga-se à primeira geração de leis de lavagem de dinheiro, que tinham no tráfico e seu exaurimento financeiro, agora perseguido autonomamente, em tipo de injusto próprio, o centro da preocupação.

Em 1999, ocorreu a Convenção de Palermo, internalizada pelo Brasil em 2004[7]. Essa apresenta aplicabilidade mais ampla do que a anterior, já que passa a considerar, como delito antecedente, além do tráfico de substâncias entorpecentes, a participação em grupo criminoso, a corrupção e a obstrução da justiça. Prevê-se, ainda, a possibilidade da persecução penal baseada em crimes antecedentes praticados em outros países, desde que respeitado o princípio da dupla incriminação (CALLEGARI; WEBER, 2014, p. 63).

A Convenção de Estrasburgo, considerada de segunda geração das leis Antilavagem de Dinheiro (doravante, ALD), ampliou o rol dos crimes antecedentes. De fato, essa geração caracteriza-se exatamente por esse aspecto, abandonando o foco no exclusivo combate à vantagem econômica angariada com tráfico de drogas. Embora o Brasil não seja um de seus signatários[8], foi por ela influenciada (OLIVEIRA, 2018, p. 16). Em verdade, o país adotou um critério de terceira geração quando passou, em 2012, a dispensar um rol taxativo de crimes antecedentes que permitiriam a subsunção típica da lavagem das respectivas vantagens financeiras.

Por fim, a Convenção de Mérida, ou Convenção das Nações Unidas contra a Corrupção, especifica que as medidas devem sempre ser

7 Através do Decreto n. 5.015/2004.

8 Pactuado somente no âmbito da União Europeia, mas que possui adesão de Estados externos a esse grupo, como EUA, Canadá e Austrália.

atualizadas e aprimoradas por novas frentes internacionais de combate à lavagem, o que não torna cada acordo internacional um novo procedimento de combate à lavagem, mas meio para o aperfeiçoamento de métodos já adotados pelos Estados (OLIVEIRA, 2018, p. 17).

Ainda nesse contexto, indispensável citar o Grupo de Ação Financeira Internacional (Gafi), instituído no ano de 1989 pelo G7, fruto da 15ª Reunião Anual ocorrida na cidade de Paris. Na ocasião, os Estados participantes se comprometeram a estabelecer cooperação internacional no combate ao tráfico de entorpecentes, lavagem de capitais, terrorismo e meio ambiente. O Gafi é reconhecido atualmente como o principal órgão no sistema internacional para direção de políticas ALD (CORDERO, 2002, p. 158-159). É composto por 39 membros (FATF, 2020) e atua na elaboração de padrões internacionais, monitoração do grau de cumplicidade dos países e financiamento de pesquisas quanto ao tema. Por ser um organismo intergovernamental, suas recomendações têm caráter não cogente, de *soft law*.

De fato, o Gafi busca assessorar e ditar recomendações, mas não dispõe da mesma capacidade sancionadora do ordenamento jurídico interno. Bem assim, não tem força vinculante típica de tratados ou convenções internacionais. Os padrões definidos pelo Gafi, mediante recomendações, devem ser adotados pelos países, implicando a omissão na inscrição em uma lista pública de Estados *não cooperantes.* Essa condição dificulta o relacionamento econômico com aqueles que observam as recomendações (ALEXANDER, 2001, p. 240-242). Aí reside o mencionado caráter de *soft law* das recomendações, bastante eficaz no ambiente de *lex mercatoria* mundializada.

3.2 A LAVAGEM DE DINHEIRO TRANSNACIONAL E A QUESTÃO DA LEI PENAL NO ESPAÇO

Nessa trajetória, pode-se perceber que os riscos da lavagem de dinheiro praticada por organizações criminosas transnacionais foram, de certa forma, mitigados no Brasil, *pari passu* à adoção de uma legislação nacional simétrica às políticas internacionais ALD. O país conta com a possibilidade de investigar e processar dentro da sua jurisdição qualquer ato de ocultação, dissimulação ou integração de dinheiro proveniente de atividade ilícita, ainda que o delito antecedente tenha sido realizado fora das fronteiras nacionais[9].

Como salientado, o Código Penal Brasileiro (CP) adota, em detrimento da teoria do resultado ou da ação, a teoria da ubiquidade para definição do local do crime (art. 6º, CP). Assim, se o ato ou o resultado tiver ocorrido em território nacional, integral ou parcialmente, afirma-se o Brasil como *locus* delitivo, autorizando-se a aplicação da lei brasileira e, *ipso facto*, sua jurisdição, pelo princípio da territorialidade (art. 5º, CP). Assim, o país fará a persecução penal de delitos segundo o critério de que tenham sido cometidos no seu território, ou seja, prepondera a noção de território jurídico a tais efeitos. Trata-se de concepção mais extensa que aquela de território físico, abrangendo os chamados territórios por extensão – art. 5º, § 1º, CP –, além de espaço aéreo e mar territorial – art. 5º, § 2º, CP.

Ademais, mesmo se cometidos fora do território brasileiro, alguns delitos podem ser regidos pela lei nacional. Basta que incidam as hipóteses de extraterritorialidade do art. 7º do CP. Para a lavagem, avulta certamente a letra do art. 7º, II, *a*, CP. Acaso o Brasil se obrigue, por convenção internacional[10], a reprimir o delito praticado em território

9 Desde que seja respeitado o critério da dupla incriminação.

10 No caso dos delitos de lavagem de dinheiro, esse comprometimento decorre da Convenção das Nações Unidas contra a Corrupção (Convenção de Mérida), adotada

estrangeiro, poderá persegui-lo, enquanto nação engajada no esforço globalizado do respectivo combate. O art. 7º, II, *a*, CP, adota o critério de extraterritorialidade denominado usualmente como princípio da universalidade da jurisdição penal, da justiça penal internacional, do direito penal internacional, entre outros sinônimos. Por ele, as nações se concertam num esforço mútuo de apoio para combater dadas espécies delitivas muito graves, a ponto de exigirem comunhão de esforços. Nesse caso, não será preciso detectar ação ou resultado, total ou parcial, no Brasil, atinente a um delito concretamente identificado de lavagem. Os critérios de extraterritorialidade são, afinal, categorias de exceção em relação ao princípio da territorialidade.

Repare-se, porém, que se trata de hipótese de extraterritorialidade condicionada (art. 7º, II, CP). Portanto, a persecução estará condicionada a que: (i) o agente esteja em território nacional; (ii) seja respeitado o critério da dupla incriminação; (iii) a lei autorize a extradição por lavagem, nos marcos do art. 82 da Lei de Migração, n. 13.445/2017; (iv) o agente não tenha sido absolvido no estrangeiro ou não tenha lá cumprido pena; bem como (v) não tenha sido perdoado no exterior ou esteja extinta sua punibilidade. São as condições do art. 7º, § 2º, CP.

Ocorre, entretanto, que, enquanto há preocupação para que os crimes internacionais de lavagem de dinheiro sejam adequadamente investigados e punidos, independentemente do local em que tenham ocorrido, desde que respeitados os citados critérios de extraterritorialidade, ou cuja ação ou o resultado tenha tocado o território nacional, inexiste norma clara quanto à solução de eventuais múltiplos processos, caso o

---

pela Assembleia Geral das Nações Unidas em 31 de outubro de 2003. O Brasil a incorporou ao seu ordenamento jurídico no ano de 2006, com a publicação do Decreto n. 5.687/2006. No art. 42, estão previstos os critérios de jurisdição ratificados, devendo-se atentar para o 42.4.

fato tenha sido praticado em diferentes países. Esse quadro, reprise-se, tende a ocorrer mais frequentemente com a evolução dos delitos informáticos, suscitando a necessidade de harmonizar-se com a máxima do *ne bis in idem*.

O art. 8º do CP brasileiro constitui norma que busca remediar aspectos do problema da múltipla incriminação. Diante da possibilidade de um sujeito ser processado por crime pelo qual já foi condenado e cumpriu pena em outro país, o dispositivo prevê que, acaso condenado também em território brasileiro, haverá compensação de penas, se iguais, ou atenuação da aplicada aqui, se distintas. Ou seja, nosso Código Penal conta expressamente com a possibilidade de litispendências internacionais, mitigando a consequência derivada da violação da vedação de duplo processamento pelo mesmo fato.

A controvérsia ficou bem exemplificada em decisão, por maioria de votos, do Superior Tribunal de Justiça (STJ), nos autos do RHC n. 78.684/SP. Com a impetração do *habeas corpus*, pretendia-se o trancamento de um processo criminal contra réu acusado, perante a jurisdição brasileira, de crime de lavagem de dinheiro pelo qual havia sido condenado pela Justiça da Suécia, em conexão com o crime antecedente de tráfico de substâncias entorpecentes. Inclusive, havia cumprido integralmente a pena naquele país. Dois votos, fundamentados no Pacto Internacional sobre Direitos Civis e Políticos[11] e na Convenção Americana sobre Direitos Humanos[12], afirmaram tratar-se de *bis in idem*.

---

11 Pacto Internacional sobre Direitos Civis e Políticos, art. 14, n. 7: "Ninguém poderá ser processado ou punido por um delito pelo qual já foi absolvido ou condenado por sentença passada em julgado, em conformidade com a lei e os procedimentos penais de cada país."

12 Convenção Americana de Direitos Humanos, art. 8º, n. 4: "O acusado absolvido por sentença passada em julgado não poderá ser submetido a novo processo pelos mesmos fatos".

Porém, sagrou-se vencedor, por três votos, o entendimento da validade da solução interna contida no CP, fundada no art. 8º, reconhecendo-se a pena cumprida no exterior como mera hipótese de atenuação. Foram rechaçados os citados dispositivos internacionais sob o fundamento de que estariam relacionadas tão somente à impossibilidade de múltiplos processos em uma mesma jurisdição, não em jurisdições diferentes, o que ofenderia o Princípio da Soberania do Estado (STJ, 2019).

4. TENDÊNCIA DE MULTIPLICIDADE DE PROCESSOS NOS CRIMES INFORMÁTICOS DE LAVAGEM DE DINHEIRO

Esse entendimento talvez coloque em evidência certo descompasso entre o critério da ubiquidade e os delitos informáticos.

A noção de ubiquidade concerne àquilo que está em todos os lugares. Na teologia, indica um dos atributos divinos. Em direito penal, a adoção desse critério tem o propósito de evitar a impunidade de uma conduta criminosa, substituindo critérios mais restritivos para definir o lugar do crime, calcados no local da ação ou do resultado. Na possibilidade de adotar-se o critério da ação em um país e do resultado em outro, e dando-se respectivamente o resultado naquele e a ação neste, o crime plurilocal – pelos modelos legais envolvidos – poderia ser reputado como não praticado no território de nenhum dos países. Abre-se um correlato risco de impunidade. Para neutralizá-lo, evitando-se situações similares em crimes plurilocais (em que a ação ou parte dela ocorre num país e o resultado ou parte dele noutro), adota-se nos códigos a ubiquidade (por todos, novamente, HUNGRIA, 2017, p. 108).

Trata-se de critério pensado na perspectiva de que o delito se realiza em um lugar físico ou geográfico, próprio de códigos penais anteriores à reviravolta provocada pela internet no âmbito das comunicações e, pois, trocas financeiras. Em crimes tradicionais, realizados no espaço

físico, o ato praticado em âmbito plurilocal ou à distância não costuma envolver inúmeros países. De modo geral, implica estados nacionais que fazem fronteiras entre si.

Porém, com os avanços tecnológicos e a tendência de aumento da prática de crimes informáticos impróprios, o *locus* do delito é o meio ambiente digital, contínuo e sem fronteiras. Ele ocorre em todos os locais, substituída a concepção física de território pela digital estendida. E, nessa quadra, pode desatar um sem-fim de jurisdições, como expressão do poder soberano de vários países. Projeta-se a proliferação das litispendências internacionais.

4.1 DIFICULDADES ADVINDAS DO MEIO AMBIENTE DIGITAL

Segundo Flores Prada (2015, p. 7), as redes digitais apresentam três grandes dificuldades para sua regulação no âmbito internacional: (i) a *universalidade*, por se tratar de uma tecnologia que não reconhece fronteiras, cuja conexão em um local permite ao usuário acessar todo o seu acervo e tudo que com ela se conecte, em qualquer ponto do globo terrestre; (ii) a *horizontalidade*, eis que o acesso ocorre de maneira descentralizada, bem como (iii) a *dependência técnica*, representada pelo modo como o ambiente virtual é desenvolvido, por meio de tecnologias que facilitem a regulação e investigação, ou que criem barreiras intransponíveis (por exemplo, a criptografia de dados).

Tais características se transportam para o delito de lavagem de dinheiro, devido à facilidade de conversão de bens, valores e direitos obtidos ilicitamente em criptomoedas: dados computacionais criptografados capazes de representar valor econômico, cujo envio pode ocorrer de maneira instantânea, para qualquer ponto do mundo (universalidade) e sem depender de instituições financeiras intermediadoras (horizontalidade) (DESCÔTEAUX, 2014).

Quanto à dependência técnica, as formas como essas transações podem ser realizadas modificaram-se sensivelmente ao longo do tempo. O método pensado pelo criador do *Bitcoin* fora possibilitar transações eletrônicas entre duas pessoas, chamadas de *ponto a ponto* (*peer-to--peer*). Algo que se assemelhasse à entrega de moeda em espécie[13], mas de maneira eletrônica e sem necessitar de intermediários (NAKAMOTO, 2008). Entretanto, o aumento de interessados em adquirir *bitcoins* trouxe ao mercado não somente aqueles que desejavam realizar o envio de valores mas também profissionais da área financeira com objetivo de desenvolver atividades empresariais. Com isso, novas possibilidades para realização das transações foram criadas.

Para compreender essa dinâmica, é necessário explicar, brevemente, o funcionamento do sistema *Bitcoin*.

Tanto as transações eletrônicas tradicionais quanto as realizadas com criptomoedas necessitam de intermediários. Naturalmente, uma transferência eletrônica não envolve a alteração do local físico em que o dinheiro se encontra. É somente o envio de um comando para alteração de uma informação armazenada em um banco de dados.

Assim sendo, há uma característica intrínseca a qualquer informação computacional que a impede de, sem a existência de intermediários, funcionar como dinheiro: a possibilidade de que múltiplas cópias do mesmo dado sejam realizadas (*double-spending problem*) (CHOHAN, 2017, p. 2-8). O mesmo ocorre, por exemplo, com o envio de um arquivo por *e-mail*, o qual, mesmo após recebido pelo destinatário, continua disponível no computador do remetente.

---

13 Aliás, o *whitepaper* publicado por Satoshi Nakamoto (pseudônimo utilizado para manter o anonimato do criador) afirma ser o *Bitcoin* um "*peer-to-peer electronic cash system*". Os termos "*cash*" e "*money*" são utilizados em contextos distintos na língua inglesa. Aquele não se refere a dinheiro circulante no sistema financeiro, mas somente a moeda em papel, que circula diretamente entre as pessoas.

Para solucionar essa dificuldade, é imprescindível que alguém confira se há saldo disponível e, sobretudo, debite o valor antes de remetê-lo a outrem. Essa tarefa, até o surgimento do *Bitcoin*, era desempenhada por um ente centralizado, geralmente o provedor do sistema de pagamento. No caso dos sistemas financeiros tradicionais, pelo banco que intermedeia o serviço de transferências.

Com o *Bitcoin*, essa dificuldade técnica foi solucionada de maneira distinta. Em vez de um único ente responsável pela verificação das informações, há um incontável número de pessoas que, organizadas na internet, oferecem força computacional (*hardwares*) para servir como pontos verificadores das transações eletrônicas (*Bitcoin nodes*). Quando se realiza uma transação, a informação é enviada a diversos computadores espalhados ao redor do mundo, que verificam concomitantemente a validade da operação. Se, para a maioria deles (50% mais um), a informação estiver correta, a transação é gravada em um grande livro-razão. Esse é o sistema de funcionamento do *blockchain*.

As informações gravadas no *blockchain* são totalmente públicas e irreversíveis. Assim, diferentemente do dinheiro em espécie, é possível a qualquer pessoa verificar todo o caminho percorrido por um *bitcoin* desde o momento de seu surgimento (mineração). No entanto, não há quebra massiva do sigilo das transações. O *blockchain* não armazena dados do usuário, somente os *endereços* (de origem e destino) do *bitcoin* e a quantidade enviada.

Não é possível, em um primeiro momento, atribuir o *endereço* de um *bitcoin* a um usuário. Entretanto, com o uso de ferramentas de investigação, essa realidade se inverte. É possível, por exemplo, descobrir o *internet protocol* (IP) de quem realizou a transação e, com isso, requisitar informações ao provedor de internet. Ainda que o autor tenha mascarado o IP por meio de sistemas como VNP ou TOR, é possível realizar a análise de todos os dados disponibilizados na rede no momento em que realizada a operação e, com isso, fazer um cruzamento de informações (*cluster analysis*).

Assim, entende-se que as transações com *bitcoins* não são anônimas, mas pseudoanônimas. O pseudoanonimato é um processo por meio do qual os dados são armazenados de maneira que não podem ser atribuídos inicialmente a determinada pessoa, exceto com o uso de informação adicional. Enquanto o anonimato é irreversível, o pseudoanonimato não é (CHA, 2018, p. 4-5).

Ainda que as transações com *bitcoins* não sejam anônimas, há maior facilidade para quem pretende movimentar dinheiro ilícito. Por não necessitar de um terceiro que realize a conferência das transações de maneira centralizada, o Estado não tem a quem endereçar regulações para mitigar os riscos de lavagem de dinheiro, especialmente de exigir a realização de procedimentos de *conhecimento do usuário* (*Know Your Customer* – KYC).

Entretanto, esse inédito modo de realizar transações financeiras também possui suas dificuldades. No caso, a falta de confiança. Ainda que seja possível enviar valores a qualquer ponto do mundo sem necessidade de uma instituição financeira intermediária, é extremamente difícil localizar pessoas que desejem negociar criptomoedas. Mesmo que se consiga, inexiste um método eficaz de garantir a segurança da operação. Para uma pessoa adquirir *bitcoins* com reais, por exemplo, restariam duas alternativas: (a) encontrar pessoalmente o sujeito que pretende vender, ou (b) realizar uma transferência da própria conta bancária à do vendedor, sem garantias de que, uma vez enviados, os *bitcoins* serão remetidos.

Diante desse problema, elaboraram-se algumas soluções. As mais relevantes são as *plataformas de troca* e as *casas de câmbio de criptomoedas*, adiante chamadas de *Exchanges Centralizadas*.

As *plataformas de troca* são aplicações que permitem aproximar interessados na compra, venda ou troca de criptomoedas. Os anúncios são dispostos publicamente em *sites*, geralmente separados por cidade ou região, havendo um sistema de pontuação para aferir a confiabilidade de cada usuário. Esse método permite duas possibilidades: (a) identificar

pessoas confiáveis para realizar a transação de maneira virtual, ou (b) encontrar pessoas próximas, para promover o encontro presencial.

Ainda que esse sistema facilite as transações, seu método de operação é limitado na medida em que exige um comportamento ativo dos usuários.

Como alternativa de mais fácil uso, surgiram as *Exchanges Centralizadas*. Seu modo de funcionamento é bastante semelhante ao das casas de câmbio tradicionais. Elas se colocam como intermediadoras no processo de troca de moeda circulante por criptomoedas, ou exclusivamente entre criptomoedas, oferecendo ao usuário uma alternativa fácil e segura para realizar a conversão. Em vez de haver a necessidade de procurar uma pessoa, basta ir a essa *Exchange* e realizar a compra ou venda de maneira direta.

Com o ingresso desses intermediadores no mercado, houve um processo de recentralização. Devido à facilidade e à segurança, os usuários passaram a preferir adquirir seus *bitcoins* diretamente dali, o que tornou expressivo o volume de negociações.

Isso alertou os Estados quanto à oportunidade de regular o ambiente das criptomoedas. O método adotado se baseou em tratar esses intermediários de maneira semelhante às instituições financeiras. Nesse sentido, o Gafi passou a recomendar aos Estados que exijam de todos os *Provedores de Serviços de Ativos Virtuais*[14] (*Virtual Asset Service Provider – VASPs*) a autorização para funcionamento[15], o armazena-

14 Esse termo engloba toda pessoa física ou jurídica que se proponha a realizar a conversão de moedas circulantes por criptomoedas, a troca, o armazenamento, a transferência ou a administração. Ou seja, nesse gênero estão inclusas as *Exchanges*, as plataformas de troca, os provedores de carteiras e qualquer outro agente intermediador de transações que envolvam esse ambiente.

15 Os países deveriam designar uma ou mais autoridade para ser responsável pelo *licenciamento ou registro* dos VASPs, os quais deverão requerer tais habilitações

mento de informações[16] e a notificação de transações suspeitas[17] (FATF, 2019, p. 59).

Entre as recomendações, a que apresenta maior efeito para fins de combate à lavagem de dinheiro são os procedimentos de KYC. Devido à natureza pública do *blockchain*, é possível saber o momento exato em que a criptomoeda passou por uma *Exchange Centralizada*. Isso permite ao Estado requerer informações acerca do usuário que realizou determinada transação suspeita.

Entretanto, como premissa da Quarta Revolução Industrial, todo modelo econômico centralizado será pressionado por iniciativas descentralizadoras (VIGNA, CASSEY, 2016, p. 140-145). Isso não foi diferente com as *Exchanges Centralizadas*. Devido ao avanço das tecnologias de criptografia, especificamente dos *contratos inteligentes* (*smart contracts*), surgiram as *Exchanges Descentralizadas* (ou *Decentralized Exchanges* – DEX).

Diferentemente das primeiras, estas não promovem interação entre o mercado de criptomoedas e as moedas circulantes, servem exclusiva-

---

dentro das jurisdições que foram criadas. Essas autoridades deverão impor condições para permitir adequada supervisão, bem como tomar medidas ou criar mecanismos para identificar a pessoa, física ou jurídica, que atue como VASP sem o devido registro ou licença, aplicando-lhe sanções.

16 Foi recomendado o *Due Diligence* para que os VASPs, enquanto entidades obrigadas, identifiquem as pessoas envolvidas na transação e, quando aplicável, o beneficiário, além de verificarem, dentro do escopo de uma análise de risco, informações, dados ou documentos, para compreender os motivos e a natureza do negócio pactuado entre as partes, e verificar informações que possam sugerir o alto risco de eventual transação para fins ALD.

17 Informações relevantes em transações que ultrapassassem USD/EUR 1.000 deveriam ser coletadas, bem como diligenciadas transações com "ativos virtuais" através de serviços, transações ou canais de entrega pseudoanônimas, tais como transações anônimas, para identificar o endereço de IP e os números dos documentos dos envolvidos.

mente para troca de uma criptomoeda por outra. Também de maneira distinta, não concentram em si as transações, somente realizam, de maneira automática e programada em um código computacional, a aproximação de interessados em realizar trocas. Uma vez localizada pessoa que queira vender e outra que pretenda comprar, a transação ocorre fora da esfera de controle da *Exchange*, de maneira *peer-to-peer*.

Mesmo nessa hipótese, inexiste o mencionado problema do déficit de confiança. A solução decorre do uso de um *contrato inteligente* (*smart contract*), um código computacional que opera de maneira automática e permite que transações *peer-to-peer*, mesmo a distância e sem que os usuários se conheçam, ocorram de maneira segura. Seu funcionamento se assemelha ao de um intermediário, mas que, no caso, é um código computacional. As duas partes remetem suas criptomoedas para dentro de um *smart contract*, ficando lá *trancadas*. Assim que os parâmetros programados são verificados (no caso, quando ambas as partes enviam o montante combinado) ele se autoexecuta, realizando a troca de maneira automática e segura. Não há a necessidade de confiar na pessoa, somente no código.

A multiplicação do número de modelos de intermediadores no mercado possibilita novas formas e locais em que o crime de lavagem de dinheiro possa vir a ocorrer. Além disso, os agentes dessa modalidade criminosa preferem utilizar provedores de serviços localizados em países que pouco se comprometem com os padrões internacionais de combate à lavagem de dinheiro (SWIFT, 2020), especialmente os que não exigem procedimentos de KYC. Segundo estimativa do *CipherTrace* (2020), 56% dos *Provedores de Serviços de Ativos Virtuais* (VASPs) no mundo executam procedimentos de KYC precários. No continente africano, esse número alcança 72%. Entende-se, portanto, que existe uma propensão para a formação de paraísos fiscais digitais.

Ainda que haja essa realidade, a tendência é os Estados exigirem que as *Exchanges* adotem medidas de combate à lavagem de dinheiro.

Entretanto, é prudente mencionar que existem *Exchanges Descentralizadas* que operam de maneira totalmente autônoma. É o caso da *UniSwap*. Assim como o *Bitcoin*, ela foi criada por uma pessoa (dessa vez identificável), mas não é controlada por ela ou qualquer entidade. Trata-se de um código aberto e em pleno funcionamento, que permite a qualquer um trocar, através de um *smart contract*, uma criptomoeda por outra[18]. Todo o lucro advindo dessa operação é revertido a quem decide cooperar para o funcionamento do sistema. Essas pessoas ocupam a função de *provedores de liquidez* (*liquidity provider*).

Nessa hipótese, o Estado não tem a quem endereçar sua regulação. Inexiste uma empresa ou uma pessoa responsável por essa *Exchange Descentralizada*. Ainda assim, esse risco deve ser contrabalanceado com o fato de que nelas não é possível converter criptomoedas em moedas circulantes. Logo, se o sujeito do crime de lavagem pretender converter esses valores em reais, por exemplo, terá de passar por uma *Exchange Centralizada* – a qual realiza procedimentos de KYC –, ou realizar outros procedimentos de maior complexidade (que, consequentemente, dificultam a movimentação de quantias expressivas).

Somado a esse risco, existem criptomoedas com mecanismos de acréscimo de anonimato. São as chamadas *privacy coins* – como o caso da Monero –, cujo *blockchain* é visível exclusivamente ao sujeito que realizou a transação[19], caso cedida voluntariamente, ou descoberta pelo Estado por meio de mecanismos de investigação ainda inexistentes (SYRACUSE; BOEHM; LUNDGREN, 2020, p. 6-14). Aliado às *Exchanges Descentra-*

---

18 Há que ser dito, entretanto, que os sistemas que operam os *smart contracts* são atualmente incompatíveis com o *blockchain* do *Bitcoin*. Eles operam principalmente no *blockchain* da *Ethereum*, mas, mesmo assim, permitem que sejam realizadas transações entre criptomoedas que operam em diferentes *blockchains*. O meio de fazer isso é através de um protocolo de *smart contract* chamado *atomic swap*.

19 Uma *chave privada* garante o sigilo.

lizadas, há possibilidade de troca de criptomoedas de *blockchain* público por *privacy coins* (GRUGGER, 2020, p. 1-7) sem procedimentos de KYC, aumentando ainda mais as hipóteses de ocultação de patrimônio ilícito.

O desenvolvimento do mercado das criptomoedas se apresenta, portanto, como um novo risco. Na medida em que a movimentação do dinheiro oriundo de atividades ilícitas dá-se literalmente ao redor do mundo, realizando-se com o auxílio de tecnologias que permitem – ou incrementam – o anonimato dessas transações, há maior facilidade nas fases de ocultação e dissimulação da lavagem. Além disso, o aumento na popularidade do respectivo uso e incremento da adoção dentro das atividades econômicas lícitas poderá facilitar, também, a etapa da lavagem consistente na integração (SOUZA; COELHO, 2015, p. 52).

As transações com cibermoedas são praticadas em sistemas que permitem conexões instantâneas e globais, que não possuem referência evidente a um local físico, através de servidores, provedores, conexões e informações localizados em qualquer ponto do mundo, ou em vários deles (FLORES PRADA, 2015, p. 10). É o caso dos VASPs, que poderão estar localizados em países menos eficientes do ponto de vista regulatório, enquanto os lavadores poderão estar em qualquer outro local físico. Nos crimes informáticos de lavagem de dinheiro, serão raros os casos que afetarão uma única jurisdição.

Com isso, o princípio da territorialidade em matéria penal, enganchado em nosso país à teoria da ubiquidade, produz a seguinte reverberação: todo delito de lavagem com recursos convertidos em moeda digital tocará o país, ao passo que, simultaneamente, tange a todos os outros territórios (GUARAGNI; RIOS, 2019, p. 173-175). De forma mais simples: toda ação no meio digital toca todo o ambiente, inclusive uma prática de lavagem, em que o proveito ilícito é convertido em dado digital.

Mesmo assim, inexistem normas internacionais aptas a solucionar, com precisão, eventuais conflitos positivos de competência internacional para processar e julgar crimes informáticos de lavagem de dinheiro.

O Pacto Internacional sobre Direitos Civis e Políticos e a Convenção Americana sobre Direitos Humanos, conquanto afirmem a impossibilidade de o sujeito ser processado criminalmente duas vezes pelo mesmo ato, podem ser entendidos pelos tribunais como regramentos internacionais que se referem exclusivamente à vedação de múltiplos processos em uma mesma jurisdição. São, assim, insuficientes para tratar o cúmulo de jurisdições de diversos países.

4.2 POSSÍVEIS SOLUÇÕES PARA O PROBLEMA

Uma solução pode ser encontrada na Convenção de Estrasburgo sobre o Cibercrime (2001). Nela há expressa sugestão quanto aos delitos que tocam múltiplas jurisdições. O art. 22, item 5, define, por exemplo, que, caso mais de uma reivindique a competência de determinado crime informático, deverá ser estabelecido diálogo para a solução do conflito. A passagem traz à memória a sugestão de Hungria, que anteviu o problema do *bis in idem* suscitado pela ideia de ubiquidade e sugeriu "o recurso aos tratados internacionais" (2017, p. 108) como solução.

No âmbito do uso de sistemas autocompositivos entre os Estados para solucionar os conflitos de competência e determinar a jurisdição ideal, Flores Prada (2015) sugere critérios para dirimi-los, afirmando a necessidade de ser observado (i) o local onde ocorrido o crime, especialmente aquele cometido por meio de sistemas informáticos cujos suportes físicos se encontrem em determinado território nacional, independentemente do lugar no qual o autor se encontre fisicamente, (ii) a nacionalidade do autor do fato, (iii) a nacionalidade da vítima, (iv) os interesses afetados de determinada nação, (v) ou cometidos em benefício de pessoa coletiva com sede em qualquer Estado signatário do acordo.

Exceto o primeiro critério, os demais são reproduções de tradicionais mecanismos que autorizam o emprego da lei de um país a crimes

cometidos fora dele. Inclusive, a nacionalidade, ativa ou passiva, é adotada pelo CP brasileiro (art. 7º, II, *a*, e § 3º). O critério do interesse converge para a defesa ou proteção de bens jurídicos, presente no Código brasileiro, mais especificamente no art. 7º, I, incisos *a*, *b* e *c*. Essa coincidência sugere a conclusão de que o meio ambiente digital aparece, na Convenção, como assimilado à noção de território externo e distinto do território estatal de referência. O texto convencional, assim, contraria a percepção do meio ambiente digital como um local contínuo, unificado, indistinto e sem fronteiras.

O mesmo autor ainda entende ser necessário observar as características do delito, tais como a dinâmica da conduta e a participação dos agentes. Nos crimes informáticos de lavagem de dinheiro, a exclusiva constatação da ocultação ou da dissimulação dos valores de proveniência ilícita permite afirmar a aplicação da lei do país onde o agente controla ou coordena o comportamento, ou onde se localiza a decisão da ação.

Nos casos em que houver integração do dinheiro ilícito, aplicar-se-á a teoria da ubiquidade e, em sendo diferentes os locais da ação e do resultado, por inexistirem normativos rígidos de preferência, deve haver diálogo no qual se priorize o local (i) de maior facilidade para a investigação, (ii) onde o resultado ofereça uma referência territorial clara e, em caso de pluralidade, apresente maior resultado, e (iii) onde o autor seja detido. Nesse critério, a definição da lei materialmente cabível evoca a ideia de prevenção, que tradicionalmente serve para firmar não a lei material aplicável ao crime, mas a competência jurisdicional.

5. CONCLUSÃO

Percebe-se que a integração dos meios físico e digital derivada da Quarta Revolução Industrial permite prospectar a conversão em regra de crimes que hoje, só eventualmente, ocorrem em múltiplas

nacionalidades. A cooperação internacional avançou de forma relevante no campo da assistência judiciária e policial, permitindo melhor combate de delitos transnacionais. Não obstante, inexistem normas internacionais eficazes para estabelecer a competência territorial no caso de afirmarem-se válidas, para um delito concreto, leis materiais de vários países, refletindo em litispendências internacionais (FLORES PRADA, 2015).

O caráter transnacional da criminalidade moderna, alavancada pelos meios tecnológicos, torna problemático o uso do princípio da territorialidade, enganchado na teoria da ubiquidade, para definir qual será o Estado cuja lei material será aplicável ao delito informático impróprio. Afinal, quando cometido no meio ambiente digital, enquanto esfera una, estendida, contínua e sem fronteiras, o crime acaba por tocar todos os locais simultaneamente, em espécie de *omnilocalidade*. Essa situação insta o acionamento de múltiplas jurisdições para processar e julgar o mesmo ato.

A questão releva, especialmente, para os crimes informáticos impróprios de lavagem de dinheiro, a partir do emprego de moedas digitais como mecanismos de ocultação e dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, valores e direitos oriundos de crimes.

Podem-se prospectar soluções pela via dos critérios previstos na Convenção dos Crimes Cibernéticos de Budapeste, no âmbito supranacional, com internalização uniforme pelos países signatários – note-se que o Brasil não o é (OLIVEIRA, 2018).

Enfim, se de um lado são necessários atos de cooperação jurídica internacional para permitir a investigação, persecução e punição dos crimes transnacionais, de outro, é preciso que sejam adotados critérios para se resolverem conflitos positivos de competência internacional. Nas hipóteses de litispendência internacional, mostra-se promissora a adoção de acordos plurinacionais para reconhecimento de decisões judiciais e categorias prévias idôneas à definição da normativa material a ser empregada.

REFERÊNCIAS

ALESSANDRI, Alberto. *Diritto penale e attività economiche*. Bologna: Il Mulino, 2010.

BADARÓ, Gustavo Henrique. *Lavagem de dinheiro*: aspectos penais e processuais penais: comentários à Lei n. 9.313/1998, com as alterações da Lei n. 12.683/2012. 3. ed. São Paulo: Revistas dos Tribunais, 2016.

BAUMAN, Zygmunt. *44 cartas do mundo líquido moderno*. São Paulo: Schwarcz-Companhia das Letras, 2011.

BERGREEN, Laurence. *Além do fim do mundo*. Rio de Janeiro: Objetiva, 2004.

BORJA JIMÉNEZ, Emiliano. *Globalización y concepciones del derecho penal*. 2009. Disponível em: https://minerva.usc.es/xmlui/handle/10347/4146. Acesso em: 23 set. 2020.

BRASIL. Superior Tribunal de Justiça. *Recurso Ordinário em Habeas Corpus n. 78.684/SP*. Relator: Ministro Joel Ilan Paciornik. Brasília, 4 dez. 2018. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201603089560&dt_publicacao=08/02/2019. Acesso em: 24 set. 2020.

CALLEGARI, André Luís; WEBER, Ariel Barazzetti. *Lavagem de dinheiro*. São Paulo: Atlas, 2014.

CHA, Shi-Cho *et al*. Privacy enhancing technologies in the Internet of Things: Perspectives and challenges. *IEEE Internet of Things Journal*, v. 6, n. 2, 2018, p. 2159-2187. Disponível em: https://ieeexplore.ieee.org/abstract/document/8515008/. Acesso em: 5 out. 2020.

CHOHAN, Usman W. The double spending problem and cryptocurren-

cies. *SSRN*, 23 dez. 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174. Acesso em: 5 out. 2020.

CIPHERTRACE, 2020. Disponível em: https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/. Acesso em: 5 out. 2020.

COINGENCKO. *Binance*. Coingenko, 2020. Disponível em: https://www.coingecko.com/en/exchanges/binance. Acesso em: 2 out. 2020.).

CONVENÇÃO sobre o cibercrime. Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 24 set. 2020.

CORDERO, Isidoro Blanco. *El delito de blanqueo de capitales*. 2. ed. Navarra: Aranzadi, 2002.

LIMA, Vinicius de Melo. A internacionalização do direito penal e a persecução ao financiamento do terrorismo. *Revista do Ministério Público do Rio Grande do Sul*, 2013. Disponível em: http://www.amprs.org.br/arquivos/revista_artigo/arquivo_1401214594.pdf. Acesso em: 24 set. 2020.

DESCÔTEAUX, David. *Bitcoin*: more than a currency, a potential for innovation. Montreal Economic Institute, 2014.

FATF. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,* FATF, 2019. Disponível em: www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html. Acesso em: 5 out. 2020.

FERWERDA, Joras. *The effects of money laundering*. Research handbook on money laundering. Edward Elgar Publishing, 2013. Disponível em: https://www.elgaronline.com/view/edcoll/9780857933997/9780857933997.00011.xml. Acesso em: 24 set. 2020.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. *Crimes no meio ambiente digital*. São Paulo: Saraiva, 2017.

FLORES PRADA, Ignacio. Prevención y solución de conflictos internacionales de jurisdicción en materia de ciberdelincuencia. *Revista Electrónica de Ciencia Penal y Criminología*, v. 17, 2015, p. 21. Disponível em: http://criminet.ugr.es/recpc/17/recpc17-21.pdf. Acesso em: 24 set. 2020.

FOLEY, Sean; KARLSEN, Jonathan R.; PUTNINŠ, Talis J. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, v. 32, n. 5, 2019, p. 1798-1853. Disponível em: https://academic.oup.com/rfs/article-abstract/32/5/1798/5427781. Acesso em: 24 set. 2020.

GUARAGNI, Fábio André; RIOS, Rodrigo Sánchez. Novas tendências de combate aos crimes cibernéticos: cooperação internacional e perspectivas na realidade brasileira contemporânea. *Revista de Estudos Criminais*, Porto Alegre, v. 18, n. 73, 2019, p. 167-196.

GUGGER, Joël. *Bitcoin-Monero Cross-chain Atomic Swap*. IACR, 2020. Disponível em: https://eprint.iacr.org/2020/1126.pdf. Acesso em: 5 out. 2020.

HUNGRIA, Nelson; DOTTI, René Ariel. *Comentários ao Código Penal*. 6. ed. Rio de Janeiro: GZ, 2017.

LIPINSKI, Victor Chemin Branco; COSTA, Daniel Tempski Ferreira da. A internacionalização do direito penal e a soberania do Estado. *Revista de Direito da FAE*, v. 1, n. 1, 2019, p. 142-172. Disponível em: https://revistadedireito.fae.edu/direito/article/view/40. Acesso em: 24 set. 2020.

MAGATTI, Mauro. *Cambio di paradigma*: Uscire dalla crisi pensando il futuro. Milano: Feltrinelli, 2017.

NAKAMOTO, Satoshi. *Bitcoin*: A peer-to-peer electronic cash system. Manubot, 2019. Disponível em: https://git.dhimmel.com/bitcoin-whitepaper/. Acesso em: 5 out. 2020.

OLIVEIRA, Marcus Vinícius Xavier de. A internacionalização do direito penal. Uma aproximação teórica a partir do crime de lavagem de capitais. *Quaestio Iuris*, v. 11, n. 1, 2018, p. 195-217. Disponível em: https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/26248. Acesso em: 24 set. 2020.

SÁNCHEZ, Jesús María Silva. *A expansão do direito penal*: aspectos da política criminal nas sociedades pós-industriais. 3. ed. Tradução de Luiz Otávio de Oliveira Rocha. São Paulo: Revista dos Tribunais, 2013. p. 80-81.

SCHWAB, Klaus. *A Quarta Revolução Industrial*. São Paulo: Edipro, 2016.

SOUZA, Arthur de Brito Gueiros; COELHO, Cecília Choeri da Silva. Questões atuais na prevenção da lavagem de dinheiro. *Revista Brasileira de Ciências Criminais*, 2020. RBCCrim 165.

STEINKO, Armando Fernández. Financial channels of money laundering in Spain. *British Journal of Criminology*, v. 52, n. 5, 2012, p. 908-931. Disponível em: https://academic.oup.com/bjc/article-abstract/52/5/908/470375. Acesso em: 24 set. 2020.

SWIFT. *Follow de money*: understanding the money laundering techniques that support large-scale cyber-heists. Bae Systems, 2020. Disponível em: https://www.swift.com/sites/default/files/files/swift_bae_report_Follow-The%20Money.pdf. Acesso em: 24 set. 2020.

SYRACUSE, Dana V; BOEHM, Joshua; LUNDGREN, Nick. *Anti-Money Laundering Regulation of Privacy-Enabling Cryptocurrencies*.

PerkinsCoie, 2020. Disponível em: https://www.perkinscoie.com/images/content/2/3/v7/237411/Perkins-Coie-LLP-White-Paper-AML-Regulation-of-Privacy-enablin.pdf. Acesso em: 5 out. 2020.

UNITED NATIONS. *Money Laundering*. 2020. Disponível em: https://www.unodc.org/unodc/en/money-laundering/index.html?ref=menuside. Acesso em: 24 set. 2020.

VIGNA, Paul; CASEY, Michael J. *The age of cryptocurrency*: how bitcoin and the blockchain are challenging the global economic order. São Paulo: Macmillan, 2016.

PROTEÇÃO DE DADOS PESSOAIS E CIBERCRIMES: A PROPOSTA DE UM BANCO DE DADOS DE POLICIAMENTO PREVENTIVO PARA A DISSEMINAÇÃO DE CONTEÚDOS ILÍCITOS NA INTERNET COM O EXEMPLO DA PORNOGRAFIA INFANTIL

Carolina Christofoletti[1]
Cíntia Rosa Pereira de Lima[2]
Kelvin Peroli[3]
Victor Gabriel Rodríguez[4]

RESUMO

Desde que o *software* Tor foi divulgado, em 2002, boa parte dos estudos sobre criminalidade cibernética tem se restringido à análise das

---

1 Graduada em Direito na Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo (USP), com experiência acadêmica na Albert Lüdwigs Freiburg Universität (Alemanha). Bolsista de mérito da USP para pesquisa de temas envolvendo pornografia infantil. Autora de artigos sobre Direito Penal Cibernético.

2 Pós-Doutora em Direito Civil na Università degli Studi di Camerino (Itália) com fomento Fapesp e Capes. Doutora em Direito Civil pela Faculdade de Direito da USP, com estágio na Ottawa University (Canadá) e bolsa Capes – PDEE. Doutorado sanduíche e Livre-Docente em Direito Civil Existencial e Patrimonial pela Faculdade

ocorrências que se dão em meio às chamadas *deep* e *dark web* (internet profunda e internet obscura). Todavia, os analistas se esquecem da regra de ouro dos criminosos: aliciar novos "parceiros" enquanto preservam o anonimato, a fim de não serem identificados pelas autoridades policiais. Nesse contexto, os clubes de pornografia infantil afiguram-se, em razão da concretude de seus materiais (que podem muito facilmente ser identificados por *softwares* de inteligência artificial e internautas vigilantes), como caso paradigma do que se pretende demonstrar. Uma vez que nem todo criminoso nasce *high-tech*, especialmente em países que ainda não sofreram a transformação digital, é coerente pressupor que as portas de entrada do submundo cibernético estejam escondidas

---

de Direito de Ribeirão Preto da USP. Professora de Direito Civil da Faculdade de Direito de Ribeirão Preto da USP. Líder e coordenadora dos grupos de pesquisa *Tutela Jurídica dos Dados Pessoais dos Usuários da Internet* e *Observatório do Marco Civil da Internet*, cadastrados no Diretório de Pesquisa do CNPq. Coordenadora do grupo de estudo *Tech Law*, do Instituto de Estudos Avançados da USP. Presidente do Instituto Avançado de Proteção de Dados (IAPD). Associada titular do Instituto Brasileiro de Responsabilidade Civil (IBERC). Membro fundador do Instituto Brasileiro de Direito Contratual (IBDCONT). Advogada.

3 Graduado em Direito na Faculdade de Direito de Ribeirão Preto da Universidade de São Paulo (USP), com experiência acadêmica na Seconda Università degli Studi di Napoli (Itália). Bolsista de mérito da USP. Membro dos grupos de pesquisa *Tutela Jurídica dos Dados Pessoais dos Usuários da Internet* e *Observatório do Marco Civil da Internet*, cadastrados no Diretório de Pesquisa do CNPq. Integrante do grupo de estudo *Tech Law*, do Instituto de Estudos Avançados da USP. Associado fundador do Instituto Avançado de Proteção de Dados (IAPD). Membro (desde a fundação) do Instituto Brasileiro de Direito Contratual (IBDCONT). Autor de livro e artigos sobre Direito Digital.

4 Professor Livre-Docente de Direito Penal da Faculdade de Direito de Ribeirão Preto da USP. Membro do Prolam/USP. Bolsista da Fundación Carolina (Espanha). Professor no mestrado da Universidad Católica de Bogotá (Colômbia). Foi professor convidado na Universidad de Valladolid e na Universidade de Granada (Espanha).

em fenômenos bastante sutis da internet aberta (*surface web*). Assim, o artigo dedica-se a iluminar a possível peça perdida do quebra-cabeça cibernético, com o exame das políticas adotadas pelos principais provedores de serviços de internet (PSI) do Brasil. A partir disso, sugere-se uma nova estratégia de policiamento preventivo, voltada a combater a criminalidade digital organizada, sustentada, conforme será demonstrado, pelo atual sistema de proteção de dados brasileiro. A relação proteção de dados e privacidade *versus* cibercriminalidade não constitui um beco sem saída, e a falácia pode estar em uma miscelânea de dados simplesmente notificados (*noticed*) e removidos (*take down*).

Palavras-chave: Lei Geral de Proteção de Dados (LGPD). Cibercrime. Banco de dados. Inteligência Artificial (IA). Vigilância global. Pornografia infantil.

ABSTRACT

Since the Tor software was released in 2002, much of the research on cybercrime has been restricted to the analysis of occurrences that take place in the so-called Deep and Dark Web. Analysts, however, forget the golden rule of criminals: they need to lure new "partners" without being identified by the police authorities. In this context, child pornography clubs appear, due to the concreteness of the materials (which can be very easily identified by Artificial Intelligence and vigilant internet users), as the paradigm case to be demonstrated here: since not every criminal is born high-tech, especially in countries that have not yet undergone digital transformation, it is consistent to assume that the entrance doors to the cyber underworld are hidden in very subtle phenomena of the Surface Web. Thus, this paper is dedicated to illuminate the possible missing piece of the cyber puzzle, with an analysis of the policies adopted by the main Internet Service Providers (ISP) in Brazil.

Based on this, a new preventive policing strategy is suggested, with a view to combating organized cybercrimes, which is sustained, as will be demonstrated, by the current Brazilian data protection system. The binomial *data protection and privacy versus cybercrime* is not necessarily a dead end, and the fallacy may be in an *omnium-gatherum* of data simply *noticed and taken down*, no more.

Keywords: Brazilian General Data Protection Law (LGPD). Cybercrime. Database. Artificial Intelligence (AI). Global Surveillance. Child Pornography.

1. INTRODUÇÃO

As revelações de Edward Snowden, em 2013, publicadas sobretudo pelo jornalista Glenn Greenwald no jornal britânico *The Guardian*, alteraram a sensibilidade internacional em relação ao tema da proteção de dados pessoais. Snowden, até então analista da Agência Nacional de Segurança dos Estados Unidos da América (NSA), vazou para a imprensa internacional uma série de documentos indicativos de que a NSA esteve, desde 2006, coletando dados pessoais de milhões de estadunidenses e pessoas de outros países por meio dos provedores de serviços de internet e telecomunicações, principalmente os programas *PRISM*[5], *Xkeyscore* (compartilhado com as agências de inteligência do *Five Eyes Alliance*[6]: EUA, Reino Unido, Canadá, Austrália e Nova Zelândia)[7] e *Bullrun*[8]. Os documentos revelaram a coleta de dados a partir das *big techs* do Vale do Silício, como *Microsoft* (a partir de 2007), *Yahoo*

5 Programa de vigilância global desenvolvido pela NSA. A esse respeito, ver Greenwald (2013b).

6 Ver Geist (2015, p. 225).

(2008), *Google* e *Facebook* (2009), *YouTube* (2010) e *Apple* (2012), mas também de outros provedores ao redor do mundo.

Tão logo as denúncias foram feitas, a vigilância cibernética passou a ser justificada pela necessidade de identificar criminosos. Por mais antitético que pareça, esse objetivo pouco colabora para a resolução do problema central, qual seja, o uso indevido dos provedores de conteúdo de internet, vistos como "salões de chá" para a criminalidade, em especial os clubes de pornografia infantil.

Se o enfoque da problemática penal com relação à proteção de dados esteve, desde então, afixada nos sistemas de inteligência repressivos, a possibilidade de "inteligência" preventiva, potencializada pelo *enforcement* das normativas de proteção de dados, tem sido pouco explorada. O objetivo desta breve incursão é demonstrar de que maneira, em estrita cooperação com tecnologias de suporte à proteção de dados (*privacy enhancing technologies*[9]), políticas mais efetivas de prevenção à disseminação de conteúdos ilícitos (a exemplo da pornografia infantil) podem ser alcançadas. Basta, conforme se demonstrará, que o objeto de análise seja transferido do agente criminoso às circunstâncias criminógenas.

---

7 Outro programa da NSA que permite a vigilância da agência de inteligência sobre uma vasta coletânea de dados coletados de milhões de usuários. A esse respeito, ver Greenwald (2013a).

8 Programa cujo objetivo é a decriptografia de dados, desenvolvido pela NSA e pelo GCHQ (*Government Communications Headquarters*), o serviço de inteligência britânico. A esse respeito, ver Greenwald (2013c).

9 Sobre o assunto, confira a definição de *Privacy Enhancing Technology* (PET) da Agência da União Europeia para a Cibersegurança (ENISA), em: https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies. Acesso em: 11 set. 2020.

2. LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) E ÂMBITO DE APLICAÇÃO

A LGPD tem como âmbito de aplicação, nos termos do respectivo art. 3º, qualquer tratamento de dados realizado por pessoa natural ou jurídica de direito público ou privado, presente uma das seguintes situações: a operação seja realizada no Brasil, os dados pessoais tenham sido coletados no País ou a operação tenha como objetivo fornecer bens, serviços ou tratar dados de indivíduos localizados no Brasil. Esse espectro de condições representa, em boa medida, a atual situação de grandes plataformas de redes sociais em operação no território brasileiro, como *Facebook*, *Instagram* e *Google*.

Em *prima facie*, consta do art. 4º da LGPD que a lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, para os quais prevê a edição de legislação específica. O ponto essencial parece estar, portanto, em reconhecer que, até que se prove a ilicitude do conteúdo analisado, o sistema de salvaguarda dos dados pessoais e da privacidade continua aplicável, devendo ser observado por qualquer política pública.

Especificações mais detalhadas da LGPD (*v.g.*, nas delimitações do art. 4º) indicam os parâmetros de abordagem para os casos limítrofes. Dado que o mapeamento e o desenvolvimento de mecanismos de predição (*predicting*) sobre a aparição de conteúdos ilícitos em provedores de serviços de internet (PSI) parecem imprescindíveis para um correto mecanismo de *compliance* com a legislação local, segundo a qual as plataformas devem evitar, tanto quanto possível, sua exploração por criminosos, alguns regramentos mínimos se mostram necessários. Aliás, até que um ilícito ocorra, a informação em questão é de domínio do sistema de proteção de dados.

Para o correto mapeamento do *contexto criminoso* em provedores de serviços de internet como os mencionados, a coleta prévia de dados

é indispensável. Bases de dados auxiliam na formulação de políticas direcionadas, o que se torna especialmente relevante no combate à disseminação de conteúdos ilícitos. Atualmente, este depende, em boa medida, de notificação feita pelos próprios usuários ou pelos *softwares* de identificação de conteúdos como o de nudez, que, não raro, operam sob a política de remoção automática na plataforma.

Nesse sentido, o § 1º do art. 4º da LGPD já informa que mesmo as operações de natureza penal deverão atentar para a *proporcionalidade* entre as medidas cabíveis (a fim de se alcançar o interesse público almejado) e a proteção dos dados pessoais, no que se refere aos *direitos do titular*, descritos nos arts. 17 a 22 da Lei[10], e aos *princípios de salvaguarda*, previstos no art. 6º: da boa-fé, da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da não discriminação e da responsabilização e prestação de contas (*accountability*).

Em poucas palavras, um sistema de boas práticas preventivo precisa, em primeiro lugar, ser capaz de reconhecer os conteúdos de pornografia infantil e identificar as circunstâncias em que aparecem, para só então estar apto a predizê-las. A LGPD possui esta função essencial: ante a possibilidade de os conteúdos reportados às autoridades e removidos (de acordo com as políticas do provedor de serviços) não desencadearem nenhum mecanismo de persecução penal, as plataformas de mapeamento preventivo deverão ser abastecidas de forma condizente com o sistema de salvaguarda dos dados pessoais.

---

10 São direitos do titular, exemplificativamente: o de acesso aos dados; o de correção de dados incompletos, inexatos ou desatualizados; o de portabilidade para outro fornecedor de serviço ou produto; o de eliminação dos dados pessoais tratados com o seu consentimento; o de revogação do consentimento; e o de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem o seu interesse.

Outro embaraço em relação às bases de dados de mapeamento preventivo parece estar, justamente, no momento de sua efetiva operabilidade. Um *software* de detecção de alertas para possíveis páginas disseminadoras de conteúdo ilícito funcionaria como parte de um sistema de inteligência? Se o conceito *inteligência* se refere comumente às informações coletadas pelos órgãos governamentais dedicados a essa função, o termo *governança* parece mais apropriado, no que envolve *boas práticas*.

Tendo em vista ser a notificação de alguns conteúdos (como os de pornografia infantil) compulsória, segundo a lei penal de alguns países (o que não é o caso da legislação brasileira), é possível sustentar que um *software* de detecção automática de redes de pornografia infantil (espelho utópico do modelo proposto) integraria um sistema de inteligência. Nada obstante, em razão de a notificação legal configurar mera faculdade das plataformas (sujeita, portanto, à análise prévia de adequação às políticas do provedor de serviços), tudo leva a crer que a abordagem de uma base de dados preventiva, operando em meio a plataformas como *Google* ou *Facebook*, não é subsumível ao conceito de inteligência. Afinal, eventual notificação às autoridades legais serve como mera *notitia criminis* para fins de persecução penal.

No mais, contanto que haja uma análise circunstancial, apta apenas a identificar os riscos do contexto (a exemplo do efeito negativo das notícias de suicídio entre as pessoas com propensão a atentar contra a própria vida[11]) dentro da plataforma, nenhuma coleta de dado pessoal é necessária. Nem o registro de IP (que pode vir a ser elemento de identificação de pessoa natural), nem os dados de conexão, nem outra circunstância relativa ao agente da conduta criminosa devem ser abordados. O poder investigativo é restrito às autoridades policiais, não podendo ser compartilhado com os provedores de serviços de internet.

---

11 Para um estudo mais aprofundado, ver Hagihara, Tarumi e Abe (2007).

Se a essas autoridades compete a identificação de redes de pornografia infantil e sua origem (com possível auxílio das plataformas, mediante o compartilhamento de informações, ainda que, *v.g.*, por determinação judicial, como dispôs o Marco Civil da Internet – MCI)[12], provedores como *Facebook* e *Google* podem não mais que gerenciar o problema. Isso significa questionar não o agente da causa, mas as circunstâncias facilitadoras. Nesse sentido, às plataformas é permitido elaborar políticas de prevenção de forma mais eficiente que os próprios serviços de inteligência criminal, sabidamente detentores de recursos econômicos e humanos reduzidos para explorar o complexo problema das *cifras negras*[13].

Talvez seja justamente este o escândalo causado pelas revelações de Edward Snowden: o problema da proteção de dados e da privacidade, que surge quando as duas esferas – pública e privada – convergem em seus interesses. O que se pretende demonstrar, todavia, é que nem sempre maior proteção de dados leva ao aumento do risco de proliferação criminosa, desde que este seja devidamente gerenciado.

---

12 Relativamente aos provedores de acesso (de conexão) à internet, o MCI dispôs o prazo de um ano para o armazenamento dos registros de conexão, sob sigilo e em ambiente controlado (*caput* do art. 13). Quanto aos provedores de conteúdo (de aplicações) de internet, o prazo estabelecido para o armazenamento dos registros de acesso é de seis meses (*caput* do art. 15). Os provedores de serviços de internet devem, ainda, observar o Decreto n. 8.771/2016, que regulamentou o MCI. Em ambos os casos, a autoridade policial ou administrativa ou o Ministério Público podem requerer, cautelarmente, que os registros sejam armazenados por tempo superior (§ 2º do art. 13 e § 2º do art. 15), o que poderá ocorrer no caso de ordem judicial.

13 O problema dos clubes de pornografia infantil, assim como do restante do universo criminal cibernético, é que não se sabe onde estão. Veja, por exemplo, a discussão sobre a localização do servidor no caso da Rota da Seda, um dos mais populares mercados negros já existentes na chamada *deep web*. Tão difícil é encontrar o servidor de um *site* protegido, que, como escreveu Cox (2014): "*The defense wanted to know which software was used to record evidence of the CAPTCHA leaking the Silk Road's IP address to investigators*".

3. BANCOS DE DADOS PARA POLICIAMENTO PREVENTIVO

Uma vez que são os próprios provedores de serviços de internet os encarregados de receber a notificação do conteúdo criminoso e decidir, em um primeiro momento, o que fazer com ela, o papel conferido a terceiros (intermediários) parece bastante limitado. De fato, identificada a ilicitude de conteúdo hospedado, ou mesmo mera contradição deste com os termos e condições de uso do provedor, o *post* é prontamente removido.

Em se tratando de pornografia infantil, é importante destacar que o conteúdo ilícito (as imagens propriamente ditas) não pode, sob nenhum regime de legalidade, ser armazenado nas plataformas. Se basta à curiosidade, as imagens mapeadas atualmente, para fins de rápida e automática identificação em rede, estão em bancos de dados geridos pelas polícias (sobretudo internacionais[14], como a Interpol), transfiguradas em *hashs* matemáticos. A ameaça do *cyber hacking* poderia, afinal, destruir os avanços de anos de trabalho contra a disseminação, que seria "perdido" (junto com as imagens, em si) em decorrência de qualquer falha mínima de cibersegurança.

O compartilhamento desses *hashs* faz com que a tarefa de busca dos conteúdos repetidos em rede seja, por parte dos provedores de conteúdo, facilitada. Esse tipo de ferramenta de detecção, embora utilize outras tecnologias, já é amplamente usado, por exemplo, pelo *Google* (como o *ID Content*, do *YouTube*[15]). Não é demais lembrar que, mesmo nos casos em que os *hashs* são liberados para fins de governança cibernética, o compartilhamento depende de uma rede formal e confiável[16].

---

14 Uma das mais importantes bases de dados, nesse sentido, é gerida pela Interpol (ICCAM). Confira: Interpol (2020).

15 A esse respeito: Lima e Peroli (2019).

16 "*Usually, data is hashed at a certain time and the hash value is protected in some way. At a later time, the data can be hashed again and compared to the protected*

Operar uma análise de dados, tratando-se reconhecidamente de pornografia infantil, traz a vantagem de superar o problema da qualificação (configuração como ilícito), a qual, principalmente quanto aos conteúdos encontrados primeiramente por um provedor, necessita da participação de múltiplas pessoas e instituições. O ideal seria que as autoridades legais pudessem checar os conteúdos denunciados. Entretanto, a quantidade de atores necessários para isso torna utópica a tarefa. O mais seguro, então, é que os algoritmos de detecção de futuras "bandeiras vermelhas" (*red flags*) sejam calculados com base em conteúdos já qualificados juridicamente.

Softwares de detecção de zonas de risco, assim como *softwares* comerciais, serviriam para localizar em qual âmbito está a necessidade do olhar humano. Havendo o risco, deverão indicar aos provedores a realização da notificação compulsória, com a qual se comprometeram.

Hoje existem diferentes tipos de algoritmos para diversos conteúdos: há algoritmos para conteúdo textual e outros para conteúdos multimídia. Em concreto, o objetivo é detectar padrões de semelhança entre páginas que abrigam pornografia infantil, a fim não de remover de imediato o conteúdo, mas selecioná-lo para exame acurado dos gestores da plataforma. Ao menos no curto prazo, isso resolve, de maneira mais ou menos eficiente, o problema de *Big Data* que está a ser gerado, por meio da inteligência artificial (IA), pelos provedores de conteúdo em rede.

4. GERAÇÃO DE CONTEÚDOS ILÍCITOS NÃO DETECTADOS PELAS PLATAFORMAS DA *SURFACE WEB*

Se a técnica de *profiling* é autorizada, mediante o consentimento do titular de dados, de acordo com a LGPD, para fim de coordenação

---

value. If the hash values match, the data has not been altered. If the values do not match, the data has been corrupted. For this system to work, the protected hash must be encrypted or kept secret from all untrusted parties." (ECPAT International, 2018, p. 14).

dos algoritmos de *marketing* (técnicas de customização), os algoritmos voltados à identificação de páginas *hosts*[17] de conteúdos de pornografia infantil também poderiam coletar dados pessoais, que constituem parte do conteúdo do *post*, em um primeiro momento, embora possam ser anonimizados, certamente[18].

Antes de tudo, é necessário restringir a abordagem a um mapeamento de caráter preventivo, que não é competente para descobrir conteúdos ilícitos, senão acidentalmente. Uma base de dados que utilize a IA e sirva para guiar a detecção de materiais de pornografia infantil em rede é, assim, distinta de um catálogo de perfis criminosos, estes, sim, de interesse do sistema de investigação e repressão de infrações penais.

A metodologia sugerida possui acepção bastante significativa. Consiste na análise de redes sociais, a partir da qual se pretende derivar estratégias de caráter preventivo, utilizando-se de informações (dados) amplamente disponíveis em provedores de serviços de internet da *surface web*[19], isto é, acessíveis, independentemente de ordem judicial, a fim de estruturá-los, gerando informações de *inteligência* passíveis de explo-

---

17 Análise semelhante foi feita com relação a uma plataforma russa utilizada para comércio de drogas, oportunidade na qual foi possível identificar alguns interesses em comum entre os usuários (*v.g.*, *hobbies*). Resultado como este seria bastante relevante a fim de rascunhar, com maior precisão, em quais lugares estão as possíveis portas de entrada para conteúdos mais extremos. (DIJKSTRA *et al*., 2014, p. 2739-2755)

18 De acordo com o inciso XI do art. 5º da LGPD, anonimização é a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

19 De fato, o uso de plataformas como *Facebook*, *Twitter* e *Google* parece ser explorado também pelos cibercriminosos. A impossibilidade de identificar o que está acontecendo faz, em termos práticos, que o problema da *surface web* se aproxime daquele da *dark* e *deep web*, cuja anonimização é o único distintivo capaz de hipotetizar o selo criminógeno desta. (DÉCARY-HÉTU; MORSELLI, 2011, p. 876-890)

ração pelos próprios provedores de serviços. Os *hotspots* do cibercrime necessitam, afinal, ainda ser identificados, em meio ao *cyberspace*.

A ideia principal é que os próprios provedores de conteúdo, ao remover conteúdos ilícitos, previamente notificados, *possam também detectar os padrões em que estes aparecem.* Apenas em 2018, *Facebook* e *Instagram* removeram o total de 12 milhões de conteúdos de pornografia infantil (NUÑEZ, 2018). Talvez os agentes de inteligência jamais alcancem, em apenas um ano, número equivalente ao de um único provedor de serviços hospedado na *dark* ou na *deep web*[20]. Atualmente, quando cessa a análise, pelos provedores, dos conteúdos ilícitos hospedados em suas plataformas, no momento em que se decide sobre isso, é previsível que uma série de dados bem importantes esteja a ser simplesmente descartada.

Não é de surpreender que a situação dos provedores de serviços, também na *surface web*, ainda seja, especialmente com relação aos conteúdos de pornografia infantil, caótica. Filtros de nudez, constantemente

20 De acordo com Daniel Sui, James Caverlle e Dakota Dudesill (2015, p. 6), "*Surface web* é a parte da *web* que está rastreada e indexada (e, portanto, encontrável) pelos mecanismos de pesquisa padrão, como o *Google* ou o *Bing*, por meio de um navegador da *web* comum. Na escuridão abaixo, após o termoclima eletrônico, estão as profundezas abissais da *deep web* (também conhecida como *invisible web* ou *hidden web*), a parte da *web* que não é rastreada e indexada e, portanto, está além do alcance do sonar dos buscadores padrões. Crescendo rapidamente dentro da *deep web*, está a *darknet* (também conhecida como *dark web*, *dark net* ou *dark internet*). Originalmente, a *dark net* se referia a qualquer ou a todos os *hosts* de rede que não podiam ser acessados pela internet. No entanto, assim que os usuários desses *hosts* de rede começaram a compartilhar arquivos (geralmente de forma anônima) em uma rede distribuída que não era indexada por mecanismos de pesquisa padrão, a *darknet* se tornou uma parte fundamental da *deep web*. Ao contrário do tráfego da *surface web* ou na maioria das partes da *deep web*, a maioria dos sites da *dark net* só podem ser acessados anonimamente." (Tradução dos autores.)

utilizados pelos provedores de conteúdo como estratégia preventiva raramente interconectam textos e páginas relacionadas ao *post*[21].

Se a checagem manual de todas as notificações encaminhadas ao provedor é mesmo impossível, dado o grande capital humano necessário, a coleta de informações sobre as circunstâncias em que se encontram as publicações notificadas sobre uma categoria específica de conteúdo (*v.g.*, pornografia infantil) pode, após esse tratamento de dados, apontar as possíveis falhas do algoritmo.

O problema é particularmente grave no tocante aos provedores de conteúdo como o *Instagram*, pois a garantia dada ao autor do material removido, de *recorrer* da remoção[22], não é estendida ao autor da notificação. O descontentamento deste não pode ser revisado, nem mesmo manualmente, pelo próprio provedor. O usuário notificante, nesses casos,

---

21 Veja, exemplificativamente, uma petição movida no parlamento inglês contra a não remoção de uma conta interconectada a outras relacionadas com pornografia infantil, após esta ser reportada à plataforma: CHANGE. Why is Instagram tolerating child pornography accounts after they have been reported? *Change*. Disponível em: https://www.change.org/p/uk-parliament-why-is-instagram-tolerating-child-porn-accounts-after-they-have-been-reported. Acesso em: 15 set. 2020.

22 Apenas de janeiro a março de 2020, 3,7 mil conteúdos reportados como pornografia infantil pelos usuários foram devolvidos à plataforma, no caso do *Facebook*, ao passo que 950 foram devolvidos sem nenhuma necessidade de apelação. Durante o mesmo período, 8,6 mil conteúdos foram examinados e removidos pela rede social. A porcentagem de quase um terço de conteúdos que voltam a circular é, ainda assim, relevante. No *Instagram*, durante o mesmo período, 3,2 mil conteúdos voltaram à circulação sem qualquer necessidade de apelação (questionável a razão pela qual os autores das postagens não apelam). A taxa de encontro de conteúdos ilícitos por meio de notificações dos usuários é maior que a porcentagem do *Facebook*, ainda que, em ambas as plataformas, a identificação automática dos conteúdos permaneça acima da taxa de 95% dos materiais "descobertos", conforme indicam os dados de transparência. (FACEBOOK, 2019)

é automaticamente remetido às Políticas da Comunidade, a fim de entender por que aquele conteúdo não viola as regras da plataforma[23].

O fato de o *Facebook*, assim como o *Instagram*, ainda estar envolto em escândalo de páginas (que permanecem *on-line*) com conteúdo de pornografia infantil (CRAWFORD, 2017), assim como ocorreu com o *Orkut* em meados de 2008 (BRASIL, 2009), pode muito bem ser explicado pelo tratamento automatizado do grande número[24] de notificações. Mais grave, é possível que o conteúdo, devidamente revisado e considerado adequado uma primeira vez, seja incluído no mecanismo como exemplo lícito, a fim de otimizar o processo.

Plausível supor, assim, que páginas de pornografia infantil possam continuar ativas nessas plataformas por longo tempo, até que um canal de denúncia externo (*v.g.*, autoridades de investigação e repressão de infrações penais ou canais de denúncia internacionais, como a Interpol) venha a apontar a necessidade de remoção. Qualquer analista do problema da cibercriminalidade há de notar que é justamente pelo drible na programação acolhida pelos *softwares* de IA que os conteúdos ilícitos estão a ser infiltrados.

Existe, no caso dos provedores de conteúdo, um dado importante com relação às páginas notificadas: elas foram apreciadas, primeiro, por um *elemento humano*[25], ou, ao menos, assim se deve supor. É crível

---

23 A questão foi pauta recente de comunicação da Comissão Europeia, na qual o objeto discutido é, entre outros: "*Prevent certain companies (in the absence of national legislative measures adopted in accordance with Article 15 of the e-privacy Directive) from continuing their own measures on voluntary detection, removal and reporting of child sexual abuse online*." (UNIÃO EUROPEIA, 2020)

24 "*Given the volume and diversity of big data, this is an inherently noisy environment, which reinforces the difficulty in identifying signals — in this case, genuine posts*." (VAN PUYVELDE; COULTHART; HOSSAIN, 2017, p. 1402)

25 Para a discussão sobre a necessidade de uma análise humana, e não meramente

presumir que o contexto das páginas notificadas e não removidas de início, mas mais tarde, por indicação ou ordem de terceiro, indica um caminho de grande potencial para a correção dos rumos do algoritmo base[26]. Ainda que o roteiro seja promissor, a rota parece muito tímida.

A escolha das redes de pornografia para exemplificar o potencial de uma base de dados de *inteligência* em ambiente controlado (privado) não é acidental. Se é verdade que outros exemplos, como células terroristas ou redes de *fake news*, pudessem ser aqui analisados, o caráter predominantemente visual (como fotos e vídeos) das redes de pornografia infantil (ainda que o conteúdo textual tampouco deva ser desprezado) facilita a seleção sobre o que há de ser destacado.

A gerência sobre os conteúdos de pornografia infantil é realizada por boa parte dos provedores de conteúdo de internet (caso do *Google*, do *Facebook* e dos respectivos grupos econômicos[27]), por sistemas de *hash*[28]. Estes talvez sejam o maior exemplo de base de dados bem-sucedida em matéria de criminalidade cibernética. O mapeamento dos padrões técnicos de imagens envolvendo pornografia infantil, possível

---

algorítmica, para filtrar o chamado *overblocking* (bloqueio excessivo), ver Ibrahim (2017).

26 "*Most algorithms will display inadvertent bias rather than explicitly coded-in bias […] Biased or discriminatory behaviour may only become apparent looking at the corpus of users as a whole – something that will not happen through individual user challenges*." (EDWARDS; VEALE, 2018)

27 Sobre os *hashs* usados pelos provedores de serviços de internet, ver Curtis (2020).

28 Uma das listas mais conhecidas de *hashs* de pornografia infantil é composta das imagens mapeadas pela *Internet Watch Foundation*. Relevante constar que, embora os *hashs* não permitam identificar imagens novas de pornografia infantil, estes conseguem reconhecer imagens já previamente mapeadas. Nesse sentido: "*Five IWF Members, Facebook, Google, Microsoft, Twitter and Yahoo, are using the hash list so far. The list will then be rolled out to all eligible Members.*" (INTERNET WATCH FOUNDATION, 2015)

tão somente pela existência de uma base de dados, possibilitou o desenvolvimento de um algoritmo que alimenta *softwares* de detecção automática de *conteúdos semelhantes*[29], como antes abordado.

Esses algoritmos, existentes no caso das imagens, certamente não existem quando se trata de *spams* de *hyperlinks*, para os quais um algoritmo de base textual seria igualmente necessário. Se a posse de imagens pelos provedores de serviços de internet, com o objetivo de aprimorar a gestão dos algoritmos, é certamente um ponto problemático, no entorno das causas de justificação, algoritmos textuais ou mesmo algoritmos de rede parecem a alternativa mais plausível, conforme se verá adiante.

A fim de esclarecer o que ocorre atualmente com as bases de dados de *hashs*, em razão do caráter ilegal de seu conteúdo[30] (nada além de extensa coleção de pornografia infantil), as imagens são, hoje, de estrito domínio das autoridades de investigação e repressão de infrações penais, que compartilham com os provedores somente os *códigos de identificação,* os *hashs*[31]. É de esperar que, em um cenário de sequestro

29 Removidos em um primeiro momento, esses conteúdos podem voltar à circulação caso o usuário responsável por eles recorra sobre a remoção e consiga reverter a decisão (automatizada) da plataforma.

30 Ainda que as imagens pudessem ser simplesmente apagadas após a formação do *hash*, a preservação delas é, por vezes, imprescindível para a identificação de vítimas. Bases de dados, inclusive internacionais, neste sentido, existem. Veja, *v.g.*, a operação lançada em 2008 pela FBI com o fim de não simplesmente identificar as imagens e frear o compartilhamento, mas efetivamente identificar as crianças: "*Candidate images for Operation Rescue Me arise from new child pornography series discovered by FBI field investigations, from forensic exams, or from nominations by National Center for Missing and Exploited Children.*" (UNIÃO EUROPEIA, s.d.)

31 "*Hash values are non-pictorial, alphanumeric values that are unique to each computer file that can serve as a 'fingerprint' of a file for matching purposes and also provide security, because the original image cannot be recreated from the hash value itself.*" (EUA, 2003)

de dados frequente, deixar essas imagens ao manejo dos provedores seja desnecessário, não havendo conformidade com o princípio de *data minimization* (do Regulamento Geral de Proteção de Dados da União Europeia ou *General Data Protection Regulation* – GDPR) ou princípio da necessidade, pela LGPD (art. 6º, III).

No entanto, isso não significa que inexiste, com relação a conteúdos que não podem ser legalmente possuídos, alternativa. O que se pretende demonstrar é que subsiste, em integral respeito à expectativa de proteção dos dados dos titulares (usuários na *web*), uma possibilidade altamente promissora, baseada na análise de redes, especialmente com relação aos conteúdos reportados pelos usuários, mas não removidos pelo provedor.

Embora a análise integral desses conteúdos pareça promissora, principalmente com relação à descoberta de mecânicas ainda pouco conhecidas da criminalidade cibernética, o enfoque sobre a contextualização das postagens que são, em verdade, novos *hashs* (removidas *primeiramente*[32] pelas plataformas, com *reupload*, em burla ao sistema) tem o potencial de oferecer respostas mais imediatas sobre a estrutura do tráfego de conteúdo ilícito, especificamente aquele que ocorre diretamente nos provedores, sem que estes sirvam apenas como agentes intermediadores[33].

---

32 A formação dos *hashs* (identificação de imagens por meio de funções matemáticas) depende que um valor inicial (*input*), no caso, a imagem, seja fornecido. Eis a razão pela qual, embora o sistema de *hashs* possa colaborar, de maneira bastante eficiente, para a rápida identificação dos conteúdos de pornografia infantil já identificados pelas agências policiais, estes nada podem fazer em relação às novas imagens, isto é, ainda não catalogadas. Uma vez que os *hashs* anteriores são rastreáveis, este é um grande incentivo para que os criminosos busquem imagens "completamente novas", como queriam, *v.g.*, os membros do *País das Maravilhas* (MCVEIGH, 2001).

33 Os intermediários representam hoje a peça ausente do quebra-cabeça dos clubes de pornografia infantil. Visto que o fechamento de um clube não impede seu reaparecimento em outra localidade da internet, é de se supor que um importante ponto de contato esteja ainda perdido em meio à complexidade do sistema de redes.

O que se pretende é superar a barreira técnica enfrentada pelos provedores de serviços de internet, que, em razão mesmo de sua popularidade, se tornam grandes "salões de chá" visados por cibercriminosos que pretendem aliciar novos membros. Justamente porque não se trata de desenvolver perfis, mas simplesmente prever, com maior precisão, a lógica de aparição dos conteúdos, uma análise de redes é possível sem intermédio de qualquer dado pessoal dos usuários.

Para esclarecer esse ponto, é necessário especificar, em primeiro lugar, o tipo de dado em jogo e por que ele importa. Nesse sentido, essencial a constatação de que não se trata de coletar qualquer tipo de informação sobre perfis que violem as denominadas *políticas da comunidade*[34]. Apesar de ser possível efetuar tal coleta em circunstâncias nas quais o conteúdo postado tenha natureza flagrantemente ilícita (a exemplo da pornografia infantil), visto que a ocorrência é de interesse para investigações criminais, não é esse o caso do que se está a propor.

Talvez o teor dos comentários no entorno de uma determinada postagem, as *tags* a ela associadas ou mesmo a descrição[35] indiquem a modalidade pela qual consumidores desse tipo de conteúdo ilícito reconhecem as páginas *hosts* ainda na internet aberta[36].

Na impossibilidade de identificar, exatamente, onde reside a falha do

---

Os intermediários explicariam, afinal, como é possível que logo após o fechamento do clube *Freedom Hosting*, um de seus servidores tenha sido simplesmente "descarregado" em outro local da internet, acessível para qualquer um que soubesse como chegar aos arquivos. O ponto principal permanece sendo, assim, identificar a localidade em que as instruções estão a ser distribuídas (HAASZ, 2017).

34 "Even with automation and company intervention, volunteer moderators are left to manage more nuanced, difficult and decidedly human issues." (KELLY, 2020)

35 Para uma abordagem alternativa ao paradigma exclusivamente baseado nas imagens, ver HU *et al.* (2007).

36 "*The pioneering Adamflowers/Farmer's Market started out as a surface web market in 2006 but transitioned to TOR in 2010. It had been selling illegal drugs to more*

algoritmo de customização (as *sugestões*, portanto), que leva a escândalos como o que se passou com o *YouTube*[37] em meados de 2019, o mapeamento circunstancial sobre os conteúdos simplesmente removidos das plataformas é capaz de indicar, com maior clareza, quais algoritmos permitem um *compliance* com a promessa ética feita pelos provedores desses serviços.

Tendo em vista que os algoritmos comerciais operam de maneira constante nas plataformas digitais, de um erro de qualificação podem advir consequências desastrosas. Nada impede, por exemplo, que um desses algoritmos garanta que o *click* sobre um dado conteúdo político-eleitoral retorne outros da mesma categoria, chegando a influenciar, em alguma medida, as eleições no país. Igualmente, é plausível que esse mesmo algoritmo sugira conteúdos de pornografia infantil, entre outras matérias mais ou menos relacionadas, quando o usuário seleciona um conteúdo de tema tangente.

Se os algoritmos comerciais se baseiam, para sugerir novos conteúdos, em modelos comportamentais assemelhados, o aparentemente ingênuo ato de publicar a foto de um bebê no banho, por exemplo, pode desencadear, de acordo com o escopo de progressão automatizada, acesso a páginas cujo conteúdo é mais extremo, em cadeia lógica que se sucede quando ausente, da parte da plataforma, ciência de que hospeda conteúdo ilícito.

No caso de conteúdos de pornografia infantil, cuja mera posse,

---

than 34 countries before it was eventually shut down by law enforcement agencies in 2012." (MELAND; BAYOUMY; SINDRE, 2020, p. 9)

37 Para uma visão mais aprofundada sobre o "buraco negro" dos algoritmos, em que palavras como "yoga", "*gymnastics stretch*" (ginástica de alongamento) ou "*bikini haul*" (ponte de biquíni), vídeos de mulheres adultas levam em poucos cliques a conteúdos de pornografia infantil *softcore* (sexualizações), ver Hancock (2019).

plausível de ocorrer ante um simples *click*[38], pode configurar crime, é justificável que a maioria dos que são efetivamente removidos pelo *Facebook* e pelo *Instagram* tenham sido encontrados pelos algoritmos de IA. Não é demais notar que as regras de notificação, as quais deveriam funcionar como incentivo a uma política de boas práticas conduzida pelos usuários, se revelam, na prática, ferramentas de intimidação. Imagine o dilema jurídico de um cidadão da União Europeia que, tendo tomado conhecimento de um conteúdo de pornografia infantil, queira notificá-lo à plataforma. Constituindo fato típico o *mero acesso*[39] ao conteúdo, é de esperar que o homem desista de agir, embora a notificação pudesse subsumir sua inocência.

Em razão da estrutura *obscuramente típica*[40] das circunstâncias que enredam as notificações de pornografia infantil em rede, supõe-se que a proliferação diária desses conteúdos sobreviva à custa de uma cifra negra que os pedófilos souberam muito bem esconder[41]. Até mesmo os algoritmos utilizados pelas plataformas "pensam" como agentes da lei, não como criminosos.

Veja que, conquanto estudos sobre *softwares* de identificação de

---

38 Para uma abordagem mais específica sobre o problema da descarga automática de *cache*, ver Gant (2012).

39 De acordo com o n. 3 do art. 5º da Diretiva (UE) n. 2011/92, sobre a luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil: "A obtenção de acesso a pornografia infantil com conhecimento de causa e por meio das tecnologias da informação e da comunicação é punível com uma pena máxima de prisão não inferior a um ano." (UNIÃO EUROPEIA, 2011)

40 Para uma discussão mais aprofundada no tema, ver Diez (2006).

41 "*Online pornography businesses usually separate the advertise-and-join Web site from the members area. The first one often contains a preview of what prospective members can expect to receive if they agree to pay a subscription fee, and it includes a hyperlink to use to obtain membership*." (LUDERS, 2007, p. 19)

nudez[42] sejam tema frequente de congressos de IA, a análise dos contextos de aparição dos conteúdos raramente acontece, quando se trata de *softwares* projetados para a *surface web*. Nas chamadas *dark* e *deep web*, ao contrário, e talvez porque o grande cerco metodológico seja encontrar os locais em que os fóruns ocorram, análises contextuais[43] já aparecem de forma mais corrente.

Ainda que a modalidade *notice and take down* adotada pelos provedores de serviços de internet impeça, em um primeiro momento, que aquele exato conteúdo continue a se proliferar em meio à plataforma, nada impede o surgimento de novas páginas, de igual natureza e identificáveis pelas mesmas características, por intermédio de uma conta falsa, apenas alguns minutos depois na mesma rede social. Onde o *hash* de identificação ainda não existe, é imperioso encontrar uma via alternativa, ao menos, a fim de identificar as áreas de risco (*bandeiras vermelhas*), que deverão, ainda, ser checadas pela equipe de pessoal até que novos algoritmos resolvam também esse problema.

É justamente esse o ponto nevrálgico que, ao menos com relação aos conteúdos de pornografia infantil, ainda se tem de resolver. Um

---

42 Os *softwares* de detecção de nudez estão, também eles, longe de resolver completamente o problema. Afinal: "*Anyone can imagine how difficult it is to capture all the nuances of child pornography imagery through color, shape, textures, and other image hand-crafted descriptors alike while, at the same time, ruling out innocuous and/or non-SEIC adult content*." (VITORINO *et al.*, 2018, p. 306). As imagens sexualizadas, sem nudez propriamente dita, estão, conforme se poderia esperar, travadas em um impasse semelhante.

43 Por exemplo, em uma pesquisa sobre mercados de drogas *on-line*, a mecânica de convites pode ser bem percebida em meio às redes abertas: "*Initial searches were made on Facebook, Instagram, Snapchat, Jodel and Twitter [...] Facebook searches led to information about groups through open drug posts, group invitations in other grey-area groups (*e.g. *shaming groups and sales groups) and other people's group requests. We then entered groups, which led to other group invitations*." (DEMANT *et al.*, 2019)

mapeamento sobre o contexto de aparição permitiria maior previsibilidade sobre: a) quais páginas de risco devem ser mais bem observadas; e b) no entorno de quais conteúdos os "*salões de chá on-line*" para consumidores de pornografia infantil em rede estão a se formar.

A aposta nas imagens explícitas parece ser um bom ponto de partida, no entanto não é o mais eficiente. Considerando que os dados de conexão podem ser facilmente acessados pelos órgãos de investigação e repressão de infrações penais, faz sentido supor que os convites para outros "*salões de chá on-line*" mais explícitos (possivelmente protegidos por senhas e alta criptografia[44]) estão a ser distribuídos de forma a "*não dar bandeira*". É justamente essa mecânica, qual seja, a bandeira "*codificada*" por organizações criminosas transnacionais, que devem ser identificadas.

5. CONCLUSÃO

A simples remoção dos conteúdos ilícitos encontrados em provedores de serviços de internet da *surface web* pode não ser o melhor caminho para garantir que os provedores dificultem, tão bem quanto possível, a usurpação de suas plataformas por redes criminosas internacionais. Porque também os criminosos fogem do óbvio, é possível que a peça ausente nos algoritmos de plataformas e nos sistemas de inteligência, que têm

44 Para além do problema técnico por detrás de códigos matemáticos, existe outro, jurídico, incidente exatamente sobre o processo penal, sobre os sistemas de criptografia sem "*backdoor*". Quando as autoridades policiais desconhecem a chave, a revelação desta depende do não silêncio do acusado. Adentra-se o campo das colaborações. Em suma: "*This becomes important when understanding why the digital encryption process works like a typical lock and key in the physical world.*" (EDGETT, 2003, p. 345)

ainda atuação majoritariamente repressiva, esteja nos próprios *posts* que violam as *políticas da comunidade* sem constituírem, todavia, fatos ilícitos. Quanto a eles, a inexistência de qualquer dever legal de notificação corrobora a tese de que podem existir vários atalhos para os "*salões de chá on-line*" criminosos que, em razão da descentralização de dados, as autoridades legais desconhecem. Os criminosos da *web* contam, afinal, com o benefício (para eles) e o problema (para as autoridades) do *Big Data*.

Todo algoritmo precisa ser alimentado por dados que o direcionem a uma funcionalidade (estruturados, portanto), razão pela qual não é crível que o amplo espectro de páginas removidas pelas plataformas seja simplesmente descartado, sem nenhum tipo de cadastro. É verdade que a interconexão das páginas e principalmente dos usuários nelas constantes pode ser um dado promissor aos sistemas de inteligência criminal, principalmente onde os *hashs* voltam a se repetir (o que indica vínculo não acidental entre a página removida e a nova *host*). Não obstante, não é esta a base de dados (de perfis) que se está, aqui, a discutir. A possível implicação criminal exigiria análise completamente distinta.

Em se tratando de mero mapeamento de circunstâncias de aparição, o desenvolvimento de algoritmos para previsão de locais de risco cibernético parece coadunar-se com a proteção requerida aos princípios gerais de salvaguarda e aos direitos dos titulares de dados, em conformidade com o art. 4º da LGPD.

Certo é que o mapeamento transnacional sobre o que ocorre dentro das plataformas geridas por provedores de serviços de internet estrangeiros possa apresentar uma visão ainda mais ampla do fenômeno, com respeito às características particulares de cada plataforma. Enquanto essa cooperação, ao menos em nível de governança, ainda não se aperfeiçoa, a implementação de análises contextualizadas de conteúdos sem impacto criminal pode fornecer bons rumos para chegar-se a um programa efetivo, *v.g.*, contra as redes de pornografia infantil em território brasileiro, mas também sobre outros conteúdos ilícitos, por análise contextual.

REFERÊNCIAS

BRASIL. Ministério Público Federal. *Operação Turko combate a pornografia infantil no Orkut em todo o país*. 18 maio 2009. Disponível em: http://www.mpf.mp.br/sp/migracao/sala-de-imprensa-unidadeprsp/noticiasprsp/18-05-09-operacao-turko-combate-a-pornografia-infantil-no-orkut-em-todo-o-pais. Acesso em: 20 set. 2020.

BRIGHT, Martin; MCVEIGH, Tracy. This club had its own chairman and treasurer. Its business was child abuse. It takes just four minutes to log into paedophile web. *The Guardian*, 11 fev. 2001. Disponível em: https://www.theguardian.com/uk/2001/feb/11/tracymcveigh.martinbright. Acesso em: 21 set. 2020.

CHANGE. Why is Instagram tolerating child pornography accounts after they have been reported? *Change*. Disponível em: https://www.change.org/p/uk-parliament-why-is-instagram-tolerating-child-porn-accounts-after-they-have-been-reported. Acesso em: 15 set. 2020.

COX, Joseph. How did the FBI find the Silk Road Servers, anyway? *Vice*, 3 out. 2014. Disponível em: https://www.vice.com/en_us/article/ae3nvg/how-did-the-fbi-find-the-silk-road-servers-anyway. Acesso em: 20 set. 2020.

CRAWFORD, Angus. Facebook failed to remove sexualised images of children. *BBC News*, 7 mar. 2017. Disponível em: https://www.bbc.com/news/technology-39187929. Acesso em: 12 set. 2020.

CURTIS, Sophie. Facebook, Google and Twitter block "hash list" of child porn images. *Telegraph*, 10 ago. 2020. Disponível em: https://www.telegraph.co.uk/technology/internet-security/11794180/Facebook-Google-and-Twitter-to-block-hash-list-of-child-porn-images.html. Acesso em: 19 set. 2020.

DÉCARY-HÉTU, David; MORSELLI, Carlo. Gang presence in social network sites. *International Journal of Cyber Criminology*, v. 5, n. 2, p. 876-890, 2011. Disponível em: http://www.cybercrimejournal.com/davidcarlo2011julyijcc.pdf. Acesso em: 21 set. 2020.

DEMANT, Jakob; BAKKEN, Silje Anderdal; OKSANEN, Atte; GUNNLAUGSSON, Helgi. Drug dealing on Facebook, Snapchat and Instagram: A qualitative analysis of novel drug markets in the Nordic countries. *Drug and Alcohol Review*, v. 38, n. 4, 2019, p. 377-385.

DIEZ, Eric R. "One Click, You're Guilty": A Troubling Precedent for Internet Child Pornography and the Fourth Amendment. *Catholic University Law Review*, v. 55, n. 3, 2006, p. 759-794. Disponível em: https://scholarship.law.edu/lawreview/vol55/iss3/9. Acesso em: 20 set. 2020.

DIJKSTRA, L. J.; YAKUSHEV, A.V.; DUIJN, P. A. C.; BOUKHANOVSKY, A.V.; SLOOT, P. M. A. Inference of the Russian drug community from one of the largest social networks in the Russian Federation. *Quality & Quantity*, v. 48, 2014, p. 2739-2755. Disponível em: https://arxiv.org/abs/1211.4783. Acesso em: 20 set. 2020.

ECPAT International. Trends in online child sexual abuse material. *ECPAT International*, abr. 2018, p. 14.

EDGETT, Sean J. Double-clicking on fourth amendment protection: encryption creates a reasonable expectation of privacy. *Pepperdine Law Review*, v. 30, n. 2, 2003, p. 345.

EDWARDS, Lilian; VEALE, Michael. Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"? *IEEE Security & Privacy*, v. 16, n. 3, p. 49, maio/jun. 2018. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3052831. Acesso em: 20 set. 2020.

EUA. Federal Bureau of Investigation. Privacy Impact Assessment (PIA) Child Victim Identification Program (CVIP) Innocent Images National Initiative (IINI). *Federal Bureau of Investigation*, 9 maio 2003. Disponível em: https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/cvip. Acesso em: 18 set. 2020.

FACEBOOK. Community Standards Enforcement Report. *Facebook Transparency 2019*. Disponível em: https://transparency.facebook.com/community-standards-enforcement#instagram-adult-nudity-and-sexual-activity. Acesso em: 18 set. 2020.

GANT, Katie. Crying over the Cache: why technology has compromised the uniform application of child pornography laws. *Fordham Law Review*, v. 81, n. 1, out. 2012, p. 319-364.

GEIST, Michael. *Law, privacy and surveillance in Canada in the Post-Snowden Era*. Ottawa: University of Ottawa Press, 2015. p. 225.

GREENWALD, Glenn. NSA paid millions to cover Prism compliance costs for tech companies. *The Guardian*, 23 ago. 2013b. Disponível em: https://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid. Acesso em: 14 set. 2020.

GREENWALD, Glenn. Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian*, 5 set. 2013c. Disponível em: https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security. Acesso em: 14 set. 2020.

GREENWALD, Glenn. XKeyscore: NSA tool collects "nearly everything a user does on the internet". *The Guardian,* 31 jul. 2013a. Disponível em: https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. Acesso em: 14 set. 2020.

HAASZ, Amanda. Underneath It All: policing international child por-

nography on the dark web. *Syracuse Journal of International Law and Commerce*, v. 43, n. 2, 2016.

HANCOCK, Jaime Rubio. YouTube enfrenta um escândalo com milhares de comentários pedófilos em vídeos de menores. *El País*, 21 fev. 2019. Disponível em: https://brasil.elpais.com/brasil/2019/02/21/tecnologia/1550748035_065824.html. Acesso em: 13 set. 2020.

HU, Weiming; WU, Ou; CHEN, Zhouyao; FU, Zhouyu; MAYBANK, Steve. Recognition of pornographic Web pages by classifying texts and images. *IEEE Trans Pattern Anal Mach Intell*, jun. 2007, p. 1019-1034.

IBRAHIM, Yasmin. Facebook and the Napalm Girl: reframing the iconic as pornographic. *Journal of Social Media and Society*, v. 3, n. 4, 20 nov. 2017, p. 1-10. Disponível em: https://journals.sagepub.com/doi/full/10.1177/2056305117743140. Acesso em: 20 set. 2020.

INTERNET WATCH FOUNDATION. Hash List "could be game-changer" in the global fight against child sexual abuse images online. *Internet Watch Foundation*, 10 ago. 2015. Disponível em: https://www.iwf.org.uk/news/hash-list-could-be-game-changer-global-fight-against-child-sexual-abuse-images-online. Acesso em: 20 set. 2020.

INTERPOL. Blocking and categorizing content. *INTERPOL*, 20 set. 2020. Disponível em: https://www.interpol.int/Crimes/Crimes-against-children/Blocking-and-categorizing-content. Acesso em: 20 set. 2020.

KELLY, Heather. Burnout, splinter factions and deleted posts: Unpaid online moderators struggle to manage divided communities. *The Seattle Times*, 25 ago. 2020. Disponível em: https://www.seattletimes.com/business/burnout-splinter-factions-and-deleted-posts-unpaid-online-moderators-struggle-to-manage-divided-communities/. Acesso em: 21 set. 2020.

LIMA, Cíntia Rosa Pereira de; PEROLI, Kelvin. *Direito digital*: compliance, regulação e governança. São Paulo: Quartier Latin, 2019.

LUDERS, Wade. Child Pornography Web Sites: Techniques used to evade law enforcement. *FBI Law Enforcement Bulletin*, v. 76, n. 7, 2007, p. 19.

MELAND, Håkon; BAYOUMY, Yara Fareed Fahmy; SINDRE, Guttorm. The Ransomware-as-a-Service economy within the darknet. *Journal of Computers and Security*, v. 92, n. 7034, 2020, p. 9.

NUÑEZ, Michael. Facebook and Instagram removed more than 12 million pieces of child porn. *Forbes*, 13 nov. 2018. Disponível em: https://forbes.kz//massmedia/facebook_and_instagram_removed_more_than_12_million_pieces_of_child_porn/?. Acesso em: 21 set. 2020.

SUI, Daniel; CAVERLLE, James; RUDESILL, Dakota. *The Deep Web and The Darknet*: a look inside the Internet's massive black box. Washington, DC: Wilson Center, 2015, p. 6. Disponível em: https://www.wilsoncenter.org/sites/default/files/stip_dark_web.pdf. Acesso em: 20 set. 2020.

UNIÃO EUROPEIA. Comissão Europeia. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*. COM (2020) 607. EU strategy for a more effective fight against child sexual abuse. Bruxelas, 24 jul. 2020. Disponível em: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf. Acesso em: 21 set. 2020.

UNIÃO EUROPEIA. Comissão Europeia. *Global alliance against child sexual abuse online*, s.d. Disponível em: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-childabuse/docs/

commitements/ga_commitment_-_united_states_en.pdf. Acesso em: 20 set. 2020.

UNIÃO EUROPEIA. Diretiva (UE) 2011/92, Parlamento Europeu e do Conselho, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho. *Jornal Oficial da União Europeia*, 17 dez. 2011. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32011L0093. Acesso em: 20 set. 2020.

VAN PUYVELDE, Damien; COULTHART, Stephan; HOSSAIN, M. Shahriar. Beyond the buzzword: Big Data and national security decision-making. *Journal of International Affairs,* v. 93, n. 6, 2017, p. 1398-1416.

VITORINO, Paulo; ÁVILA, Sandra; PEREZ, Maurício; ROCHA, Anderson. Leveraging deep neural networks to fight child pornography in the age of social media. *Journal of Visual Communication and Image Representation*, v. 50, 2018, p. 306. Disponível em: https://www.researchgate.net/publication/321868875_Leveraging_Deep_Neural_Networks_to_Fight_Child_Pornography_in_the_Age_of_Social_Media. Acesso em: 20 set. 2020.

O ANTEPROJETO DA "LGPD PENAL", A (IN)SEGURANÇA PÚBLICA E A (NÃO) PERSECUÇÃO PENAL[1]

Paulo Rubens Carvalho Marques[2]
Pablo Coutinho Barreto[3]
Octávio Celso Gondim Paulo Neto[4]

Em 18 de setembro de 2020, entrou em vigor a Lei n. 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), que disciplinou o uso, a proteção e a transferência de dados de pessoas naturais no Brasil.

Conforme disposto em seu art. 4º, III, a LGPD não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais. O § 1º do mesmo artigo dispõe que nesses casos o tratamento de dados pessoais será regido por legislação específica.

Visando atender, *parcialmente*, ao mandamento legislativo contido no § 1º do art. 4º da LGPD[5], a Câmara dos Deputados, por meio de

2 Procurador da República (MPF).

3 Procurador da República (MPF).

4 Promotor de Justiça (MP/PB).

5 Diz-se "parcialmente" porque o anteprojeto da Comissão de Juristas não se debruçou

Ato do Presidente de 26 de novembro de 2019, instituiu comissão de juristas destinada a elaborar anteprojeto de legislação específica para o tratamento de dados pessoais no âmbito da segurança pública, investigação penal e repressão de infrações penais.

A mencionada Comissão de Juristas apresentou anteprojeto da chamada "LGPD Penal", em 5 de novembro de 2020, mediante texto[6] que poderá afetar severa e negativamente as atividades de todos os órgãos envolvidos, direta ou indiretamente, na investigação criminal, repressão penal e/ou segurança pública.

Conforme apontado na própria Exposição de Motivos do anteprojeto, a Comissão de Juristas foi fortemente influenciada pela **Diretiva n. 2016/680** do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

Ocorre que uma simples leitura comparativa entre o texto apresentado pela Comissão de Juristas e a normativa europeia evidencia inegável descompasso, notadamente em relação aos objetivos normativos e às dimensões do tratamento dos dados pessoais. Vejamos.

A **Diretiva (UE) n. 2016/680** enuncia expressamente seus objetivos, quais sejam os de (i) *proteger os direitos e liberdades fundamentais das pessoas singulares*, nomeadamente o seu direito à proteção de dados pessoais, **e** (ii) *assegurar o livre intercâmbio desses dados pelas autoridades competentes na União Europeia* (Considerando 93).

Para a concretização desse duplo objetivo, o sistema esquadrinhado pela Diretiva Europeia alcança o tratamento de dados pessoais realizado pelas

---

sobre a temática da proteção dos dados pessoais nos campos da defesa nacional e da segurança do Estado.

6 O anteprojeto é composto por 11 capítulos e 68 artigos, podendo ser acessado no seguinte *link*: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf.

autoridades competentes para efeitos de **prevenção**, **investigação**, **detecção** ou **repressão** de infrações penais ou **execução** de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública (art. 1º, 1).

A seu turno, embora influenciado pela Diretiva (UE) n. 2016/680, o texto do **anteprojeto** apenas importou as lógicas da **investigação** e **repressão** de infrações penais, esquecendo os importantíssimos pilares da prevenção e da detecção de condutas desviantes, que reclamam a utilização de massas de dados, em ambientes restritos e controlados.

E mais. Em vez de estabelecer balizas para o intercâmbio de dados entre as autoridades competentes, o **anteprojeto** estabeleceu restrições desproporcionais e distantes da realidade, como as previstas nos arts. 14, § 2º; 43; e 45, § 1º, "*sem oferecer, em contrapartida, uma melhoria palpável dos direitos das pessoas em causa*"[7].

Em verdade, o compartilhamento de bancos de dados entre os atores da persecução penal e da segurança pública consiste em emanação concreta do princípio da eficiência, contribuindo sobremaneira para a proteção suficiente de bens jurídicos de relevância constitucional, notadamente o direito fundamental à segurança. É o caso daqueles tutelados pelos crimes de lavagem de dinheiro, de financiamento do terrorismo e pela miríade de crimes compreendidos pela chamada "criminalidade dos poderosos" – praticados por indivíduos que não eram alcançados pelos métodos tradicionais de investigação por não se enquadrarem na chamada "criminalidade conforme ao estereótipo".

A tentativa de impor restrições desproporcionais à circulação de dados entre as autoridades competentes também contraria premissas

---

7 Advertência formulada pela relatora Ursula Männle, deputada, ao Parlamento do Estado da Baviera, no Parecer do Comitê das Regiões sobre o pacote de Proteção de Dados (2012/C 391/13). Como se vê, *a questão não se resolve em termos de limitação à livre circulação de dados, mas na exigência da adoção de mecanismos de segurança que assegurem um elevado nível de proteção de tais dados pessoais*.

básicas da própria diretiva europeia, como aquela assentada no Considerando 27:

> *Para efeitos de prevenção, investigação ou repressão de infrações penais*, **é necessário que as autoridades competentes tratem os dados pessoais**, recolhidos no contexto da prevenção, investigação, deteção ou repressão de infrações penais específicas **para além desse contexto**, *a fim de obter uma melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detetadas*.

Nesse contexto, não causa estranheza que o anteprojeto tenha incorrido em confusão conceitual que pretende atribuir natureza probatória a todo "dado pessoal", ignorando que em boa parte dos casos o manejo de dados, sobretudo nos campos da prevenção e da detecção de infrações penais, serve ao propósito de orientar a atuação dos órgãos de persecução e auxiliar na prospecção de trilhas investigativas[8].

Também deve ser destacada a *excessiva amplitude do conceito de dado pessoal*, entendido como qualquer "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I), disponibilizada em "suporte eletrônico ou físico" (art. 5º, V).

Assim, ao pretender regular todos os aspectos referentes ao tratamento de dados pessoais, *físicos ou eletrônicos*, na persecução penal e na segurança pública, o anteprojeto impacta diretamente temas regulados

8 Ou seja: em vez da atuação em casos levados a conhecimento das autoridades apenas tardiamente – e sujeitos, ao menos na fase inicial, aos vieses, interesses e versões dos noticiantes –, o cruzamento de bases de dados possibilita uma atuação sólida e tempestiva. Nesse modelo, somente após deparar-se com a necessidade de atuar, é que são deflagradas as investigações e, aí sim, produzidas provas.

por outros diplomas, como o da prova penal e das técnicas especiais de investigação, causando embaraços ao processo penal.

Para reforçar o hiato existente entre a normativa europeia e a práxis que o anteprojeto pretende instituir, é válido mencionar a experiência de Portugal, que, ao transpor a Diretiva (UE) n. 2016/680 para o seu ordenamento jurídico, expressamente excluiu do âmbito de incidência de sua LGPD Penal os dados constantes de processo penal, decisão judicial, registro criminal e os demais referentes ao sistema judicial (cf. art. 68 da Lei n. 59/2019, de 8 de agosto de 2019).

Não é só. Também vem de Portugal um exemplo de como tratar adequadamente a questão do compartilhamento de dados entre as autoridades competentes. O art. 69 do mencionado diploma é taxativo ao afirmar que o disposto na lei de proteção de dados pessoais "*não implica qualquer restrição ou limitação na partilha e intercâmbio de dados entre os órgãos de polícia criminal e destes com as autoridades judiciárias, no âmbito do dever de cooperação estabelecido na lei de organização da investigação criminal* (...)".

Pelas bandas de cá, Ministérios Públicos e Polícias, nas esferas federal e estaduais, têm-se notabilizado pelo desenvolvimento e compartilhamento de métodos inovadores para a análise otimizada de massas de dados, a fim de fortalecer não apenas os mecanismos de repressão como de prevenção à corrupção, à lavagem de capitais, ao financiamento do terrorismo e a outros crimes graves, em linha com as recomendações do Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (GAFI/FATF). Tal cenário, entretanto, seria profundamente afetado com a eventual aprovação, ainda que parcial, de texto semelhante ao do anteprojeto referido.

Pode-se afirmar, sem qualquer exagero, que eventual aprovação do anteprojeto promoverá a proteção de dados em direção à insegurança pública e à não persecução penal.