UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
NÍVEL MESTRADO

BIANCA KAINI LAZZARETTI

O USO DE DADOS PESSOAIS E A SEGURANÇA PÚBLICA:
perspectivas práticas e teóricas da regulação no Brasil

São Leopoldo
2022

BIANCA KAINI LAZZARETTI

O USO DE DADOS PESSOAIS E A SEGURANÇA PÚBLICA:
perspectivas práticas e teóricas da regulação no Brasil

Dissertação apresentada como requisito parcial para obtenção do título de Mestra em Direito, pelo Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos (UNISINOS).

Orientadora: Prof.ª Dra. Raquel von Hohendorff

São Leopoldo

2022

L432u Lazzaretti, Bianca Kaini.
O uso de dados pessoais e a segurança pública : perspectivas práticas e teóricas da regulação no Brasil / Bianca Kaini Lazzaretti. – 2022.
150 f. : il. ; 30 cm.

Dissertação (mestrado) – Universidade do Vale do Rio dos Sinos, Programa de Pós-Graduação em Direito, 2022.
"Orientadora: Profa. Dra. Raquel von Hohendorff"

1. Direito constitucional -- Leis. 2. Proteção de dados -- Leis. 3. Proteção de dados -- regulação 4. Segurança pública. I. Título.

CDU 34

Dados Internacionais de Catalogação na Publicação (CIP)
(Bibliotecária: Silvana Dornelles Studzinski – CRB 10/2524)

UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO – PPGD
NÍVEL MESTRADO

A dissertação intitulada: "**O USO DE DADOS PESSOAIS E A SEGURANÇA PÚBLICA: perspectivas práticas e teóricas da regulação no Brasil"**, elaborada pela mestranda Bianca Kaini Lazzaretti**,** foi julgada adequada e aprovada por todos os membros da Banca Examinadora para a obtenção do título de MESTRE EM DIREITO.

São Leopoldo, 30 de setembro de 2022.

Prof. Dr. **Anderson Vichinkeski Teixeira,**
Coordenador do Programa de Pós-Graduação em Direito.

Apresentada à Banca integrada pelos seguintes professores:

Presidente: Dra. Raquel von Hohendorff_____*Participação por Webconferência*_____

Membro: Dra. Taysa Schiocchet _____*Participação por Webconferência*_____

Membro: Dr. Wilson Engelmann_____*Participação por Webconferência*_____

AGRADECIMENTOS À CAPES

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Para minha avó Lucena, que viu minha entrada no mestrado de perto, mas que acompanhou a conclusão desta etapa a uma distância irremediável.

AGRADECIMENTOS

Não há outra forma de começar meus agradecimentos, senão por aquela que sempre me apoiou e deu forças para enfrentar o mundo: minha mãe. A ela, a mais pura gratidão por todo sacrifício, carinho e confiança. Que eu possa sempre retribuir e multiplicar tudo isso.

Um agradecimento a toda minha família pelos momentos de descontração, de aconselhamento, de apoio, de paciência. Sou feliz por poder contar com pessoas tão bondosas, que me ensinam a empatia e aquecem meu coração.

Sou grata aos meus amigos, os de Três Coroas e os espalhados pelo mundo, mas especialmente àqueles que me acompanharam de perto durante a elaboração deste trabalho. À querida amiga Anita da Cunha, que me auxiliou desde o pré-projeto até a redação final da dissertação, com preciosas considerações e trocas.

Gratidão especial para aquela que, além de amiga, foi colega nos dois anos de mestrado e passou pela tensão da dissertação agora, assim como eu: Victória Frainer. Obrigada pelo apoio e incentivo.

Agradeço aos professores, à secretaria e ao atendimento do PPGD da Unisinos. Cada minuto na universidade é valioso para mim. Sou grata por todas as oportunidades, ensinamentos e por todo o auxílio recebido nesta instituição, que tenho orgulho de chamar de “segunda casa”.

Também preciso agradecer aos professores presentes na banca de qualificação desta dissertação, Profa. Dra. Taysa Schiocchet e Prof. Wilson Engelmann. Vocês são inspiração e têm forte influência na Bianca pesquisadora.

Por fim, minha imensa gratidão à minha orientadora, Profa. Dra. Raquel von Hohendorff. Que sorte a minha ter você na minha vida. Obrigada por todo o suporte e confiança. Conta comigo!

Dentre tantas coisas ruins que aconteceram ao longo desses dois anos – perdas para a morte, perdas para a vida, Covid-19, crises em diversos níveis – vocês são a minha razão para acreditar, para sorrir, para agradecer. Obrigada por tudo.

“Tudo deve tornar-se visível; o imperativo da transparência coloca em suspeita tudo o que não se submete à visibilidade. E é nisso que está seu poder e sua violência”.[1]

[1] HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis: Vozes, 2017. p. 35.

RESUMO

Em um contexto de rápida evolução tecnológica, em que se tem uma hiperconexão, a quantidade de dados pessoais disponíveis e as possibilidades de sua utilização são sem precedentes. Diversas práticas já aplicam tecnologias de análise desses dados sob justificativa de prevenção e repressão penal. Com a necessidade de conciliar os direitos fundamentais à proteção de dados pessoais e à segurança pública, têm se destacado algumas propostas de regulação da temática – a principal é o Projeto de Lei nº 1.515, de 2022, apresentado à Câmara dos Deputados. Nesse sentido, o presente trabalho é movido pela seguinte questão de pesquisa: em que medida a proposta da LGPD penal (Projeto de Lei nº 1.515 de 2022) limita e garante o direito fundamental à proteção de dados pessoais dentro do contexto da garantia da segurança pública em sentido amplo? Para responder a essa pergunta, a pesquisa desenvolveu-se pelo método sistêmico-construtivista. A dissertação divide-se em duas partes: a primeira, exploratória, visa conceituar e identificar os dados pessoais e possíveis usos na esfera penal; a segunda, de natureza descritiva, busca definir os direitos fundamentais colidentes, com a identificação das possibilidades de restrição e o "limite aos limites" impostos por um direito sobre o outro. Conclui-se que o PL nº 1.515/2022 sobrevaloriza a segurança pública, invadindo o núcleo essencial do direito fundamental à proteção de dados pessoais, mais limitando este último direito do que garantindo-o.

Palavras-chave: proteção de dados pessoais; segurança pública; LGPD; direito constitucional.

ABSTRACT

In a context of rapid technological evolution, hyperconnected, the amount of personal data available and the possibilities of its use are unprecedented. Several practices already apply technologies to analyze these data under the justification of criminal prevention and repression. With the need to reconcile the fundamental rights to personal data protection and public safety, some proposals for regulation of the theme have stood out - the main one being Bill no. 1.515, of 2022, presented to the House of Representatives of Brazil. In this sense, the present work is driven by the following research question: to what extent does the proposed criminal LGPD (Bill No. 1.515 of 2022) limit and guarantee the fundamental right to the protection of personal data within the context of ensuring public security in a broad sense? To answer this, the research used the systemic-constructivist method. The dissertation is divided into two parts: the first, exploratory, aims to conceptualize and identify personal data and possible uses in the criminal sphere; the second, descriptive, seeks to define the colliding fundamental rights, with the identification of the possibilities of restriction and the "limit to the limits" imposed by one right over the other. We conclude that the Bill no. 1.515/2022 overvalues public security, invading the essential core of the fundamental right to the protection of personal data, limiting the latter right rather than guaranteeing it.

Keywords: personal data protection; public safety; GDPR; constitutional law.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

No Brasil, a Lei Geral de Proteção de Dados brasileira (LGPD), Lei nº 13.709/2018, entrou plenamente em vigor em 1º de agosto de 2021.[2] A norma é considerada o principal marco regulatório acerca do tema no país, apresentando conceitos, princípios e finalidades basilares para as práticas de processamento de dados.

Apesar de todo avanço na proteção regulatória dos dados, a LGPD excluiu de seu âmbito de aplicação, expressamente, o tratamento de dados realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão penal (artigo 4º).[3] Por isso, em 2020, foi instituída uma comissão de juristas para elaboração de uma proposta de lei de proteção de dados na área penal,[4] que resultou em um anteprojeto apresentado à Câmara dos Deputados.[5] Depois, em julho de 2022, foi protocolado o Projeto de Lei nº 1.515 de 2022, também visando regulamentar a matéria.[6]

Em fevereiro de 2022, foi aprovada a Emenda Constitucional nº 115, de 2022, que acrescentou ao artigo 5º da Constituição Federal o inciso LXXIX, prevendo explicitamente a proteção de dados pessoais como direito fundamental.[7] Diante desse cenário, em que se tem um direito fundamental recentemente reconhecido, uma lacuna legislativa acerca da proteção de dados na esfera penal, bem como uma

---

2 A *vacatio legis* era, inicialmente, de 24 meses a partir da publicação da Lei. Entretanto, tal prazo foi estendido pela Lei nº 14.010/2020 e pela Medida Provisória nº 959/2020. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 ago. 2022.

3 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 ago. 2022.

4 ANTEPROJETO de lei disciplina proteção de dados em investigações criminais. **Consultor Jurídico**, São Paulo, 31 out. 2020. Disponível em: https://www.conjur.com.br/2020-out-31/anteprojeto-disciplina-protecao-dados-investigacoes-criminais. Acesso em: 28 fev. 2022.

5 CORDEIRO, Nefi *et al.* **Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal**. Brasília, DF, 2020. Disponível em: https://www.conjur.com.br/dl/anteprojeto-lei-disciplina-protecao.pdf. Acesso em: 28 fev. 2022.

6 ARMANDO, Coronel. **Projeto de lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 7 jun. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node09wqlrgv9qemi1qa4zbdv699tb12566378.node0?codteor=2182274&filename=Tramitacao-PL+1515/2022. Acesso em: 1 ago. 2022.

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

proposta de regulação da matéria, faz-se relevante questionar: em que medida a proposta da LGPD penal (Projeto de Lei nº 1.515 de 2022) limita e garante o direito fundamental à proteção de dados pessoais dentro do contexto da garantia da segurança pública em sentido amplo? É esta pergunta que norteia esta dissertação.

Como objetivo geral, busca-se analisar a proposta de regulamentação da proteção de dados pessoais no âmbito penal à luz de sua função de limitação ao direito fundamental à proteção de dados. Como objetivos específicos, correspondentes a determinados itens do trabalho, pretende-se:

a) explorar os conceitos atinentes ao tratamento de dados pessoais, de modo a possibilitar a compreensão sobre as atividades de processamento desses dados na esfera penal (capítulo 2.1);
b) mapear as possibilidades de utilização dos dados pessoais nas investigações criminais e na persecução penal, mediante análise de casos e acontecimentos relacionados (capítulo 2.2);
c) identificar os contornos do direito fundamental à proteção de dados pessoais, a fim de determinar seu âmbito de proteção e seus modificadores (capítulo 3.1);
d) investigar a teoria dos direitos fundamentais, aproximando as noções de âmbito de aplicação, limites e limites aos limites impostos a esses direitos com a temática em estudo (capítulo 3.1);
e) analisar o Projeto de Lei nº 1.515 de 2022 à luz do direito fundamental à proteção de dados pessoais e considerando os limites e permissões gerados pela sua aplicação (capítulo 3.2);
f) pesquisar as normas vigentes que tratem de proteção ou de hipóteses de tratamento de dados e que possam ser aplicadas à esfera da segurança pública (capítulo 3.2).

O trabalho está organizado de acordo com o método francês, composto de duas partes, cada uma com dois capítulos. Isso porque, sob o ponto de vista metodológico, a pesquisa é inicialmente exploratória, na medida em que a primeira parte pretende oportunizar maior familiaridade com o problema, tornando-o mais explícito e considerando diversos aspectos a ele relacionados,[8] recorrendo a fontes

[8] GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2018. *E-book* (não paginado). Disponível em:

não restritas à área do direito. Posteriormente, a segunda parte possui natureza descritiva, abordando o ordenamento jurídico à luz da teoria dos direitos fundamentais.

A vertente teórico metodológica a que se filia esta dissertação é a jurídico-social, tendo em vista que se preocupa com a realização concreta do direito, considerando sua eficiência, eficácia e efetividade.[9] Ademais, mescla elementos de pesquisa teórica e empírica, caracterizando-se como qualitativa, com a coleta e análise de uma variedade de recursos que permitam compreender o fenômeno social estudado.

A investigação é orientada pelo método sistêmico-construtivista, que considera a realidade como uma construção de um observador, que analisa todas as peculiaridades implicadas na observação. Ele pressupõe reflexões a partir de um conjunto de categorias teóricas, advindas da Matriz Pragmático-Sistêmica,[10] que possuem coerência teórica auto-referencial. Essa escolha permite a compreensão de múltiplas dinâmicas comunicativas em um ambiente complexo, como é o caso do contexto criado pelas novas tecnologias, visto se tratar de uma estratégia autopoiética de reflexão jurídica.[11]

Como técnicas de pesquisa, utiliza-se pesquisa bibliográfica, com uso de material publicado em livros, periódicos e anais de eventos científicos, por exemplo, com suporte físico ou virtual; e pesquisa documental, por meio do levantamento e análise de projetos de lei, legislação vigente e outros documentos normativos, bem como relatórios.

---

https://integrada.minhabiblioteca.com.br/#/books/9788597012934/cfi/6/10!/4/8@0:53.2. Acesso em: 25 jul. 2022.

9 GUSTIN, Miracy Barbosa de Sousa; DIAS, Tereza Fonseca; NICÁCIO, Camila Silva. **(Re)pensando a pesquisa jurídica**: teoria e prática. 5. ed. rev., ampl. e atual. São Paulo: Almedina, 2020.

10 "É a perspectiva da Matriz Pragmático-Sistêmica, que nos permite a incursão na Teoria dos Sistemas Sociais de Niklas Luhmann, assim como, na obra de outros autores que compartilham da mesma perspectiva e consideram em suas reflexões categorias como paradoxo, complexidade, contingência e policontexturalidade". ROCHA, Leonel Severo. **Epistemologia jurídica e democracia**. 2. ed. São Leopoldo: UNISINOS, 2003. p. 100.

11 HOHENDORFF, Raquel von. **A contribuição do *safe by design* na estruturação autorregulatória da gestão dos riscos nanotecnológicos**: lidando com a improbabilidade da comunicação inter-sistêmica entre o direito e a ciência em busca de mecanismos para concretar os objetivos de sustentabilidade do milênio. 478 p. Tese (Doutorado em Direito) – Universidade do Vale do Rio dos Sinos. Programa de Pós-Graduação em Direito, São Leopoldo, 2018. p. 28-29. Disponível em: http://www.repositorio.jesuita.org.br/handle/UNISINOS/7055. Acesso em: 22 jul. 2022.

A justificativa para a escolha do problema está na atualidade da temática, visto que cada vez mais se implementam tecnologias que permitem a utilização de dados pessoais pelo Estado, muitas vezes sem que haja lei autorizando ou sem que se questione a necessidade de regulação. Especialmente nos últimos anos, houve uma intensificação na coleta de dados da população – ampliando os riscos e possibilidades inerentes à prática, à margem do Direito, que avança lentamente quando comparado à tecnologia.[12]

Além disso, há relevância em tal análise também sob o ponto de vista teórico, visto que a legislação e as práticas relacionadas ao tratamento de dados pessoais no âmbito da segurança pública avançam rapidamente. Assim, é fundamental o estudo da efetividade das garantias constitucionais e infraconstitucionais, visando a proporcionalidade entre o resguardo do interesse público e das liberdades individuais, correlacionando teoria e prática – o que se pretende com esse estudo.

A pesquisa também possui relevância social, eis que o Estado já coleta dados dos cidadãos, como se verá no item 2.2. Com mais dados disponíveis, surgem novas utilizações e variadas consequências para os indivíduos e para a coletividade. A intenção, nesse sentido, é colocar em debate essa utilização em massa de informações da população, de modo a dar visibilidade e impulsionar a discussão sobre o tema, por meio da avaliação da constitucionalidade destas práticas.

Por fim, cabe destacar que esta dissertação se adequa à Linha de Pesquisa Sociedade, Novos Direitos e Transnacionalização (Linha 2) do Programa de Pós-Graduação em Direito (PPGD) da Unisinos. Conforme informação disponível no *site* do PPGD, as pesquisas desenvolvidas nesta linha visam investigar temáticas ligadas às mudanças operadas no Direito por elementos como transformações institucionais e a globalização. Os estudos possuem, também, enfoque nos direitos exsurgentes, como é o caso dos direitos humanos e fundamentais e dos direitos e deveres gerados pelas novas tecnologias, priorizando uma perspectiva transdisciplinar na discussão da Sociedade, por meio de aportes teóricos contemporâneos. Além disso, está alinhado às pesquisas da Profa. Dra. Raquel von Hohendorff, orientadora deste trabalho, na

[12] O fundamento para tal argumento pode ser facilmente vislumbrado tomando como exemplo a Lei Geral de Proteção de Dados brasileira: sua publicação se deu em 2018, mas sua vigência só se implementou completamente em 2021 – três anos depois. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jun. 2022.

medida em que versa sobre inovação tecnológica, partindo de uma perspectiva transdisciplinar, ligada à noção de complexidade.

Dentro desse contexto, importante destacar a relevância do estudo enquanto pesquisa aplicada. Utilizando um olhar transdisciplinar e sistêmico-construtivista, o trabalho pretende abordar o problema de modo que seja possível oferecer um retorno para a sociedade, causando impacto não somente teórico, mas também social com os resultados obtidos.

2 CONTEXTUALIZANDO O USO DE DADOS PESSOAIS PARA FINS DE GARANTIA DA SEGURANÇA PÚBLICA SOB UMA PERSPECTIVA TRANSDISCIPLINAR E VOLTADA PARA AS PRÁTICAS SOCIAIS

Quando se ouve falar em vigilância, é comum pensar em algumas figuras icônicas consolidadas após muitas décadas de debates sobre o assunto. É o caso do Grande Irmão, entidade ficcional criada por Orwell na obra 1984, que tudo vê para tudo controlar.[13] Outra imagem que pode vir à mente é a do pan-óptico de Bentham, que representa a prisão ideal, na qual os guardas têm total visão dos apenados, que por sua vez não veem nada.[14] Porém, todos esses modelos incorporados a um certo senso comum acerca da vigilância já não dão mais conta de representar o fenômeno na atualidade.

Para compreender o contexto contemporâneo, faz-se relevante observar, ainda que superficialmente, a trajetória que se traçou até o momento enquanto evolução da vida em sociedade. Nesse sentido, a história pode ser contada de diversas maneiras.

Uma das abordagens possíveis é a que considera as profundas alterações no modo de viver como revoluções. Assim, pode-se falar na Revolução Agrícola, na Industrial e na Digital, bem como na Quarta Revolução Industrial, sentida atualmente. Enquanto a Terceira Revolução Industrial foi marcada pelo surgimento dos computadores pessoais e da Internet, dentre outros avanços tecnológicos, a Quarta Revolução constitui a evolução e a interconexão de toda essa tecnologia com outros espaços, especialmente o físico, digital e biológico.[15]

Dessa maneira, criam-se possibilidades tecnológicas com velocidade e profundidade inéditas. Com a evolução de uma computação cada vez mais minúscula, surgiu e populariza-se um mercado de produtos inteligentes, vestíveis ou que possam ser incorporados a todos os espaços da vida humana – casa, trabalho, carro etc. Esses equipamentos são conectados à Internet (cada vez mais rápida e acessível), constantemente coletando, armazenando e compartilhando dados que formam o *Big Data*, tornando-se informações geralmente por meio de análises mediadas por algoritmos e inteligência artificial.

---

13 ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2014.
14 FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. 27. ed. [*S. l.*]: Petrópolis, 1987.
15 SCHWAB, Klaus. **A Quarta Revolução Industrial**. 1. ed. São Paulo: EDIPRO, 2019. *E-book* (não paginado).

Os impactos dessa Revolução são sentidos aos poucos e dificilmente podem ser completamente antecipados. Isso porque a incerteza é elemento constitutivo importante do risco, do qual não é possível se desvencilhar mais na sociedade contemporânea, especialmente no cenário da inovação.[16] Entretanto, para que o pleno potencial tecnológico seja desfrutado e os efeitos negativos sejam mitigados, é necessário pensar esses resultados a partir da realidade já conhecida.

Nesse sentido, ao olhar para o mundo atual, identifica-se um ambiente hipercontectado. De acordo com Magrani, a noção de hiperconectividade foi firmada:

> [...] para descrever o estado de disponibilidade dos indivíduos para se comunicar a qualquer momento. Esse termo possui alguns desdobramentos importantes. Podemos citar alguns deles: o conceito de *always-on*, estado em que as pessoas estão conectadas a todo o momento; a possibilidade de estar prontamente acessível (*readily accessible*); a riqueza de informações; a interatividade; e o armazenamento ininterrupto de dados (*always recording*). O termo hiperconectividade encontra-se hoje atrelado às comunicações entre indivíduos (*person-to-person*, P2P), indivíduos e máquina (*human-to-machine*, H2M) e entre máquinas (*machine-to-machine*, M2M) valendo-se, para tanto, de diferentes meios de comunicação. Há, neste contexto, um fluxo contínuo de informações e uma massiva produção de dados.[17]

Assim, os espaços contemporâneos são repletos de aparelhos que gravam som e imagem constantemente, equipados com sistemas de geolocalização, que têm acesso irrestrito e constante aos mais diversos dados pessoais (inclusive sensíveis). Incentiva-se uma hiperconectividade, sendo normal expor os mais íntimos detalhes de corpo e mente. A vigilância, nesse cenário, é uma atividade que merece atenção renovada.

Por isso, atualmente, há uma grande preocupação com a proteção dos dados pessoais coletados, processados, armazenados e tratados por meio de novas tecnologias. Termos como *Big Data*, algoritmos, inteligência artificial, dentre outros, popularizaram-se nos últimos anos, ultrapassando a área da ciência da computação e ganhando um espaço cada vez maior nos debates jurídicos e sociais.

Este capítulo (2) contextualiza a coleta e o tratamento de dados pessoais, especialmente com finalidade de garantia da segurança pública. No primeiro item

---

[16] AREOSA, João. A globalização dos riscos sociais e os acidentes tecnológicos. **Pensamiento Americano**, Barranquilla, v. 9, n. 17, p. 151-176, jul./dez. 2016.

[17] MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019. p. 20.

(2.1), são apresentados conceitos relativos ao universo dos dados pessoais, buscando situar o leitor na problemática e fornecer subsídios para a compreensão sobre as atividades de processamento desses dados na esfera da segurança. Já o segundo (2.2) possui caráter mais específico, mapeando iniciativas e acontecimentos que caracterizam o uso de dados pessoais no âmbito da segurança pública.

Antes de prosseguir, é importante destacar que esta parte da pesquisa é orientada por uma perspectiva exploratória. Portanto, visa delimitar melhor os contornos da problemática abordada, por meio da utilização de referências oriundas de outras áreas do conhecimento – em uma perspectiva transdisciplinar – e pela observação de casos concretos, com um viés empírico de identificação de narrativas e práticas sociais.

Esta abordagem transdisciplinar, inclusive, justifica-se na medida em que esse olhar pode auxiliar na compreensão do objeto aqui em estudo – que é naturalmente relacionado a mais de uma área do conhecimento, situando-se na fronteira entre ciências matemáticas, da computação, sociais, de engenharia, e outras. Isso porque, como explica Hohendorff:

> Em função da globalização, o papel do jurídico desloca-se sucessivamente de uma perspectiva estrutural (preocupada com questões normativas do direito) para uma perspectiva funcionalista (voltada para as funções sociais do direito), possibilitando ao Direito o uso de técnicas transdisciplinares. Assim, cabe ao Direito o uso de técnicas transdisciplinares, de modo a não mais permanecer inerte e estanque frente aos novos desafios trazidos pela revolução tecnocientífica.[18]

Ainda, considerando a extensão e a complexidade da realidade estudada, relevante deixar claro que não é o objetivo o esgotamento da temática. Isso porque considera-se tarefa inexecutável a de abordar todos os conceitos e casos que podem ser úteis para a compreensão do uso de dados pessoais com finalidade de garantia da segurança na esfera pública. Em primeiro lugar, porque se trata de tecnologias em transformação constante e ágil. Os conceitos aqui trabalhados já estão, de certa forma, estabelecidos – motivo pelo qual se considera que são úteis a análise e não estarão obsoletos tão rapidamente. Em segundo lugar, é impossível dominar todas as

[18] HOHENDORFF, Raquel Von. Revolução nanotecnológica, riscos e reflexos no Direito: os aportes necessários da Transdisciplinaridade. *In*: ENGELMANN, Wilson; WITTMANN, Cristian (org.). **Direitos humanos e novas tecnologias**. Jundiaí: Paco Editorial, 2015. p. 32.

práticas sociais, que são cada vez mais plurais no mundo globalizado. Portanto, foram selecionados os fatos que melhor exemplifiquem o uso já existente e as perspectivas para o futuro próximo da tecnovigilância.

2.1 Noções conceituais acerca da coleta e do tratamento de dados pessoais

Para compreender o tratamento de dados pessoais, sua realização pelos mais diversos atores e por meio de variados instrumentos, importa conceituar, primeiramente, o que são dados.[19] De acordo com Hoffmann-Riem, eles são sinais ou símbolos que podem ser reproduzidos e transportados por meios técnicos e que não possuem significado intrínseco.[20] Além disso, pode-se qualificar os dados como pessoais quando estão vinculados a uma pessoa singular, sendo capazes de identificá-la e individualizá-la.[21] O seguinte quadro apresenta uma lista de dados considerados pessoais:

Quadro 1 – Tipos de dados pessoais

Tipo de dado pessoal	**Exemplos**
Conteúdo criado pelo usuário	Postagens em blogs, fotos, vídeos
Dados sobre atividades e comportamentos	Inclui o que as pessoas procuram e veem na Internet, suas compras online, quanto e como pagam
Dados sociais	Contatos e amigos em redes sociais
Dados de localização	Endereço, geolocalização, endereço IP
Dados demográficos	Idade gênero, raça, renda, preferências sexuais, filiação política
Dados de identificação	Nome, dados financeiros, de saúde, números de documentos, registros policiais
Dados biométricos	Impressões digitais, face, geometria da mão, dinâmica do caminhar, assinatura, DNA

Fonte: adaptado da OECD[22] e ampliado pela autora com base em Loureiro e Carneiro.[23]

---

19 Com relação à conceituação apresentada neste trabalho para os dados, priorizou-se a perspectiva trazida por autores que pesquisam as relações entre Direito e tecnologia em detrimento de uma abordagem mais voltada para a técnica da ciência da computação, eis que assim já se restringe a perspectiva ao objeto do trabalho.

20 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021.

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

22 OECD. **Exploring the economics of personal data**: a survey of methodologies for measuring monetary value: OECD Digital Economy Papers. [*S. l.*]: OECD, 2013. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en. Acesso em: 13 ago. 2022.

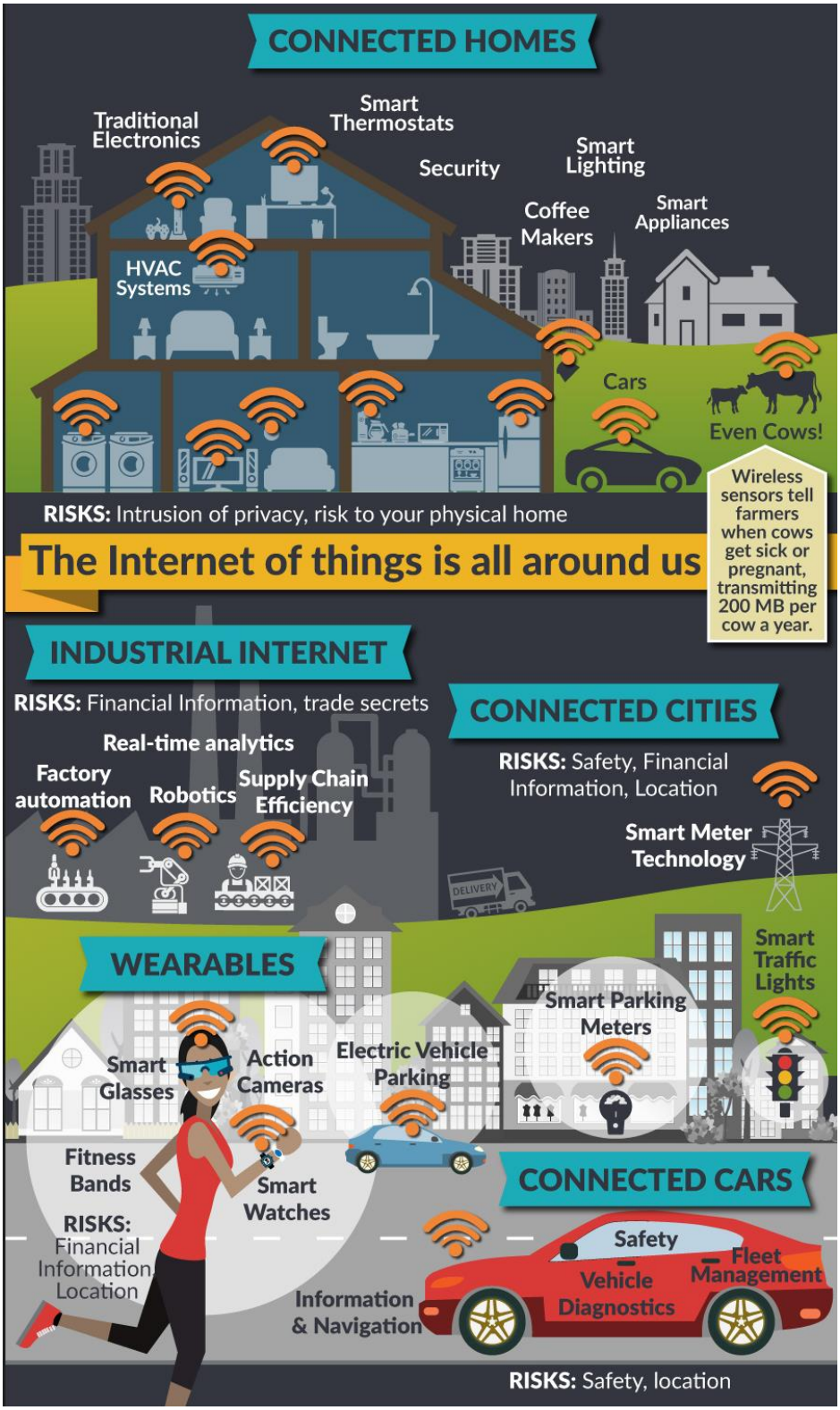
23 LOUREIRO, Maria Fernanda Battaglin; CARNEIRO, João Víctor Vieira. Problematizando o direito à privacidade e à proteção de dados pessoais em face da vigilância biométrica. **Teknokultura**: Revista de Cultura Digital y Movimientos Sociales, Madrid, v. 17, n. 2, p. 204–213, 2020.

Toda esta variedade de dados pode ser colhida por diversos meios. Aparelhos como computadores, *smartphones*, câmeras e diversos outros são comuns na maior parte dos ambientes urbanos. Entretanto, em um contexto de Quarta Revolução Industrial, hiperconectado, ganha destaque a noção de *Internet of Things* (IoT), ou Internet das coisas. De acordo com Magrani, trata-se de "[...] um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas [...]".[24] Criam-se, assim, cada vez mais equipamentos conectados à rede e entre si (vide figura 1), que coletam dados pessoais o tempo todo.

Disponível em: https://revistas.ucm.es/index.php/TEKN/article/view/69479. Acesso em: 30 ago. 2022.

[24] MAGRANI, Eduardo. **Internet das coisas**. Rio de Janeiro: FGV, 2018. *E-book*. p. 20.

Figura 1 – Infográfico com tipos de IoTs



Fonte: adaptado de Computer Science Zone.[25]

[25] SECURITY and the internet of things. *In*: COMPUTER Science Zone, [*s. l.*], 2015. Disponível em: https://www.computersciencezone.org/security-internet-of-things/. Acesso em: 14 ago. 2022.

Esses dados, coletados por uma diversidade cada vez maior de eletrônicos, ao se tornarem objeto da comunicação (entre humanos ou máquinas), podem receber significado e portar informações.[26] Como aponta Bioni, dados e informações, apesar de serem muito utilizados como sinônimos, não o são: “O dado é o estado primitivo da informação, pois não é algo *per se* que acresce conhecimento. Dados são simplesmente *fatos brutos* que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação”.[27] Assim, dados seriam matéria bruta, ainda não processada ou ressignificada, enquanto a informação faria referência a algo que está além do dado, atribuindo a ele uma depuração inicial de conteúdo.[28] Essa distinção também é feita por Floridi, segundo o qual dados fazem parte de uma noção mais ampla, visto que não são encontrados estruturadamente e, para serem considerados informações, devem passar por um tratamento que lhes confira certas qualidades (*well-formed*, *meaningful* e *truthful data*).[29]

Por outro lado, dentro do sistema do Direito, merecem destaque os conceitos apresentados pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), principal marco normativo sobre a temática. É no artigo 5º que a LGPD define dado pessoal, dado pessoal sensível e dado anonimizado, bem como o tratamento:

> 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;
> III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; [...]
> 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

---

26 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021.

27 BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 36.

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

29 FLORIDI, Luciano. Semantic Conceptions of Information. *In*: ZALTA, Edward (ed.). **The Stanford Encyclopedia of Philosophy**. [Stanford: Stanford University], Winter 2019. Disponível em: https://plato.stanford.edu/entries/information-semantic/. Acesso em: 15 jun. 2022.

> informação, modificação, comunicação, transferência, difusão ou extração; [...].[30]

É possível notar que a LGPD mistura os conceitos de dado e informação, na medida em que define dados como informações. Entretanto, quando fala do tratamento, menciona “informação” ao tratar da “avaliação” dos dados, transparecendo, também, uma certa diferenciação.

Quanto aos dados pessoais sensíveis, verifica-se que são aqueles que têm maior potencial de causar discriminação,[31] marginalização e segregação. Por isso, recebem proteção especial na LGPD, somente podendo ser tratados em casos específicos, elencados no artigo 11. Nesse sentido, a anonimização dos dados pode ser uma ferramenta relevante, na medida em que, conforme disposto no inciso III, o dado anonimizado não é relacionável a um titular.[32]

O tratamento dos dados, como visto na definição legal, abrange uma série de ações que podem ser tomadas. Muitas delas são realizadas com o auxílio de ferramentas como os algoritmos. Hoffmann-Riem os define como regras de ação adotadas em etapas para a resolução de problemas, incorporadas ao meio digital (embora não seja uma novidade criada pelas tecnologias computacionais).[33] Sendo assim, eles caracterizam, inclusive, os códigos que formam um programa de computador.

Uma utilização que se faz dos algoritmos se dá por meio da inteligência artificial (IA). Conceituar a IA, entretanto, não é uma tarefa simples nem breve.[34] De acordo com Russell e Norvig, trata-se de um campo de estudo que busca “não apenas compreender, mas também construir entidades inteligentes”.[35] Para eles, há uma

---

30 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 jul. 2022.

31 KIRA, Beatriz; TAMBELLI, Clarice Nassar. **Data protection in Brazil**: critical analysis of the Brazilian legislation. São Paulo: InternetLab, 2016. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2017/03/Legal-Framework-Analysis-Brazil.pdf. Acesso em: 20 out. 2022.

32 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 jul. 2022.

33 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021.

34 Razão pela qual não se pretende exaurir o assunto. A finalidade, então, é expor as noções fundamentais para a compreensão do que é a IA e seus desdobramentos, de modo que posteriormente se possa avaliar os potenciais riscos e benefícios de seu uso em termos de uso de dados pessoais pelo Estado para fins de garantia da segurança pública.

35 RUSSELL, Stuart; NORVIG, Peter. **Inteligência artificial**. Rio de Janeiro: Elsevier, 2013. *E-book* (não paginado).

variedade de definições possíveis, alinhadas a categorias diversas que têm se desenvolvido ao longo dos anos, de forma independente, porém conectada, a depender da área de estudo e da sua finalidade. Assim, a IA pode ser associada ao comportamento ou ao raciocínio, imitando a razão ou as ações humanas, ou, ainda, mensurando seu sucesso a partir de um ideal de racionalidade (não necessariamente alcançado pelo ser humano).[36]

De maneira geral e resumida, pode-se compreender a IA "[...] como o desenvolvimento de ferramentas informáticas que emulem a inteligência humana ou que executem funções a ela relacionadas, tais como raciocínio, aprendizagem, adaptabilidade, percepção e interação com o meio físico etc.".[37] Para Hoffmann-Riem, o objetivo dos sistemas de IA seria a reprodução digital de modelos de tomada de decisão, visando a resolução de problemas.[38]

Um avanço nessa tecnologia é o fato de que, cada vez mais, ela consegue se autodesenvolver independentemente da intervenção humana.[39] Isso ocorre por meio do que se chama de *machine learning* (aprendizado de máquina), que é a capacidade que um sistema possui de aprender com base em dados anteriormente fornecidos (classificados por seres humanos ou não), realizando associações e apresentando conclusões na forma de previsões, exprimidas como novos dados. Essa atividade é possibilitada pelo processamento de linguagem natural (*natural language processing*), que é a capacidade de um programa computacional compreender e transformar a linguagem humana em linguagem de programação.[40]

Esse aprendizado de máquina pode ser de natureza profunda. O *deep learning*, como é conhecida essa modalidade, pode ser caracterizado como um processo em que "o próprio algoritmo detecta seus erros e realiza os ajustes necessários para

---

36 RUSSELL, Stuart; NORVIG, Peter. **Inteligência artificial**. Rio de Janeiro: Elsevier, 2013. *E-book* (não paginado).

37 MEDINA, José Miguel Garcia; MARTINS, João Paulo Nery dos Passos. A era da inteligência artificial: as máquinas poderão tomar decisões judiciais? **Revista dos Tribunais**, [*s. l.*], v. 1020/2020, p. 2, out. 2020. Disponível em: https://cutt.ly/0knyKSP. Acesso em: 15 jan. 2022.

38 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021.

39 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021.

40 TACCA, Adriano; ROCHA, Leonel Severo. Inteligência artificial: reflexos no sistema do direito. **Revista do Programa de Pós-Graduação em Direito da UFC**, Fortaleza, v. 38, n. 2, p. 53–68, jul./dez. 2018. Disponível em: www.periodicos.ufc.br/nomos/article/ download/20493/95963. Acesso em: 15 jan. 2022.

aprimorar seus resultados".[41] Frequentemente, os modelos de aprendizagem profunda operam por meio de *artificial neural networks*, que são sistemas computacionais que imitam, rudimentarmente, as redes neurais biológicas – compostas por "bilhões de células – os neurônios –, que controlam cada função e parte do nosso organismo"[42] e se relacionam por sinapses, formando uma rede capaz de processar e armazenar informação. Essas redes neurais artificiais, atualmente, já contam com diversas camadas intermediárias, responsáveis por tarefas específicas, que possibilitam o uso da IA em problemas cada vez mais complexos.[43]

Nota-se que a tecnologia permite um tratamento cada vez mais intenso e amplo de dados. Nesse sentido, tem-se a noção de *Big Data*, que, de acordo com Hoffmann-Riem, pode ser definido como o uso de uma grande quantidade e variedade de dados.[44] Ele também é qualificado como uma tecnologia capaz de agregar diversos dados distintos, transformando-os em um só.[45] Identificam-se algumas características do *Big Data*:

Quadro 2 – Características do *Big Data*

Volume - *High Volume*	Enorme quantidade de dados processados
Variedade - *High Variety*	Grande variedade de tipos de dados e formas de tratamento
Velocidade - *High Velocity*	Processamento muito rápido de dados
Veracidade - *Veracity*	Possibilidade de aplicação de IA para verificação de qualidade
Valor - *Value*	Como consequência, os dados adquirem elevado valor econômico

Fonte: elaborado pela autora com base em Hoffmann-Riem[46] e Lindoso.[47]

41 BOEING, Daniel Henrique Arruda; ROSA, Alexandre Morais da. **Ensinando um robô a julgar**: pragmática, discricionariedade e vieses no uso de aprendizado de máquina no Judiciário. Florianópolis: Emais, 2020. p. 20.

42 GABRIEL, Martha. **Você, eu e os robôs**: pequeno manual do mundo digital. São Paulo: Atlas, 2018. p. 205.

43 BOEING, Daniel Henrique Arruda; ROSA, Alexandre Morais da. **Ensinando um robô a julgar: pragmática, discricionariedade e vieses no uso de aprendizado de máquina no Judiciário**. Florianópolis: Emais, 2020.

44 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021.

45 LINDOSO, Maria Cristine Branco. **Discriminação de gênero no tratamento automatizado de dados pessoais**: como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021. *E-book*.

46 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021.

47 LINDOSO, Maria Cristine Branco. **Discriminação de gênero no tratamento automatizado de dados pessoais**: como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021. *E-book*.

O atributo mais visível é o volume, tendo em vista que se destaca o crescimento de centros de processamento de dados em hiper escala, mantidos por 24 empresas operadoras.[48] Em 2016, existiam 338 e a projeção era de que essa quantidade quase dobrasse até 2021:

Figura 2 – Crescimento dos centros de processamento de dados em hiper escala

Fonte: CISCO.[49]

Em 2016, esses centros já eram responsáveis por processar 6,8 Zettabytes (ZB) por ano, com perspectiva de que esse volume de dados aumentaria para 20,6 ZB até 2021.[50] Para colocar em perspectiva, 1 ZB equivale a 1.099.511.627.776 de Gigabytes (GB). Pensando que o iPhone 13 possui no mínimo 128 GB de armazenamento,[51] pode-se dizer que, para armazenar 6,8 ZB, seriam necessários

---

48 Para ser considerada uma operadora em hiper escala, uma empresa precisa atender a determinados critérios, baseados no rendimento anual, a depender da área de atuação. CISCO. **Cisco global cloud index**: forcast and methodology, 2016-2021. San Jose: Cisco Systems, 2018. Disponível em: https://virtualization.network/Resources/Whitepapers/0b75cf2e-0c53-4891-918e-b542a5d364c5_white-paper-c11-738085.pdf. Acesso em: 13 ago. 2022.

49 CISCO. **Cisco global cloud index**: forcast and methodology, 2016-2021. San Jose: Cisco Systems, 2018. Disponível em: https://virtualization.network/Resources/Whitepapers/0b75cf2e-0c53-4891-918e-b542a5d364c5_white-paper-c11-738085.pdf. Acesso em: 13 ago. 2022.p. 7.

50 CISCO. **Cisco global cloud index**: forcast and methodology, 2016-2021. San Jose: Cisco Systems, 2018. Disponível em: https://virtualization.network/Resources/Whitepapers/0b75cf2e-0c53-4891-918e-b542a5d364c5_white-paper-c11-738085.pdf. Acesso em: 13 ago. 2022.

51 BUY IPHONE 13. *In*: APPLE, [*S. l.*, 2022?]. Disponível em: https://www.apple.com/shop/buy-iphone/iphone-13. Acesso em: 13 ago. 2022.

58.411.555.225,6 de aparelhos – aproximadamente 7 iPhones por pessoa no planeta.[52] [53]

Como aponta Bioni, o *Big Data* utiliza um novo tipo de linguagem de processamento, que dispensa uma etapa trabalhosa e demorada de estruturação dos dados para posterior análise.[54] Trata-se da *not only structured query language* (NoSQL), que surge como alternativa à consolidada *structured query language* (SQL).[55]

Na SQL, tem-se um modelo relacional, em que os dados são estruturados ("seguem uma organização rígida e predeterminada, facilitando a sua recuperação e processamento de forma eficaz")[56] em linhas e colunas, formando tabelas que se relacionam com outras tabelas por meio de operadores específicos (projeção, seleção, junção e divisão).[57] Por outro lado, o processamento na NoSQL pode ser realizado com dados não estruturados, que possuem natureza dinâmica e flexível. Como apontam Pereira *et al*.: "Isso significa que não há um campo ou formato específico do dado que será inserido no arquivo, estando livre para conter inclusive diferentes tipos no mesmo documento. São exemplos de dados não estruturados imagens, textos, vídeos e documentos".[58]

Não sendo necessária prévia estruturação, economiza-se tempo, mesmo quando o volume de dados aumenta e se diversifica. Assim, como explica Bioni:

> [...] os dados passaram a ser analisados não mais em pequenas quantidades ou por amostras, mas em toda a sua extensão. Há um salto quanto ao volume de dados processados, tornando-se possível correlacionar uma série de fatos (dados), estabelecendo-se entre eles

---

52 Considerando a população mundial atual estimada em 7.967.279.270 pessoas. WORLDOMETER. **Real time world statistics**. [*S. l.*]: Worldometer, [2022?]. Disponível em: http://www.worldometers.info/. Acesso em: 13 ago. 2022.

53 Cálculo inspirado pelo realizado em: STUCKE, Maurice E.; GRUNES, Allen P. **Big data and competition policy**. Oxford, United Kingdom: Oxford University Press, 2016.

54 BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

55 Utilizada por empresas como Microsoft, Oracle, dentre outras. PUGA, Sandra; FRANÇA, Edson; GOYA, Milton. **Banco de dados**: implementação em SQL, PL/SQL e Oracle 11g. 1. ed. São Paulo: Pearson Education do Brasil, 2013. *E-book*.

56 PEREIRA, Mariana Araújo *et al*. **Framework de Big Data**. 1. ed. Porto Alegre: SAGAH, 2019. p. 142. *E-book*.

57 PUGA, Sandra; FRANÇA, Edson; GOYA, Milton. **Banco de dados**: implementação em SQL, PL/SQL e Oracle 11g. 1. ed. São Paulo: Pearson Education do Brasil, 2013. *E-book*.

58 PEREIRA, Mariana Araújo *et al*. **Framework de Big Data**. 1. ed. Porto Alegre: SAGAH, 2019. p. 144. *E-book*.

> relações para desvendar *padrões* e, por conseguinte, inferir, inclusive, *probabilidades* de acontecimentos futuros.[59]

Além disso, com o auxílio da IA, podem ser realizados diversos tratamentos com essa massa de dados, o que se chama *Big Data Analytics*. Hoffmann-Riem cita três análises que podem ser feitas, com finalidades distintas: a) descritiva; b) preditiva; e c) prescritiva. A descritiva encarrega-se da seleção e preparação dos dados para análise, envolvendo ações como a "priorização, classificação e filtragem".[60] Já a análise preditiva busca indicadores de certa probabilidade de ocorrência de determinados eventos, tendo como objetivo "fornecer ideias para o comportamento humano e, por exemplo, identificar tendências de desenvolvimento e padrões de comportamento a fim de prever comportamentos futuros e, com base nisso, ser capaz de tomar decisões na forma de Tomada de Decisão Automatizada (ADM)".[61] Por fim, nas palavras do autor:

> A análise prescritiva visa a recomendações de ação, a fim de utilizar conhecimentos descritivos e preditivos para atingir objetivos específicos, tais como seleção personalizada em preços ou estratégias e táticas para influenciar atitudes e comportamentos, incluindo a influência na formação da opinião pública, bem como na percepção e apoio/prevenção de desenvolvimentos sociais.[62]

No ramo jurídico, todas essas espécies de análise já possuem aplicação. No âmbito dos tribunais, Boering identifica três tipos de uso do aprendizado de máquina: a) classificador; b) relator; c) robô-juiz.[63] O classificador tem como função a busca de materiais que possam fundamentar decisões (análise descritiva). O relator, para além da mera pesquisa de documentos, deve ser capaz de analisar o material encontrado, aprofundando-se em sua estrutura e até mesmo realizando previsões de decisões tomadas por certos tribunais (análise preditiva). O terceiro tipo também poderia realizar previsões, mas, por seu alto grau de precisão ou pela baixa complexidade do

---

59 BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 41.

60 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021. p. 17.

61 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021. p. 18.

62 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021. p. 18.

63 BOEING, Daniel Henrique Arruda; ROSA, Alexandre Morais da. **Ensinando um robô a julgar**: pragmática, discricionariedade e vieses no uso de aprendizado de máquina no Judiciário. Florianópolis: Emais, 2020.

caso, elas seriam tomadas como decisões por si mesmas – dispensando a atuação do juiz (análise prescritiva).[64]

Esse terceiro nível, ou tipo, citado pela doutrina (ainda) não existe na prática – uma completa substituição do magistrado na tarefa decisória – eis que ainda é necessária, no mínimo, uma revisão da decisão produzida pelo algoritmo. O que se tem atualmente são ferramentas que possibilitam a triagem, classificação e organização de documentos e peças processuais, que realizam pesquisa de legislação, jurisprudência (inclusive com finalidade preditiva) e literatura jurídica, bem como começam a ser introduzidos algoritmos capazes de sugerir esboços de decisões judiciais.[65]

São diversos os exemplos de algoritmos atuantes nos tribunais brasileiros. O que mais tem atraído atenção, desde seu lançamento, em 2018, é o VICTOR, projeto encomendado pelo Supremo Tribunal Federal (STF) à Universidade de Brasília. Sob a promessa de agilizar a tramitação de processos, o programa é tido como o "[...] maior e mais complexo Projeto de [inteligência artificial] do Poder Judiciário e, talvez, de toda a Administração Pública Brasileira".[66] Sua promessa é realizar a leitura dos recursos extraordinários recebidos pelo Tribunal, identificando quais se vinculam a temas de repercussão geral, tendo apresentado 93% de assertividade em testes.[67] A ideia é que ele não fique adstrito a esse objetivo inicial e, por isso, a ampliação de suas habilidades já era discutida desde antes de seu lançamento – condicionada, de certa maneira, às limitações da própria tecnologia.[68]

---

64 LAZZARETTI, Bianca Kaini; HOHENDORFF, Raquel Von. O uso de inteligência artificial na tomada de decisões judiciais: uma análise sob a perspectiva da Crítica Hermenêutica do Direito. **RDUno**: Revista do Programa de Pós-Graduação em Direito da Unochapecó, Chapecó, v. 3, n. 4, p. 15–32, 2021.

65 ARCENO, Taynara Silva. **Inteligência artificial no Tribunal de Justiça do Rio Grande do Sul**: desafios e possibilidades no atual estado da arte. 155 f. Dissertação (Mestrado em Direito) - Universidade do Vale do Rio dos Sinos, São Leopoldo, 2021. Disponível em: http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/9861/Taynara%20Silva%20Arceno_.pdf?sequence=1&isAllowed=y. Acesso em: 12 ago. 2022.

66 INTELIGÊNCIA artificial vai agilizar a tramitação de processos no STF. *In*: SUPREMO TRIBUNAL FEDERAL (STF). **Notícias STF**. Brasília, DF, 30 maio 2018. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=380038. Acesso em: 9 jan. 2022.

67 SOUSA, Weslei Gomes De. **Inteligência artificial e celeridade processual no Judiciário**: mito, realidade ou necessidade? Dissertação (Mestrado em Administração) – Universidade de Brasília, Brasília, DF, 2020. Disponível em: https://repositorio.unb.br/bitstream/10482/38772/1/2020_WesleiGomesdeSousa.pdf. Acesso em: 4 fev. 2022.

68 INTELIGÊNCIA artificial vai agilizar a tramitação de processos no STF. *In*: SUPREMO TRIBUNAL FEDERAL (STF). **Notícias STF**. Brasília, DF, 30 maio 2018. Disponível em:

Mas há outros sistemas que já são usados nos tribunais brasileiros.[69] O sistema SAJ Tribunais, utilizado pelos Tribunais de Justiça dos Estados do Acre, Alagoas, Amazonas, Ceará, Mato Grosso do Sul, Santa Catarina e São Paulo, conta com seis categorias de documentos: despacho, decisão interlocutória, sentença, termo de audiência, ato ordinatório e ajuizamento. Todos esses atos podem:

> [...] ser emitidos de forma totalmente automática ou podem ser configurados para serem apenas preparados para conferência e continuação em cartório em momento posterior. Assim, as determinações do magistrado poderão – ou não – gerar automaticamente os expedientes subordinados a elas sem que seja necessária a atuação do cartório.[70]

Fora dos tribunais, também é possível verificar outros usos da inteligência artificial. De acordo com Almeida e Menezes, identificam-se dez usos da IA em serviços públicos, com expressivo quantitativo em termos de utilização.[71] Eles são descritos no seguinte quadro:

Quadro 3 – Tipologias de inteligência artificial utilizadas no setor público

Tipologia de IA	**Descrição**	**Exemplos (Europa)**
Análise de segurança e inteligência de ameaças	Sistemas que têm a tarefa de analisar e monitorar informações de segurança e prevenir ou detectar atividades maliciosas	A autoridade de segurança nacional da Noruega usa um sistema baseado em *machine learning* que permite a análise automática de qualquer *malware* detectado para aumentar a cybersegurança

http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=380038. Acesso em: 9 jan. 2022.

69 Várias iniciativas do uso de inteligência artificial nos tribunais brasileiros, para além do exemplo aqui citado, foram detalhadas por Engelmann e Fröhlich, assim como por Arceno. Para mais detalhes: ENGELMANN, Wilson; FRÖHLICH, Afonso Vinício Kirschner. Inteligência artificial aplicada à decisão judicial: o papel dos algoritmos no processo de tomada de decisão. **Revista Jurídica**, Blumenau, v. 24, n. 54, e8274, mai./ago. 2020. Disponível em: https://proxy.furb.br/ojs/index.php/juridica/issue/view/474. Acesso em: 9 jan. 2022. ARCENO, Taynara Silva. **Inteligência artificial no Tribunal de Justiça do Rio Grande do Sul**: desafios e possibilidades no atual estado da arte. 155 f. Dissertação (Mestrado em Direito) - Universidade do Vale do Rio dos Sinos, São Leopoldo, 2021. Disponível em: http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/9861/Taynara%20Silva%20Arceno_.pdf?sequence=1&isAllowed=y. Acesso em: 12 ago. 2022.

70 NASCIMENTO, Heloisa Kreutz do. **O que são Atos no SAJ Tribunais?** *In*: QUÍRON. [*S. l.*], 22 jan. 2021. Disponível em: https://quiron.softplan.com.br/hc/pt-br/articles/360016031993-O-que-s%C3%A3o-Atos-no-SAJ-Tribunais-. Acesso em: 3 fev. 2022.

71 ALMEIDA, Guilherme Alberto Almeida de; MENEZES, José Henrique Videira. Inteligência artificial e inovação no setor público. *In*: VAINZOF, Rony; GUTIERREZ, Andriei (org.). **Inteligência artificial**: sociedade, economia e Estado. São Paulo: Thomson Reuters Brasil, 2021. p. 569–602.

Análise preditiva, simulação e visualização de dados	Soluções que aprendem cm grandes conjuntos de dados para identificar padrões que são usados para visualizar, simular ou prever novas configurações	Desde 2012, a polícia da cidade de Zurique utiliza um *software* que prevê assaltos. Com base nessas previsões, a polícia pôde ser encaminhada para conferir esses locais e limitar o acontecimento de crimes
Aprendizado de máquina (*machine learning*), Aprendizado profundo (*deep learning*)	Embora quase todas as outras categorias usem aprendizado de máquina, essa categoria residual abarca soluções de IA que não cabem em outras classificações	Na República Tcheca, IA é usada em serviços sociais para facilitar que os cidadãos permaneçam em seu ambiente natural pelo maior tempo possível
Chatbots, agentes virtuais, assistentes digitais inteligentes, e sistemas de recomendação	Esta tipologia inclui assistentes virtualizados ou '*bots'* usados para fornecer conselhos genéricos aos usuários e para recomendações relacionadas a comportamentos	Na Letônia, o Chatbot UNA é usado para ajudar a responder questões frequentemente realizadas acerca do processo de registro de uma empresa
Gestão do conhecimento com base na IA	Sistemas capazes de criar uma coleção pesquisável de descrições de casos, textos e outros *insights* a serem compartilhadas com especialistas para análise posterior	Na Eslováquia, um sistema de IA é usado pelo governo para ajudar na navegação e busca de dados semânticos relevantes
Processamento de áudio	Aplicativos capazes de detectar e reconhecer, som, música e outras formas de áudio, incluindo fala, permitindo o reconhecimento de voz e a transcrição de palavras faladas	Corti, na Dinamarca, é usado para processar o áudio de chamadas de emergência para detectar se quem liga poderia ter uma parada cardíaca
Processamento de linguagem natural, mineração de texto e análise de fala	Aplicativos capazes de reconhecer e analisar voz, texto escrito e comunicar-se de volta	Em Dublin, uma IA analisa as opiniões dos cidadãos da região para um panorama de suas maiores preocupações, por meio da análise dos tweets (Twitter) locais com vários algoritmos
Robótica cognitiva, automação de processos e veículos conectados e automatizados	Tecnologias de automação de processos, que pode ser realizado por meio de *hardware* ou *software* robotizado	Uso de veículos autônomos em um aeroporto da Noruega para melhorar a limpeza de neve nas pistas de decolagem

Sistemas especialistas, sistemas baseados em regras, tomada de decisão algorítmica	Implementações aparentemente distantes, porém, reunidas por sua orientação predominante para facilitar ou automatizar totalmente os processos de tomada de decisão de relevância potencial para os setores público e privado	Sistema de seleção de berçários na Varsóvia. O algoritmo considera os dados fornecidos pelos pais durante o registro, calcula a pontuação e atribui automaticamente as crianças em berçários individuais.
Visão computacional e reconhecimento de identidade	Aplicativos que usam imagem, vídeo ou reconhecimento facial para obter informações sobre o ambiente externo e/ou a identidade de pessoas ou objetos específicos	Na Estônia, o sistema SATIKAS é usado para detectar pastagens cortadas ou não por meio de imagens de satélite

Fonte: adaptado de Almeida e Menezes,[72] exemplos com base em Misuraca e Van Noordt.[73]

Portanto, o uso de *Big Data Analytics* permite o tratamento facilitado de bases de dados antes muito confusas, o que cria diversas possibilidades e vários riscos, tanto no âmbito público como privado.[74] Nesse sentido, esses tipos de análise têm potencial de implementação para as mais diversas finalidades, como é o caso do policiamento preditivo, que busca identificar probabilidades relacionadas ao cometimento de crimes.[75]

Neste item, foram apresentados os conceitos fundamentais para a compreensão do uso dos dados pessoais na era da Quarta Revolução Industrial, com a exploração de conceitos básicos e um panorama dos usos da inteligência artificial no cenário jurídico. No item 2.2, serão abordados, mais especificamente, a coleta e análise de dados pessoais no âmbito criminal.

---

72 ALMEIDA, Guilherme Alberto Almeida de; MENEZES, José Henrique Videira. Inteligência artificial e inovação no setor público. *In*: VAINZOF, Rony; GUTIERREZ, Andriei (org.). **Inteligência artificial: sociedade, economia e Estado**. São Paulo: Thomson Reuters Brasil, 2021. p. 581–582.

73 MISURACA, Gianluca; NOORDT, Colin van. **AI watch**: artificial Intelligence in public services: overview of the use and impact of AI in public services in the EU: Science for Policy Report. Luxembourg: European Commission, 2020. Disponível em: https://bit.ly/3TsZ6vV. Acesso em: 14 ago. 2022.

74 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021.

75 HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. 1 ed. Rio de Janeiro: Forense, 2021.

2.2 Um panorama não exaustivo das possibilidades de uso de dados pessoais na segurança pública

O uso de dados pessoais no âmbito penal costuma ser diferenciado por suas finalidades, de garantia da segurança pública e de investigação ou persecução criminal. Variam as possibilidades de análise de dados, os atores envolvidos, os objetivos, bem como os direitos protegidos e limitados por essas práticas. Nesse sentido, importante abordar as distinções conceituais do tratamento de dados na esfera penal, assim como algumas práticas sociais que podem auxiliar na compreensão das vantagens e dos desafios que acompanham a inovação nessa área.

Quando se menciona a garantia da segurança pública (em sentido estrito), a questão é de prevenção. Nesse caso, são utilizados recursos de vigilância, anteriores ao acontecimento de qualquer fato delitivo. Por outro lado, o uso de dados pessoais para fins de investigação ou persecução penal está relacionado a um objeto bem delimitado.[76] Direciona-se, assim, à repressão de fatos já consumados, com a apuração de provas e de autoria.

Juntas, as noções de prevenção e repressão penal compõem o que se chama de segurança pública em sentido amplo. Também fazem parte deste conceito amplo de segurança as atividades de defesa nacional e de segurança do Estado. Essa divisão é feita com base no artigo 4º, III, da LGPD – que excluiu as atividades de segurança pública, defesa nacional, segurança do Estado, bem como de investigação e repressão de infrações penais de seu escopo.[77]

As atividades de defesa nacional, de acordo com Abreu, “[...] são aquelas de cunho militar em situações de conflito armado principalmente contra ameaças externas”.[78] A segurança do Estado, por sua vez, tem a atuação voltada para ações de inteligência e contrainteligência, que compõem a “atividade de inteligência”, assim conceituada pela Política Nacional de Inteligência: “exercício permanente de ações

---

[76] MARGETH, Ana Lara; CARNEIRO, Giovana. Caminhos para a proteção de dados pessoais na segurança pública e investigação criminal: lições do Seminário Internacional da Comissão de Juristas. *In*: ITS Rio, [*s. l.*], 11 ago. 2020. Disponível em: https://bit.ly/3dX6n6P. Acesso em: 4 ago. 2022.

[77] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jun. 2022.

[78] ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book*. p. 597.

especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado".[79] Pode-se dizer que estas também são atividades de prevenção, na medida em que visam manter a ordem pública e a paz, mas com foco na proteção da coletividade em uma perspectiva difusa, não tão voltada à defesa de bens jurídicos individuais.

Há quem diga, por outro lado, que as atividades de inteligência – por sua natureza informativa, de assessoria ao presidente da República – não se confundem com ações de segurança.[80] Entretanto, como se verá nas próximas páginas, a Agência Brasileira de Inteligência – ABIN, que é o principal órgão de inteligência no Brasil, já esteve envolvida em algumas polêmicas envolvendo o tratamento de dados com justificativa de garantia da segurança. Além disso, a legislação nacional prevê a atuação da agência (e outros órgãos de inteligência do país) em tarefas como o enfrentamento do crime organizado, gerenciamento de armas e munições, dentre outras.[81] Por isso a análise, aqui, inclui estas operações dentre as realizadas com finalidade de prevenção criminal.

Observa-se, ainda, que há mais um ponto de atenção quanto ao uso de dados pessoais no âmbito criminal, que não consta no rol da LGPD: pós-condenação, em que já se tem uma pena em execução ou cumprida. Estes dados ficam disponíveis em sistemas de tribunais e de outros órgãos, como Ministério Público e Defensoria Pública, além de compor atestados de antecedentes e sistemas de consultas integradas.

Outra forma de classificar o processamento de dados pessoais para finalidade de garantia da segurança pública (*lato sensu*) é com relação a sua origem, em correlação com as finalidades de seu tratamento. Essa diferenciação é ilustrada e sintetizada na figura 3:

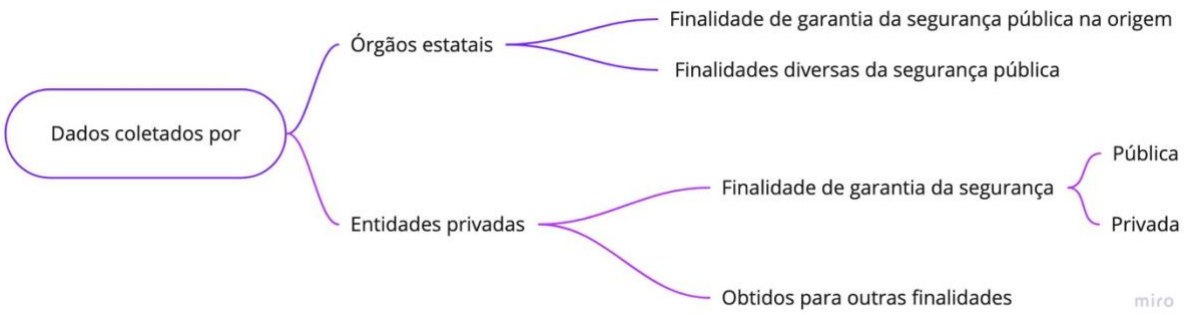
---

79 BRASIL. **Decreto nº 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Decreto/D8793.htm. Acesso em: 18 ago. 2022.

80 DIAS, Tatiana; MARTINS, Rafael Moro Martins. Documentos vazados mostram que Abin pediu ao Serpro dados e fotos de todas as CNHs do país. *In*: THE INTERCEPT, [*s. l.*], 6 jun. 2020. Disponível em: https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/. Acesso em: 28 fev. 2022.

81 AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). **Atividade de inteligência no Brasil**. Brasília, DF: ABIN, 2020. v. 5: Cadernos de legislação da ABIN. *E-book*.

Figura 3 – Classificação dos dados pela origem e finalidade



Fonte: elaborado pela autora com base em Abreu.[82]

Nesse sentido, os dados utilizados sob justificativa de prevenção e repressão penal podem ser coletados pelo Estado ou pelo setor privado. A finalidade da coleta pode ser, desde o início, a garantia da segurança pública. Entretanto, há um universo de dados obtidos para outros fins – que também são utilizados para atividades de segurança. O quadro abaixo exemplifica os dados, sua origem e finalidade inicial:

Quadro 4 – Exemplos de dados pessoais usados para garantia da segurança púbica (*lato sensu*)

Origem	Finalidade original	Exemplos
Órgãos estatais	Garantia da segurança	Identificação criminal, dados biométricos, DNA, imagens de câmeras de monitoramento, dados coletados por tornozeleiras eletrônicas
	Outras finalidades	Documentação civil, registros de condutores, usuários de transportes públicos, registro educacional, cadastros em órgãos de prestação de serviços básicos (água, energia elétrica)
Entidades privadas	Garantia da segurança	Câmeras de vigilância privada, controle biométrico e identificação facial (sistemas privados)
	Outras finalidades	Empresas de telefonia, bancos, serviços de transporte individual, de entrega, redes sociais

Fonte: elaborado pela autora com base em Abreu.[83]

[82] ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book*.

[83] ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book*.

Todas estas categorias auxiliam na compreensão da problemática que é o tratamento de dados pessoais no âmbito criminal. Trata-se de uma enorme quantidade e variedade de dados, oriundos de diversas fontes de coleta. Dentro da noção ampla de segurança pública, podem ser utilizados para prevenção ou repressão penal. Tudo isso é feito sem que haja uma regulação própria. Portanto, a prática tem gerado preocupação e alguns casos já tiveram destaque na última década.

A ação pontual de titulares do dever de garantia da segurança pública[84] com uso de novas tecnologias computacionais já se mostrou repleta de desafios. É o que ocorre com o espelhamento de tela do *WhatsApp* sem a autorização do suspeito como forma de vigiar suas atividades de comunicação. O que ocorre é que a polícia, ao abordar um suspeito, apreende o celular do investigado e espelha *WhatsApp* na versão *Web*. Com isso, habilita um computador a realizar diversas operações de comunicação do aplicativo, em tempo real. Basta uma autenticação para que o investigador possa visualizar, apagar ou enviar mensagens como se fosse o proprietário do perfil, não havendo qualquer registro do responsável pela ação.

Embora essa atividade venha sendo reprimida pelo Superior Tribunal de Justiça,[85] ainda se veem casos nos Tribunais de Justiça do país, indicando que se realiza o espelhamento e monitoramento das comunicações realizadas pelo aplicativo, inclusive com autorização judicial. Os argumentos utilizados para permitir o espelhamento envolvem: a equiparação com a quebra de sigilo telemático; possibilidade de realização no bojo da ação controlada, visando o enfrentamento do crime organizado; e, inclusive, a necessidade de comprovação, pela defesa, de que houve adulteração de prova (o que é tecnicamente impossível, diante da inexistência de recurso de rastreio do usuário que realizou a comunicação).[86]

---

84 De acordo com a Constituição Federal, nos incisos do artigo 144: polícia federal, polícia rodoviária federal, polícia ferroviária federal, polícias civis, polícias militares e corpos de bombeiros militares, polícias penais federal, estaduais e distrital. BRASIL. **Constituição Federal**. [Constituição (1988)]. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 ago. 2022.

85 BRASIL. Superior Tribunal de Justiça (6. Turma). **Recurso em Habeas Corpus nº 99.735 Santa Catarina**. Recurso ordinário em habeas corpus. Penal e processo penal. Tráfico de drogas e associação ao tráfico. Autorização judicial de espelhamento, via whatsapp web, das conversas realizadas pelo investigado com terceiros. [...]. Recorrentes: A C DA C, D C DA C. Recorrido: Ministério Público do Estado de Santa Catarina. Relatora: Ministra Laurita Vaz, 27 de novembro de 2018. Disponível em: https://cutt.ly/YcmT6m3. Acesso em: 3 abr. 2022.

86 LAZZARETTI, Bianca Kaini; FORTIN, Eleonora Jotz Pacheco. O espelhamento via *WhatsApp Web* e direitos fundamentais em risco: como a licitude da prova é justificada nos tribunais. *In*: ENCONTRO VIRTUAL DO CONPEDI, 3., 2021, Florianópolis. **Direito penal, processo penal e constituição II**. Florianópolis: CONPEDI, 2021. Disponível em:

Também com relação a dados que são coletados ou mediados por empresas privadas é problemático o acesso dos órgãos públicos à geolocalização, registros de acesso à Internet (como endereços IP, sites visitados) e informações pessoais inseridas por usuários de serviços online. No caso da investigação do assassinato de Marielle Franco e de Anderson Gomes, a determinação do juízo criminal de primeira instância acolheu pedido do Ministério Público do Rio de Janeiro, que requereu:

> [...] os dados de geolocalização de todos os usuários que estavam nos arredores de onde foi visto o carro usado pelos atiradores em um intervalo de quinze minutos, bem como buscas no Google de qualquer usuário que tenha procurado por determinados termos específicos (‘Marielle Franco’, ‘vereadora Marielle’, ‘agenda Marielle’, ‘agenda vereadora Marielle’, ‘Casa das Pretas’, ‘Rua dos Inválidos 122’ e ‘Rua dos Inválidos’) até cinco dias antes do crime.[87]

A empresa recorreu da decisão, afirmando que, no Brasil, são vedadas as interceptações e quebras de sigilo genéricas, tornando a medida desproporcional. Nesse sentido, defende que o fornecimento desses dados para a investigação viola a privacidade de uma grande quantidade de pessoas não relacionadas ao crime. O recurso, porém, foi desprovido pelo Superior Tribunal de Justiça – sob justificativa de que, para a quebra de sigilo de dados, a autoridade judiciária não tem a obrigação de indicar os investigados, até mesmo por se tratar de uma análise voltada para identificação de usuários suspeitos.[88]

Nos Estados Unidos, em maio de 2022, foi revogada a decisão *Roe vs. Wade* – que assegurava o direito ao aborto no país desde 1973. Com isso, a tendência é que a maior parte dos estados norte-americanos criminalizem a prática:

---

http://site.conpedi.org.br/publicacoes/276gsltp/3b53n985/9dZHOuAi3hOVaDy7.pdf. Acesso em: 22 jun. 2022.

87 ABRUSIO, Juliana *et al.* Dados de geolocalização e a investigação do caso Marielle. **Consultor Jurídico**, São Paulo, 7 jul. 2020. Disponível em: https://www.conjur.com.br/2020-jul-07/direito-digital-dados-geolocalizacao-investigacao-marielle. Acesso em: 31 jul. 2022.

88 JOSINO, Clarissa Nogueira. **Dados pessoais, segurança pública e investigação criminal**: um panorama da proteção de dados e seus desafios regulatórios no Brasil. 2021. 53 f. Monografia (Graduação em Direito) - Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2021. Disponível em: https://repositorio.ufc.br/handle/riufc/58510. Acesso em: 30 ago. 2022.

Figura 4 – Mapa da criminalização do aborto nos Estados Unidos

Fonte: Poder 360.[89]

Com a transformação do direito constitucional ao aborto em crime, os dados sensíveis compartilhados legitimamente e em uma relação de confiança pelas pessoas, clínicas que faziam o procedimento e financiadores tornam-se uma ameaça aos envolvidos.[90] As discussões a este respeito ainda são embrionárias, tendo em vista que se trata de acontecimento muito recente. Porém, já é possível identificar sérios riscos em termos de privacidade e com relação à proporcionalidade do uso dos dados para garantia da efetividade penal.

Tem-se antecipado que, em alguns lugares, dados de busca online por informações sobre onde realizar o aborto, geolocalização, mensagens[91] e até mesmo

---

89 22 ESTADOS dos EUA devem banir aborto com revisão de Roe vs Wade. *In*: PODER 360. [*S. l.*], 25 jun. 2022. Disponível em: https://www.poder360.com.br/internacional/22-estados-dos-eua-devem-banir-aborto-com-revisao-de-roe-vs-wade/. Acesso em: 21 ago. 2022.

90 SOUZA, Sartorelli Venâncio de. Criminalização e proteção de dados: análise do caso Roe vs Wade. **Consultor Jurídico**, São Paulo, 26 jul. 2022. Disponível em: https://www.conjur.com.br/2022-jul-26/flora-sartorelli-criminalizacao-protecao-dados. Acesso em: 21 ago. 2022..

91 KORN, Jennifer; DUFFY, Clare. Como dados pessoais podem ser usados para fazer cumprir leis antiaborto nos EUA. *In:* CNN Brasil, Nova Iorque, 25 jun. 2022. Disponível em: https://www.cnnbrasil.com.br/tecnologia/como-dados-pessoais-podem-ser-usados-para-fazer-cumprir-leis-antiaborto-nos-eua/. Acesso em: 21 ago. 2022.

registros em aplicativos de controle de ciclo menstrual possam ser usados para indiciar pessoas.[92] Aponta-se que estes dados sensíveis, relacionados à saúde reprodutiva, possam ser utilizados de duas maneiras. Primeiro, para investigação e persecução penal, em um caso específico. Segundo, como vigilância massiva para descoberta de condutas suspeitas.[93]

Como afirma Angwin, "Vivemos em uma Nação de Arrasto – um mundo de rastreamento indiscriminado em que instituições estão estocando dados sobre indivíduos em um ritmo sem precedentes".[94] Por meio de aplicação de análises preditivas sobre essa grande quantidade de dados, tem-se a prática de *dataveillance*. Observa-se que, com isso, desloca-se "[...] o problema da coleta de dados do mundo físico para o virtual. Isso permite que as novas tecnologias violem os direitos humanos de modos completamente imprevisíveis para aqueles que não compreendem, adequadamente, essa categoria [...]".[95]

Quando a questão é o tratamento de uma grande quantidade de dados, o problema parece se agravar e tornar-se mais polêmico. O caso *Snowden* é símbolo dos debates sobre a proteção dos dados e da privacidade de usuários de Internet perante o Estado. Em 2013, Edward Snowden, um assistente técnico terceirizado da CIA, agência de inteligência dos Estados Unidos da América, revelou um grande programa de espionagem por meio do qual a NSA (Agência Nacional de Segurança

---

92 Destaca-se que estes "*apps*" servem para que as pessoas registrem a duração e a ocorrência da menstruação, bem como informações sobre a gravidez. Ao iniciar o acompanhamento da gestação no celular, e depois interromper, pode servir como gatilho para uma investigação sobre aborto. Na política de privacidade do aplicativo Flo, por exemplo, consta que: "Também podemos partilhar alguns dos seus Dados Pessoais nas seguintes circunstâncias especiais: em resposta a intimações, ordens judiciais ou processos legais, na medida permitida e conforme as restrições da lei (inclusive para atender aos requisitos de segurança nacional ou de aplicação da lei); [...]". FLO. **Política de privacidade**. [*S. l.*]: Flo, 6 out. 2020. Disponível em: https://flo.health/pt/politica-de-privacidade. Acesso em: 21 ago. 2022.

93 SOUZA, Sartorelli Venâncio de. Criminalização e proteção de dados: análise do caso Roe vs Wade. **Consultor Jurídico**, São Paulo, 26 jul. 2022. Disponível em: https://www.conjur.com.br/2022-jul-26/flora-sartorelli-criminalizacao-protecao-dados. Acesso em: 21 ago. 2022.

94 Tradução nossa de: "We are living in a Dragnet Nation—a world of indiscriminate tracking where institutions are stockpiling data about individuals at an unprecedented pace". ANGWIN, Julia. **Dragnet nation**: a quest for privacy, security, and freedom in a world of relentless surveillance. New York: Times Books, Henry Holt and Company, 2014. *E-book* (não paginado).

95 MENEZES NETO, Elias Jacob de; MORAIS, Jose Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. **Revista Brasileira de Políticas Públicas**, Brasília, DF, v. 7, n. 3, p. 196, 2017. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/4840. Acesso em: 30 ago. 2022.

norte-americana) “monitorava milhões de telefones e dados de usuários online, nos Estados Unidos e em países estrangeiros”.[96]

Glenn Greenwald, advogado e jornalista que auxiliou Snowden a expor o esquema de vigilância, publicou um livro falando sobre o caso. Em “Sem lugar para se esconder”, ele relata que:

> O acervo de documentos reunido por Edward Snowden era espantoso tanto pelo tamanho quanto pela abrangência. [...] Os milhares de programas de vigilância descritos por aquele acervo não tinham sido previstos para ir a público por quem os implementara. Muitos tinham por alvo a população dos Estados Unidos, mas dezenas de países mundo afora – inclusive democracias em geral vistas como aliadas dos Estados Unidos, como França, Brasil, Índia e Alemanha – também eram alvo de uma vigilância em massa indiscriminada.[97]

Estima-se que, só no Brasil, foram cerca de 2,3 bilhões de telefonemas e e-mails monitorados pela agência estrangeira, incluindo comunicações de autoridades. O governo norte-americano reconheceu o programa, mas justificou a ação com o combate ao terrorismo, afirmando que o conteúdo das comunicações não teria sido analisado, mas sim as informações ao seu respeito, como data e hora (*metadados*).[98]

No Brasil, a vigilância tecnológica também ganhou destaque. Em 2013, quando o país enfrentava uma onda de manifestações, o Governo Federal mobilizou a Agência Brasileira de Inteligência (ABIN) no monitoramento de redes sociais.[99] Depois, em 2017, noticiou-se a análise massiva de postagens realizadas na Internet, a serviço da presidência da República, mas mediado por uma empresa privada – a agência publicitária Isobar Brasil.[100]

Mais recentemente, a ABIN foi protagonista em outra polêmica relacionada ao amplo acesso a dados da população. Em 2020, a agência negociava com a Serpro o

---

96 PILATI, José Isaac; OLIVO, Mikhail Vieira Chancelier de. Um novo olhar sobre o Direito à privacidade: Caso Snowden e Pós-modernidade jurídica. **Seqüência**, Florianópolis, v. 35, n. 69, p. 285, 2014. Disponível em: http://www.scielo.br/pdf/seq/n69/12.pdf. Acesso em: 12 jul. 2021.

97 GREENWALD, Glenn. **Sem lugar para se esconder**. 1. ed. Rio de Janeiro: Sextante, 2014. *E-book*. p. 176.

98 PILATI, José Isaac; OLIVO, Mikhail Vieira Chancelier de. Um novo olhar sobre o Direito à privacidade: Caso Snowden e Pós-modernidade jurídica. **Seqüência**, Florianópolis, v. 35, n. 69, p. 285, 2014. Disponível em: http://www.scielo.br/pdf/seq/n69/12.pdf. Acesso em: 12 jul. 2021.

99 ABIN monta rede para monitorar internet. *In:* ÉPOCA Negócios, São Paulo, 14 jul. 2013. Disponível em: https://epocanegocios.globo.com/Informacao/Acao/noticia/2013/06/abin-monta-rede-para-monitorar-internet.html. Acesso em: 18 ago. 2022.

100 PORTINARI, Natália. Planalto usa dados de agência para monitorar política em redes sociais. *In*: FOLHA de São Paulo, São Paulo, 11 abr. 2017. Disponível em: http://www1.folha.uol.com.br/poder/2017/04/1874399-planalto-usa-dados-de-agencia-de-sp-para-monitorar-redes-sociais.shtml. Acesso em: 18 ago. 2022.

compartilhamento de mais de 76 milhões de carteiras de motorista do país. A Serpro é a empresa pública de processamento de dados que detém um gigantesco banco com dados de condutores, como nome, filiação, endereço, telefone, veículos e fotos. Esse banco de dados, juntamente com o de CPFs, é um dos únicos em nível nacional – tendo em vista que as carteiras de identidade, por exemplo, são registradas e geridas no estado em que foram emitidas. A cooperação entre ABIN e Serpro estaria ancorada no Decreto nº 10.046, de 2019, que autoriza o compartilhamento de dados na administração federal.[101]

Posteriormente, foi ajuizada a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695, contestando a medida de intercâmbio de dados entre ABIN e Serpro. O argumento era de que, na verdade, a prática não se enquadra nas hipóteses de compartilhamento do Decreto nº 10.046, assim como a vigilância tida como massiva e indiscriminada de cidadãos não é atividade de inteligência, portanto, não é responsabilidade da ABIN.[102] Alguns dias depois, a Advocacia-Geral da União informou ao Supremo Tribunal Federal que o acordo de compartilhamento de dados foi revogado.[103]

Destaca-se, nestes casos, o problema da falta de transparência a respeito da finalidade da vigilância, bem como dos resultados práticos das ações, com explicitação dos dados utilizados e das consequências jurídicas de seu uso. Ou seja, não se sabe se o processamento desses dados resultou em algum benefício efetivo em termos de garantia da segurança, ou mesmo em potencial, seja em termos de repressão ou de prevenção. Não foram apresentadas justificativas, nem houve preocupação com o consentimento do titular dos dados, assim como também não houve demonstração de zelo com outros direitos e garantias fundamentais possivelmente envolvidos.

---

101 DIAS, Tatiana; MARTINS, Rafael Moro Martins. Documentos vazados mostram que Abin pediu ao Serpro dados e fotos de todas as CNHs do país. *In*: THE INTERCEPT, [*s. l.*], 6 jun. 2020. Disponível em: https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/. Acesso em: 28 fev. 2022.

102 STF vai julgar acordo de compartilhamento de dados entre Serpro e ABIN. *In*: CONVERGÊNCIA Digital, [*s. l.*], 19 jun. 2020. Disponível em: https://www.convergenciadigital.com.br/Seguranca/STF-vai-julgar-acordo-de-compartilhamento-de-dados-entre-Serpro-e-ABIN-53978.html?UserActiveTemplate=site. Acesso em: 28 fev. 2022.

103 GROSSMANN, Luís Osvaldo. **Governo revoga compartilhamento de dados entre Serpro e Abin**. *In*: CONVERGÊNCIA Digital, [*s. l.*], 25 jun. 2020. Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=54011&sid=18. Acesso em: 28 fev. 2022.

Outro caso de compartilhamento de dados entre órgãos governamentais ocorreu durante a pandemia de Covid-19. A Medida Provisória (MP) nº 954, de 2020, previa que o Instituto Brasileiro de Geografia e Estatística (IBGE) tivesse acesso a dados de usuários de telecomunicações. A finalidade seria a de produção de estatística oficial, com vedação expressa de compartilhamento dos dados com outros órgãos públicos ou entidades privadas, bem como de utilização para outros fins.[104]

Porém, foram propostas ações diretas de inconstitucionalidade, tendo em vista que o acesso, pelo IBGE, a estes dados viola a dignidade da pessoa humana, a intimidade, a vida privada, a honra, a imagem e o sigilo dos dados.[105] A MP foi atacada por não precisar qual o objetivo da estatística que seria realizada, ou mesmo sua finalidade, bem como por não ter demonstrado interesse público legítimo que atendesse à critérios de necessidade, adequação e proporcionalidade.[106] Uma liminar suspendeu a MP, que, depois, perdeu a validade pelo decurso do prazo de vigência.[107]

Neste caso, ainda que a proposta inicial não fosse de garantia da segurança pública, assim como também não era permitido o compartilhamento com outros órgãos, a medida tinha contornos amplos. Desse modo, ao não delimitar os fins da estatística que visava produzir, poderia servir de material para o controle estatal – inclusive na área de prevenção e repressão penal.

Recentemente, o júri do caso da Boate Kiss foi anulado porque o Ministério Público (MP) utilizou informações privilegiadas sobre os jurados, obtidas no Sistema

---

104 BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Dispõe 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, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: Presidência da República, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 18 ago. 2022.

105 SUPREMO começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE. *In*: NOTÍCIAS STF, Brasília, DF, 6 maio 2020. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442823. Acesso em: 4 jul. 2022.

106 VALENTE, Fernanda. MP 954 não define como e para que serão usados dados coletados, diz Rosa Weber. **Consultor Jurídico**, São Paulo, 2020. Disponível em: https://www.conjur.com.br/2020-mai-06/mp-954-nao-define-finalidade-dados-coletados-rosa-weber. Acesso em: 18 ago. 2022.

107 MP QUE obrigava operadoras a compartilhar dados com o IBGE perde validade. *In*: CÂMARA dos Deputados, Brasília, DF, 18 ago. 2020. Disponível em: https://www.camara.leg.br/noticias/685115-mp-que-obrigava-operadoras-a-compartilhar-dados-com-o-ibge-perde-validade/. Acesso em: 18 ago. 2022.

de Consultas Integradas (SCI).[108] Esse banco de dados reúne informações de pessoas condenadas e do cumprimento da pena no estado do Rio Grande do Sul, inclusive de amigos ou familiares que realizam visitas em presídios. O acesso do MP ao SCI é possível por conta de um acordo firmado entre a instituição e o Poder Executivo estadual, renovado por meio do Acordo de Cooperação Técnica nº 01/2022 até julho de 2027.[109]

O que o MP fez foi procurar o nome dos prospectivos jurados no SCI, a fim de requerer a dispensa daqueles que tivessem qualquer ligação com uma pessoa condenada por algum delito. Do ponto de vista fático, a ação do MP foi criticada por ser notadamente discriminatória – eliminando 97 pessoas do júri por terem contato com apenados, alguns há mais de 20 anos. Pela perspectiva jurídica, violou o direito fundamental à proteção de dados e a paridade de armas – visto que as defesas particulares não têm acesso ao sistema. Além disso, ficou evidente a violação da privacidade no caso, inclusive sem o consentimento dos envolvidos.[110]

Outra utilização de dados pessoais para fins de garantia da segurança pública é o reconhecimento facial. Trata-se de análise, realizada por meio de algoritmos, de imagens coletadas por câmeras de vigilância (públicas ou privadas), ou mesmo em fotografias e vídeos obtidos na Internet ou por policiais em abordagens. Com isso, busca-se traços biométricos que sejam capazes de identificar uma pessoa, por meio de comparações entre a imagem analisada e bancos de dados (governamentais, de empresas, com o *Big Data* etc.).

No Brasil, desde 2011, foram reportados publicamente pelo menos 48 casos de implementação dessa tecnologia por autoridades públicas (inclusive com parcerias

---

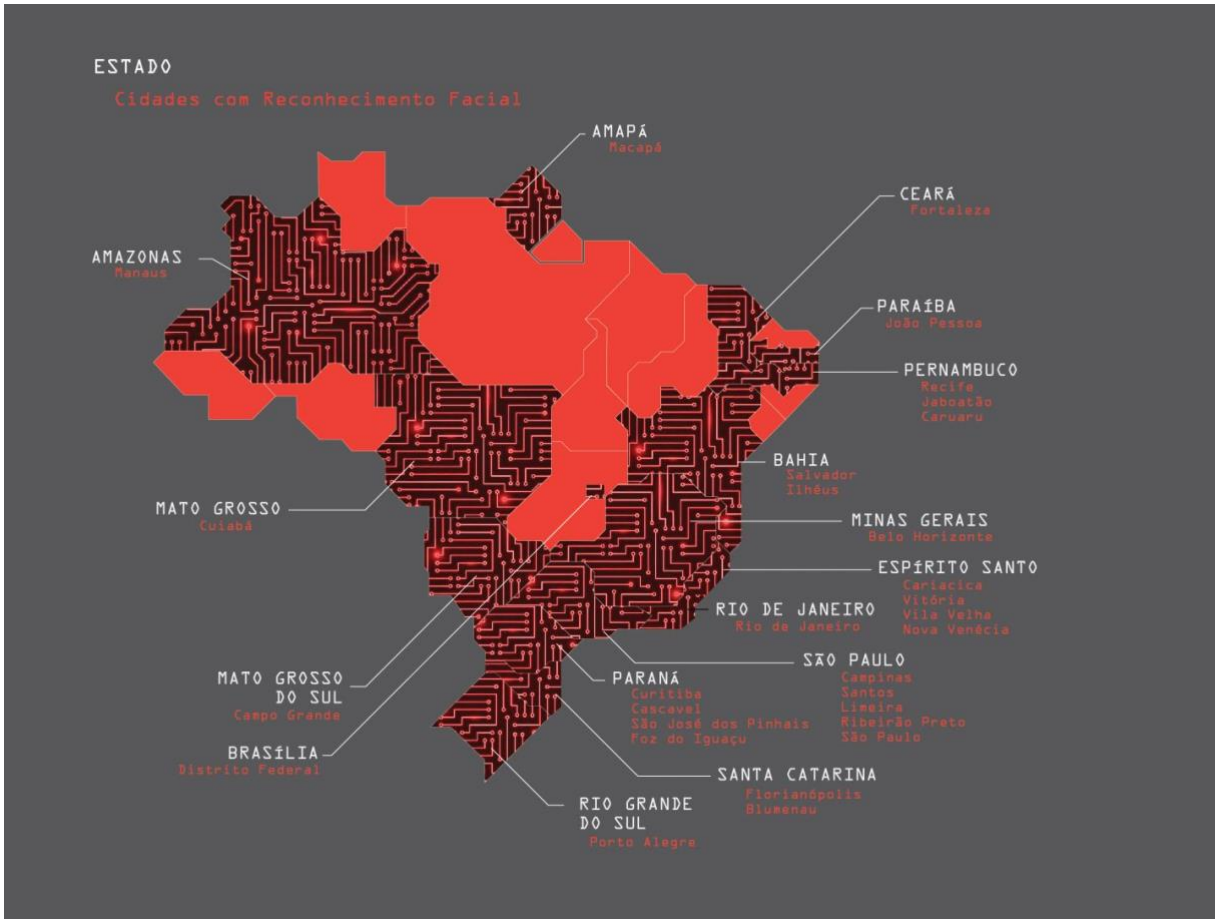
[108] JÚRI DA Boate Kiss é anulado pelo Tribunal de Justiça do RS. *In*: DIÁRIO Catarinense, [*s. l.*], 3 ago. 2022. Disponível em: https://www.nsctotal.com.br/noticias/juri-da-boate-kiss-e-anulado-pelo-tribunal-de-justica-do-rs. Acesso em: 19 ago. 2022.

[109] RIO GRANDE DO SUL, Ministério Público. **Acordo de Cooperação Técnica SR/PF/RS e MP/RS nº 01/2022**. Acordo de cooperação técnica que entre si celebram a união, por intermédio da Polícia Federal, com a interveniência da Superintendência Regional da Polícia Federal no Rio Grande do Sul - SR/PF/RS e o Ministério Público do estado do Rio Grande do Sul, por intermédio da Procuradoria-Geral de Justiça, para os fins que especifica. Porto Alegre: Procuradoria-Geral de Justiça, 2022. Disponível em: https://transparencia.mprs.mp.br/media/convenios/convenio/Acordo_de_Coopera%C3%A7%C3%A3o_T%C3%A9cnica_JRb6QGx.pdf. Acesso em: 19 ago. 2022.

[110] SARLET, Ingo Wolfgang. Mais uma vez o caso da boate Kiss: a proteção de dados pessoais. **Consultor Jurídico**, São Paulo, 2022. Disponível em: https://www.conjur.com.br/2022-ago-12/direitos-fundamentais-vez-boate-kiss-protecao-dados-pessoais. Acesso em: 19 ago. 2022.

no setor privado), sendo 13 destes voltados à segurança pública.[111] O Instituto Igarapé mapeou essas iniciativas:

Figura 5 – Mapa do uso de reconhecimento facial no Brasil



Fonte: Instituto Igarapé.[112]

No Rio de Janeiro, a utilização de câmeras de monitoramento conectadas a sistemas de reconhecimento facial para finalidade de garantia da segurança pública já teve impactos preocupantes. Em 2019, foi anunciada a instalação de 140 equipamentos dessa natureza, depois de teste realizado durante o carnaval que resultou no cumprimento de oito mandados de prisão em 10 dias de operação.[113] A prática é assim descrita:

---

111 INSTITUTO IGARAPÉ. Reconhecimento facial no Brasil. *In*: INSTITUTO Igarapé. [Rio de Janeiro], 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 12 jul. 2022.

112 INSTITUTO IGARAPÉ. Reconhecimento facial no Brasil. *In*: INSTITUTO Igarapé. [Rio de Janeiro], 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 12 jul. 2022.

113 WITZEL anuncia reconhecimento facial no Maracanã e Santos Dumont: serão instaladas 140 câmeras na capital do estado do Rio de Janeiro; projeto piloto, no Carnaval, fez com que fossem cumpridos oito mandados de prisão. *In*: VEJA, São Paulo, 29 mar. 2019. Disponível em:

> Através de um sistema integrado ao banco de dados da Polícia Civil, em questão de segundos as câmeras escaneiam os rostos de transeuntes e os comparam com os de procurados pela Justiça. Quando o software, disponibilizado em convênio estabelecido com a empresa de telefonia Oi, considera as imagens semelhantes, emite um alerta e informa o grau de confiabilidade. [...] Com base instalada no Centro Integrado de Comando e Controle (CICC), 12 agentes por turno têm a missão de acompanhar as imagens. A corporação realizou treinamentos de capacitação nos últimos meses e tem 100 agentes para o trabalho.[114]

Ou seja, há um alto investimento de recursos técnicos (tecnológicos) e humanos nas iniciativas de reconhecimento facial. Enquanto esta tecnologia conquista espaço e é celebrado como sucesso,[115] já se tem notícia de acontecimentos que denotam o que se tem chamado de vieses algorítmicos, que são uma grande preocupação relacionada a essa tecnologia – ao lado dos riscos envolvendo imprecisão e o uso de dados sensíveis.[116]

Em maio de 2019, no Rio de Janeiro, uma mulher foi equivocadamente identificada pelo sistema de reconhecimento facial e detida pelos crimes de homicídio e ocultação de cadáver – sendo que a verdadeira procurada sequer estava foragida,

---

https://veja.abril.com.br/politica/witzel-anuncia-reconhecimento-facial-no-maracana-e-santos-dumont/. Acesso em: 22 mar. 2022.

[114] COPACABANA e Maracanã ganham sistema de câmeras de reconhecimento facial. *In*: SEGURANÇA Eletrônica. [*S. l.,* 2017c]. Disponível em: https://revistasegurancaeletronica.com.br/copacabana-e-maracana-ganham-sistema-de-cameras-de-reconhecimento-facial/. Acesso em: 22 nov. 2021.

[115] "BIG BROTHER Rio": reconhecimento facial usado no carnaval será ampliado. *In*: TILT Uol. [*S. l.*], 30 mar. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/03/30/big-brother-rio-reconhecimento-facial-usado-no-carnaval-sera-ampliado.htm. Acesso em: 19 ago. 2022.

[116] Essas categorias – vieses, imprecisão e riscos do uso de dados sensíveis – não são problemas exclusivamente associados ao uso da tecnologia de reconhecimento facial. Os vieses consistem em influências capazes de gerar discriminação, seja por causa de um algoritmo injusto, pela má qualidade dos dados ou pela utilização inadequada dos resultados obtidos. A imprecisão está relacionada ao percentual de falhas identificáveis nos usos de novas tecnologias de identificação e individualização de pessoas. Ademais, há diversos potenciais nocivos que envolvem a utilização de dados pessoais sensíveis, como os dados biométricos – também relacionados à discriminação, mas também à privacidade, dignidade e outros direitos fundamentais. MELO, Pedro Raphael Vieira. **Reconhecimento facial automatizado para fins de segurança pública e seus riscos aos titulares dos dados biométricos**. 31 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Instituto Brasileiro de Ensino Desenvolvimento e Pesquisa (IDP), Brasília, DF, 2020. Disponível em: https://repositorio.idp.edu.br//handle/123456789/3523. Acesso em: 26 jul. 2022. BRAGA, Carolina. Discriminação nas decisões por algoritmos: polícia preditiva. *Em*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 671–696.

e sim presa desde 2015.[117] A Polícia Militar, na ocasião, explicou que a probabilidade de acerto do algoritmo era de 70%.[118] Como observa Siqueira:

> As semelhanças faciais num mesmo contingente populacional também fazem com que, quanto maior a base de dados utilizada, maior seja a probabilidade de falsos positivos – ocorrências em que o sistema atribui incorretamente o rosto analisado a outro ao qual ele não corresponde de fato.[119]

Além dos resultados imprecisos ou errados, há uma preocupação com o potencial discriminatório e marginalizante da prática. A Rede de Observatórios da Segurança realizou o monitoramento do uso dessa tecnologia em quatro estados (Bahia, Rio de Janeiro, Santa Catarina e Paraíba), de março a outubro de 2019. Dentre 42 pessoas abordadas, 90,5% eram negras.[120] Por isso, o reconhecimento facial é uma utilização da inteligência artificial considerada de risco elevado.[121]

Também é preciso ter em conta que, com a Internet das coisas, são cada vez mais diversas as fontes e possibilidades de coleta de imagem e som. Com uma tecnologia computacional que progride para uma escala quase microscópica, são criados sensores que podem ser facilmente acoplados a câmeras e adaptados nos mais diversificados portadores. Causa estranhamento a ideia de um rato carregando uma câmera, mas com a união entre neurociência e computação isso já é realidade:

---

117 WERNECK, Antônio. Reconhecimento facial falha em segundo dia, e mulher inocente é confundida com criminosa já presa. *In*: O GLOBO, [*s. l.*], 11 jul. 2019. Disponível em: https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913. Acesso em: 19 ago. 2022.

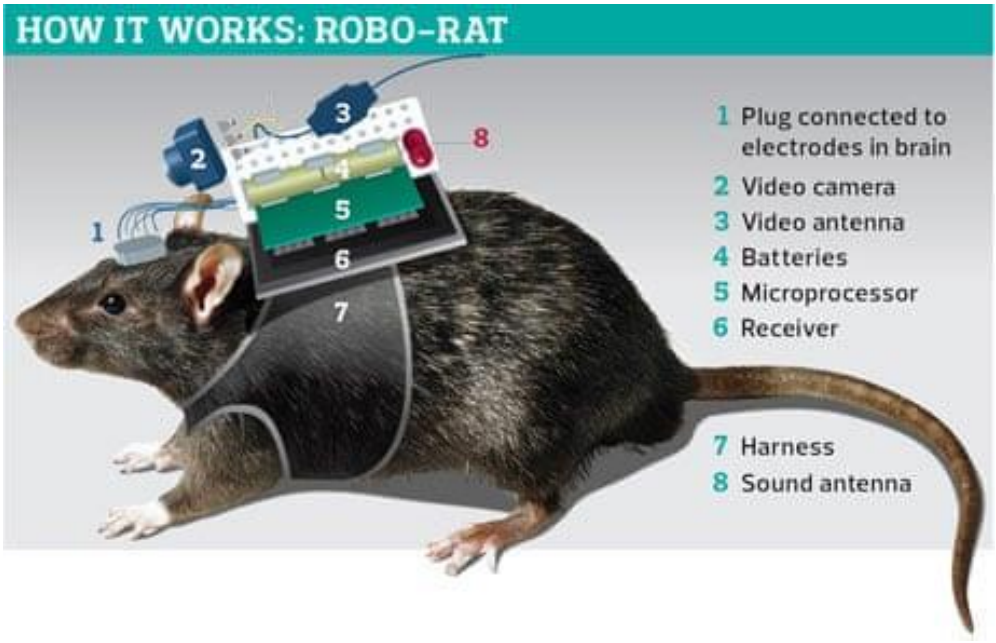
118 SISTEMA de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. *In*: G1, [*s. l.*], 11 jul. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 19 ago. 2022.

119 SIQUEIRA, Deborah. A tecnologia de reconhecimento facial aplicada à segurança pública. *In*: JOTA Info, [*s. l.*], 23 jul. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-tecnologia-de-reconhecimento-facial-aplicada-a-seguranca-publica-23072019. Acesso em: 19 ago. 2022.

120 NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. *In*: REDE OBSERVATÓRIOS DA SEGURANÇA. **Retratos da violência**: cinco meses de monitoramento, análises e descobertas. [*S. l.*]: CESEC, 2019. p. 69.

121 CANTARINI, Paola. Marco legal da IA (PL 21/20): análise comparativa à luz da regulamentação europeia (AI Act) e a questão da proteção do segredo industrial. *In*: COLOMBO, Cristiano; ENGELMANN, Wilson; FALEIROS JÚNIOR, José Luiz de Moura (org.). **Tutela jurídica do corpo eletrônico**: novos desafios ao direito digital. Indaiatuba: Foco, 2022. p. 703–722.

Figura 6 – Componentes de um “rato robô”



Fonte: The Observer.[122]

Por meio de eletrodos conectados ao cérebro do roedor, ligados a um microprocessador e a um transmissor sem fios, espera-se que seja possível manipular o comportamento e os movimentos do “rato robô”.[123] A intenção alegada é o treinamento do animal para atividades como o resgate em emergências, sendo que os ratos conseguem entrar em locais que um cão farejador ou um bombeiro, por exemplo, não conseguem alcançar.[124]

Porém, já há tecnologia semelhante sendo comercializada online – como é o caso do *RoboRoach Bundle*, vendido por US$ 159,99 e enviado para o mundo todo pela empresa norte-americana *Backyard Brains*.[125] Trata-se de um equipamento computacional passível de acoplamento em baratas (vivas, que a companhia também vende) e que permite o controle do inseto por meio de um aplicativo de *smartphone*. Qualquer um pode adquirir o item, que poderá ser utilizado para as mais diversas

---

122 ANTHES, Emily. The race to create “insect cyborgs”. **The Observer**, [*s. l.*], 17 fev. 2013. Science. Disponível em: https://www.theguardian.com/science/2013/feb/17/race-to-create-insect-cyborgs. Acesso em: 12 ago. 2022.

123 YU, Yipeng *et al.* Automatic training of rat cyborgs for navigation. **Computational Intelligence and Neuroscience**, [*s. l.*], v. 2016, p. e6459251, 2016. Disponível em: https://www.hindawi.com/journals/cin/2016/6459251/. Acesso em: 30 ago. 2022.

124 ANTHES, Emily. The race to create “insect cyborgs”. **The Observer**, [*s. l.*], 17 fev. 2013. Science. Disponível em: https://www.theguardian.com/science/2013/feb/17/race-to-create-insect-cyborgs. Acesso em: 12 ago. 2022.

125 BACKYARD BRAINS. **The RoboRoach Bundle**. Ann Arbor: Backyard Brains, [2022?]. Disponível em: https://backyardbrains.com/products/roboroach. Acesso em: 19 ago. 2022.

finalidades.[126] Assim, além de toda a preocupação que essa tecnologia deveria despertar em termos da ética com o uso de animais, o risco para a privacidade é extremamente elevado.

Ademais, com acesso a bancos de dados que possam servir para comparação, qualquer imagem contendo as feições de uma pessoa torna-se objeto para a aplicação de tecnologias de reconhecimento – também sujeito às interferências conhecidas como *deepfakes*.[127] Desse modo, não há uma preocupação com o consentimento do titular dos dados ou com a apresentação de justificativa proporcional para a utilização de conteúdo constante em sites e redes sociais. Como explica Joh:

> Ao aplicar a análise computadorizada a grandes coleções de dados digitalizados, as agências policiais podem identificar pessoas e atividades suspeitas em grande escala. Embora essas ferramentas sejam úteis para rastrear evidências de crimes passados, o *big data* também fornece à polícia novas capacidades para identificar ameaças atuais e futuras.[128]

Isso eleva a preocupação com os poderes dos agentes policiais. De fato, há diversas outras atividades que também auxiliam esses órgãos na atividade de garantia da segurança. Muitas delas estão incluídas na análise de dados chamada de policiamento preditivo. Nessa prática estão incluídos o objetivo de previsão de delitos, locais ou grupos de infratores específicos, mas também a criação de um controle indireto do comportamento, com a dissuasão pelo conhecimento de que a tecnologia pode ser utilizada para garantir a segurança pública.[129]

---

[126] Mendes e Pinheiro, inclusive, apontam que pode haver outros usos intrusivos na privacidade para os insetos ciborgues, conjecturando a hipótese de manipulação dessa ferramenta para coleta de DNA sem consentimento do titular desse dado sensível. MENDES, Gilmar Ferreira; PINHEIRO, Jurandi Borges. Interceptações e privacidade: novas tecnologias e a Constituição. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 231–250.

[127] *Deepfake* é uma mídia falsa, criada por ferramentas de aprendizado profundo, chamadas de redes adversárias generativas (GANs), uma rede detectora que analisa uma rede forjadora, que se retroalimentam para melhorar suas habilidades. Por meio desta tecnologia, é possível obter um vídeo, por exemplo, em que uma pessoa fala ou faz algo que nunca aconteceu no mundo real. LEE, Kai-Fu; QIUFAN, Chen. **2041**: como a inteligência artificial vai mudar sua vida nas próximas décadas. Rio de Janeiro: Globo Livros, 2022.

[128] Tradução nossa de: “By applying computer analytics to very large collections of digitized data,6 law enforcement agencies can identify suspicious persons and activities on a massive scale.7 While these tools are useful in tracking down evidence of past crimes, big data also provides the police with new capabilities to identify ongoing and future threats”. JOH, Elizabeth E. The new surveillance discretion: automated suspicion, big data, and policing symposium: policing in America on the 50th anniversary of Miranda v. Arizona. **Harvard Law & Policy Review**, [*s. l.*], v. 10, n. 1, p. 18, 2016.

[129] HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. Rio de Janeiro: Forense, 2021.

Estas tecnologias prometem identificar onde um crime pode acontecer em determinado lapso temporal (policiamento preditivo baseado no local) ou quem se envolverá em um delito, como vítima ou infrator (baseado na pessoa).[130] Há inúmeros programas que fazem esses tipos de análise. Com relação ao local, destaca-se o Geolitica (antigo PredPol).

O PredPol/Geolitica mudou a forma como a polícia se relaciona com os recursos tecnológicos, que se tornaram o centro da ação policial.[131] Atualmente, a empresa alega "[...] proteger uma a cada 30 pessoas nos Estados Unidos".[132] Seu algoritmo foi originalmente desenvolvido para medir os impactos sísmicos de um terremoto, mas constatou-se que a criminalidade segue um padrão semelhante. Assim, parte-se da ideia de que há um efeito cascata, sendo que a ocorrência de um crime em uma determinada área pode ser o gatilho para um novo delito no mesmo local em breve.[133] O sistema tem várias telas com estatísticas, dentre as quais o seguinte *printscreen*:

---

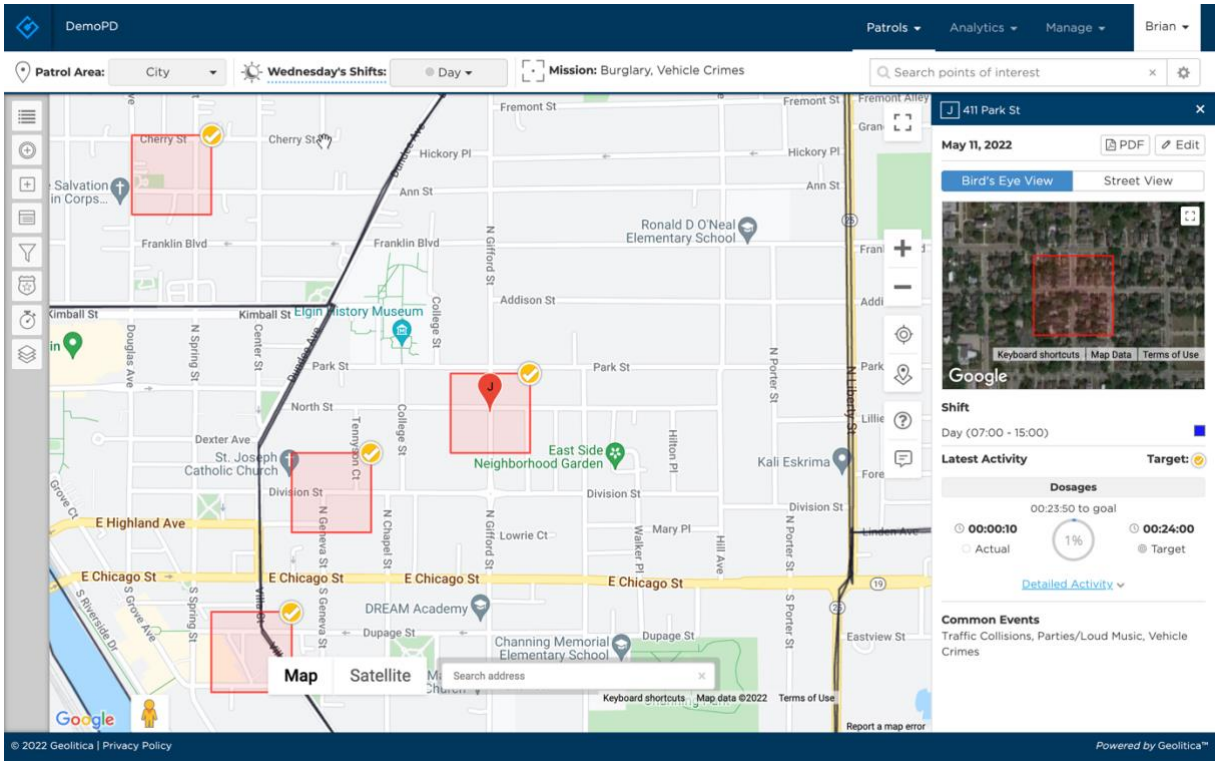
130 BRAGA, Carolina. Discriminação nas decisões por algoritmos: polícia preditiva. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 671–696.

131 BENBOUZID, Bilel. To predict and to manage: predictive policing in the United States. **Big Data & Society**, [*s. l.*], v. 6, n. 1, 2019. Disponível em: https://journals.sagepub.com/doi/pdf/10.1177/2053951719861703. Acesso em: 30 ago. 2022.

132 GEOLITICA. **Company**. Santa Cruz: Geolitica, [2022?]. Disponível em: https://geolitica.com/company/. Acesso em: 21 ago. 2022.

133 FERGUSON, Andrew G. **The rise of big data policing**: surveillance, race, and the future of law enforcement. New York: New York University Press, 2017. *E-book*.

Figura 7 – Previsão de eventos comuns por local



Fonte: Geolitica.[134]

No canto inferior da imagem, se lê: “Eventos comuns: colisões de tráfego, festas/música alta, crimes com veículos” (tradução nossa). As áreas delimitadas em vermelho, no mapa, são os locais onde eles ocorrem. Percebe-se a possibilidade de alterar os parâmetros da pesquisa, indicando o perímetro, o período e o tipo de crime que se quer prever.

De acordo com O’Neil, o principal problema desse sistema é que ele considera crimes menores da mesma forma que os mais graves. Ao adotar o sistema, os departamentos policiais podem optar por incluir ou não crimes de “perturbação”, como vadiagem e consumo ou venda de pequenas quantidades de entorpecentes. Normalmente, esses delitos não seriam registrados se o policial não os presenciasse. Porém, sua inclusão no sistema distorce a análise realizada:

> Uma vez que os dados de perturbação fluam para dentro de um modelo de previsão, mais policiais são atraídos para aqueles bairros, onde é mais provável que prendam mais pessoas. Afinal, mesmo que o objetivo seja impedir assaltos, assassinatos e estupros, sempre haverá períodos calmos. É da natureza do patrulhamento. E se um policial em patrulha vê alguns jovens que não parecem ter mais de

[134] GEOLITICA. **Using Geolitica to implement DDACTS**. Santa Cruz: Geolitica, [2022?]. Disponível em: https://geolitica.com/blog/using-geolitica-to-implement-ddacts/. Acesso em: 21 ago. 2022.

> dezesseis anos bebendo algo de uma garrafa escondida, ele os para. Esses tipos de crimes de menor grau povoam os modelos com mais e mais pontos, e os modelos enviam os policiais de volta aos mesmos bairros. Isso cria um ciclo nocivo de feedback. A própria polícia gera novos dados, o que justifica mais policiamento. E nossos presídios se enchem de centenas de milhares de pessoas condenadas por crimes sem vítimas. A maioria delas vem de bairros empobrecidos, e a maioria é negra ou hispânica.[135]

Portanto, essas ferramentas, que são vendidas com a promessa de neutralização de preconceitos (conscientes ou não)[136] e que afirmam não considerar cor de pele,[137] fornecem resultados contaminados de vieses. Nesse sentido, são potenciais catalizadores de discriminação, assim como a tecnologia de reconhecimento facial – que usa a imagem da pessoa e não consegue negar as influências de raça e cor.

Assim, ocorre o mesmo com o policiamento preditivo baseado na pessoa. Nessa área, destacam-se as pontuações de ameaça – que também são utilizados no judiciário para fins de dosimetria da pena e sua execução, neste caso, chamados de *risk assessment practices*.[138] Em suma, os algoritmos analisam dados – publicamente disponíveis, como em redes sociais, ou coletados pelos órgãos de segurança – para categorizar riscos de determinado indivíduo cometer um crime.[139]

No caso dos *risk assessments*, há dados que são coletados especificamente para a finalidade de análise algorítmica quando uma pessoa entra no sistema prisional. Trata-se de questionários como o *Level of Service Inventory* (LSI), utilizado em Idaho, nos Estados Unidos, que é uma página assim:

---

135 O'NEIL, Cathy. **Algoritmos de destruição em massa**. 1. ed. Santo André: Rua do Sabão, 2020. p. 83.

136 BRAGA, Carolina. Discriminação nas decisões por algoritmos: polícia preditiva. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 671–696.

137 O'NEIL, Cathy. **Algoritmos de destruição em massa**. 1. ed. Santo André: Rua do Sabão, 2020.

138 SULOCKI, Victoria de. Novas tecnologias, velhas discriminações: ou da falta de reflexão sobre o sistema de algoritmos na Justiça Criminal. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 651–670.

139 BRAGA, Carolina. Discriminação nas decisões por algoritmos: polícia preditiva. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 671–696.

Figura 8 – Questionário de *risk assessment* do LSI

LEVEL OF SERVICE INVENTORY – REVISED (IDOC)

Client Name:_____ IDOC#:_____

Staff Name:_____ LSI Completion Date:_____ Scoring Reminders for the Paper Scoresheet

Enter scores for items 1-54 using 0 for no (no risk) and 1 for yes (risk).

CRIMINAL HISTORY

1. _____ (E) *Any prior convictions, adult / number* ☐ (Count Box)
2. _____ (E) *Two or more prior convictions* (0=No 1=Risk)
3. _____ (E) *Three or more prior convictions*
4. _____ (C) *Three or more present offenses / number* ☐
5. _____ (E) *Arrested under age 16 / age 1st arrest* ☐
6. _____ (E) *Ever incarcerated upon conviction*
7. _____ (E) *Escape history - institution*
8. _____ (E) *Ever punished for institutional misconduct / number* ☐
9. _____ (E) *Charge laid or probation / parole suspended during prior community supervision*
10. _____ (E) *Record of assault / violence*

Subtotal Score_____/10 = (%)

EDUCATION / EMPLOYMENT

When in labor market:

11. _____ (C, IN2) *Currently unemployed*
12. _____ (YR, IN2) *Frequently unemployed*
13. _____ (E) *Never employed for a full year*
14. _____ (E) *Ever fired*

School or when in school:

15. _____ (E) *Less than regular grade 10*
16. _____ (E) *Less than regular grade 12*
17. _____ (E) *Suspended or expelled at least once*

Homemaker, Pensioner: 18 only

School, work, unemployed: 18, 19, 20

18. _____ (C) *Participation / Performance* 0 1 2 3 +_____ (Rater Box)
19. _____ (C) *Peer interactions* 0 1 2 3 +_____ (0=No 1=Risk)
20. _____ (C) *Authority interactions* 0 1 2 3 +_____

Subtotal Score_____/10 = (%)

Remember! The Rater Boxes clue you into what protective factors are present or lacking! Score these based on the client's perspective.

FINANCIAL

21. _____ (YR) *Problems* 0 1 2 3 +_____
22. _____ (YR) *Reliance upon social assistance*

Subtotal Score_____/2 = (%)

FAMILY / MARITAL

23. _____ (YR) *Dissatisfaction with marital or equivalent situation* 0 1 2 3 +_____
24. _____ (YR) *Non rewarding, parental* 0 1 2 3 +_____
25. _____ (YR) *Non rewarding, other* 0 1 2 3 +_____
26. _____ (E) *Criminal family / spouse*

Subtotal Score_____/4 = (%)

ACCOMMODATION

27. _____ (C) *Unsatisfactory* 0 1 2 3 +_____
28. _____ (YR, IN2) *3 or more address changes last year / number* ☐
29. _____ (C) *High crime neighborhood*

Subtotal Score_____/3 = (%)

LEISURE / RECREATION

30. _____ (YR, IN2) *No recent participation in organized activity*
31. _____ (YR) *Could make better use of time* 0 1 2 3 +_____

Subtotal Score_____/2 = (%)

COMPANIONS

32. _____ (YR) *A social isolate*
33. _____ (YR) *Some criminal acquaintances*
34. _____ (YR) *Some criminal friends*
35. _____ (YR) *Few anti-criminal acquaintances*
36. _____ (YR) *Few anti-criminal friends*

Subtotal Score_____/5 = (%)

ALCOHOL / DRUG PROBLEMS

37. _____ (E) *Alcohol problem, ever*
38. _____ (E) *Drug problem, ever*
39. _____ (YR, IN2) *Alcohol problem, currently* 0 1 2 3 +_____
40. _____ (YR, IN2) *Drug problem, currently* 0 1 2 3 +_____

Specify drug:_____

41. _____ (YR) *Law violation*
42. _____ (YR) *Marital / family*
43. _____ (YR) *School / work*
44. _____ (YR) *Medical*
45. _____ (YR) *Other Clinical indicators*

Specify:_____

Subtotal Score_____/9 = (%)

EMOTIONAL / PERSONAL

46. _____ (YR) *Moderate interference*
47. _____ (YR) *Severe interference*
48. _____ (E) *Mental health treatment, past*
49. _____ (YR) *Mental health treatment, current*
50. _____ (YR) *Psychological assessment indicated*

Area:_____

Subtotal Score_____/5 = (%)

ATTITUDE / ORIENTATION

51. _____ (C) *Supportive of crime* 0 1 2 3 +_____
52. _____ (C) *Unfavorable attitude toward convention* 0 1 2 3 +_____ (0=No 1=Risk)
53. _____ (C) *Poor attitude toward sentence / conviction*
54. _____ (C) *Poor attitude towards supervision*

Subtotal Score_____/4 = (%)

TOTAL RISK SCORE _____

TOTAL PROTECTIVE SCORE _____

HIGHEST CRIMINOGENIC NEED _____

STAGE OF CHANGE _____

Results Interpretation Area

Total Risk = Total of 1s and 0s.

Total Protective = Total of all Rater Boxes

High Crim Need = most potent domain in the wall.

Stage of Change = client's stage of change in the high crim need you selected. You can use the Readiness Scale (Hanna's Precursor Model) to confirm.

	CH	E/E	Fin	Fam	Accm	Leis	Comp	A/D	Em/Pr	Att	
High	8-10	8-10	2	4	3	2	4-5	7-9	4-5	4	*High*
Mod/High	6-7	5-7		3	2		3	5-6	3	3	*Mod/High*
Moderate	3-5	3-4	1	2	1	1	2	3-4	2	2	*Moderate*
Low/Mod	1-2	2	0	1	0	0	1	1-2	1	1	*Low/Mod*
Low	0	0-1		0			0	0	0	0	*Low*

Fonte: EPIC.[140]

Os critérios dos questionários realizados para esse fim variam de aspectos subjetivos (saúde mental, personalidade, isolamento social etc.) até informações

[140] ELECTRONIC PRIVACY INFORMATION CENTER (EPIC). **Liberty at risk, pre-trial risk assessment tools in the U.S**. Washington, DC: EPIC, 2021. Disponível em: https://archive.epic.org/LibertyAtRiskReport.pdf. Acesso em: 16 jun. 2022.

privadas (estado civil, financeiro, residencial etc.).[141] Também verifica prévio envolvimento com delitos e o que o respondente pensa sobre o crime.

Além do problema dos vieses, muito marcante no policiamento preditivo,[142] é preocupante que nem sempre existe um controle de validade (validação) do programa utilizado. Também é preciso considerar a questão da transparência, incluindo o fato de que, muitas vezes, os sistemas pertencem a empresas privadas – o que dificulta sobremaneira a identificação dos processos de tomada de decisão e seu esclarecimento.[143]

Com alguns exemplos já se pode constatar que as novas tecnologias prometem inúmeros benefícios para a garantia da segurança pública. Porém, também se percebe que há muitos riscos para direitos fundamentais individuais, como o recentemente incluído no rol constitucional direito à proteção de dados pessoais. O próximo capítulo, nesse sentido, pretende delinear os contornos dos direitos em colisão, a fim de verificar em que medida é possível limitar o direito à proteção de dados pessoais para garantir a realização do direito à segurança pública.

---

141 SULOCKI, Victoria de. Novas tecnologias, velhas discriminações: ou da falta de reflexão sobre o sistema de algoritmos na Justiça Criminal. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 651–670.

142 BRAGA, Carolina. Discriminação nas decisões por algoritmos: polícia preditiva. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 671–696.

143 ELECTRONIC PRIVACY INFORMATION CENTER (EPIC). **Liberty at risk, pre-trial risk assessment tools in the U.S**. Washington, DC: EPIC, 2021. Disponível em: https://archive.epic.org/LibertyAtRiskReport.pdf. Acesso em: 16 jun. 2022.

3 OS DIREITOS FUNDAMENTAIS À SEGURANÇA PÚBLICA E À PROTEÇÃO DE DADOS PESSOAIS NO DIREITO CONSTITUCIONAL E INFRACONSTITUCIONAL BRASILEIRO

A ciência e a técnica tornaram-se uma nova forma de ideologia. Habermas fala em uma "consciência tecnocrática", menos ideológica que as ideologias anteriores. Ela transforma a ciência em um "feitiço", com maior alcance e potencial de dominação, pois não visa apenas o atendimento dos interesses de uma ou outra classe, mas também de todo o gênero humano. A técnica, nesse contexto, apresenta-se como fundamental para a satisfação de "necessidades privatizadas".[144]

De acordo com Gabriel, há uma diferença entre técnica e tecnologia, que ele assim explica:

> Técnica é o processo de produção de instrumentos em nome do aprimoramento das nossas condições de vida. Tecnologia, em contrapartida, é mais do que a soma dos instrumentos que se encontram em uso em um determinado tempo. Ela designa, antes, o nosso *logos;* ou seja, a nossa representação daquilo que é técnica.[145]

A era digital é revolucionária no sentido de que produziu uma técnica que administra tecnologias, fazendo com que a técnica forneça, atualmente, representações do que o ser humano quer fazer e ser.[146] O poder relacionado à técnica e às tecnologias, nesse sentido, é sem precedentes. Surge, então, um novo paradoxo, como apontado por Schiocchet: "A questão ética central, encontrada na sociedade tecnocientífica, explicita-se no paradoxo da técnica moderna, quando não é o fracasso, mas o seu sucesso, que pode levar a uma catástrofe global".[147]

Os riscos do sucesso da técnica ficam evidentes quando se pensa que ele se sustenta em uma falácia: da sua neutralidade. Como bem coloca Galimberti:

---

144 HABERMAS, Jürgen. **Técnica e ciência como "ideologia"**. 1. ed. Lisboa: Edições 70, 2011. p. 80–81.

145 GABRIEL, Markus. **O sentido do pensar**: a filosofia desafia a inteligência artificial. Petrópolis: Vozes, 2021. p. 135.

146 GABRIEL, Markus. **O sentido do pensar**: a filosofia desafia a inteligência artificial. Petrópolis: Vozes, 2021.

147 SCHIOCCHET, Taysa. O humano entre o direito e a genética: pressupostos para o debate legislativo acerca das implicações jurídicas concernentes à criação de bancos de perfis genéticos para fins de persecução criminal no Brasil. *In*: SCHIOCCHET, Taysa (org.). **Bancos de perfis genéticos para fins de persecução criminal**: análise interdisciplinar e em direito comparado. Rio de Janeiro: Multifoco, 2015. p. 37.

> Para nos orientar, precisamos antes de tudo acabar com as falsas inocências, com a fábula da técnica *neutra*, que só oferece os *meios*, cabendo depois aos homens empregá-los para o bem ou para o mal. A técnica não é neutra, porque cria um mundo com determinadas características com as quais não podemos deixar de conviver e, vivendo com elas, contrair hábitos que nos transformam obrigatoriamente.[148]

Não apenas o bom ou mau uso da técnica constitui um risco. Sua mera utilização modifica o ser humano.[149] Porém, como aponta Lyon, não se pode avançar para um determinismo tecnológico,[150] perspectiva reducionista sob a qual "[...] o fator tecnológico é determinante de um sistema cultural como um todo; ele determina [...] a forma dos sistemas sociais, da tecnologia e da sociedade".[151] Nesse sentido, é importante não subestimar o papel dos fatores sociais na configuração da tecnologia, nem a variedade de contextos sociais que mediam sua utilização – o que, por sua vez, não torna os impactos tecnológicos diretamente previsíveis.[152]

Assim, "No quadro de uma sociedade técnica, o Estado tem de intervir antes as novas ameaças de uma técnica que aumentou as fontes de perigo".[153] O Direito, nesse contexto, tem relevante papel social na modulação dos impactos do uso de novas tecnologias – sobretudo quando elas são utilizadas sob justificativa de efetivar algum direito. É o caso das atividades exploradas no item anterior deste trabalho, que prometem um incremento na garantia da segurança pública (*lato sensu*), mas que geram uma variedade de novos riscos a outros direitos. Como salienta Doneda:

> Novas técnicas e métodos devem ser construídos para a efetiva tutela de direitos que, não raro, deve procurar meios para incidir diretamente em processos que, aparentemente, estariam alheios à pessoa em si, como o da implementação e uso de novas tecnologias, porém cujos

---

148 GALIMBERTI, Umberto. **Psiche e techne**: o homem na idade da técnica. São Paulo: Paulus, 2006. p. 8.

149 GALIMBERTI, Umberto. O ser humano na era da técnica. **Cadernos IHU Ideais**, São Leopoldo, v. 13, n. 218, 2015.

150 LYON, David. **El ojo electrónico**: el auge de la sociedad de la vigilancia. Madrid: Alianza, 1995.

151 MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. Apontamentos sobre direito, ciência e tecnologia na perspectiva de políticas públicas sobre regulação em ciência e tecnologia. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 91.

152 LYON, David. **El ojo electrónico**: el auge de la sociedad de la vigilancia. Madrid: Alianza, 1995.

153 LOUREIRO, João Carlos. Constituição, tecnologia e risco(s): entre medo(s) e esperança(s). *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 52.

> reflexos incidem direta – e por vezes cruelmente – sobre a arquitetura de nossas vidas, quando não sobre nós mesmos.[154]

Por isso, este capítulo (3), de natureza descritiva, pretende identificar os contornos do direito fundamental à segurança pública, bem como da recentemente positivada garantia fundamental à proteção de dados pessoais – que a ele pode ser contraposta. Com isso, a intenção é delimitar seus respectivos âmbitos de proteção para que se possa analisar a aparente colisão entre estes direitos, com a apreciação das limitações que podem ser impostas aos direitos fundamentais (3.1).

Em seguida, o item 3.2 objetiva mapear a legislação vigente e prospectiva acerca da prevenção e repressão penal realizada com uso de dados pessoais. Nesse sentido, busca-se analisar, especialmente, o Projeto de Lei nº 1.515, de 2022 (LGPD Penal), a fim de identificar como essa norma pretende equalizar a realização dos direitos fundamentais à proteção de dados pessoais e à segurança pública.

3.1 Os contornos, a colisão e as limitações dos direitos fundamentais à segurança pública e à proteção de dados pessoais

O termo “segurança” aparece 34 vezes na Constituição de 1988, sendo 25 dessas referências relacionadas à seguridade social. Além dessa concepção, há diversos outros significados para a ocorrência do substantivo no texto constitucional. É possível identificar que a polissemia do termo permite que ele possa “[...] significar coisas tão dispares como certeza jurídica, proteção civil contra desastres, garantia em face dos arbítrios estatais e segurança pública enquanto garantia da ordem pública, além dos novos conceitos de segurança humana, segurança alimentar e tantos outros”.[155]

No preâmbulo da Constituição, a segurança é citada como valor supremo a ser garantido pelo Estado Democrático de Direito instituído pela nova ordem

---

[154] DONEDA, Danilo. Prefácio. *In*: COLOMBO, Cristiano; ENGELMANN, Wilson; FALEIROS JÚNIOR, José Luiz de Moura (org.). **Tutela jurídica do corpo eletrônico**: novos desafios ao direito digital. Indaiatuba: Foco, 2022. p. X.

[155] ERTHAL, Carolina Naciff de Andrade. **A segurança pública como direito fundamental e como tarefa estatal na Constituição brasileira de 1988**. 228 f. Dissertação (Mestrado em Direito e Ciência Jurídica) - Universidade de Lisboa, Lisboa, 2020. Disponível em: https://repositorio.ul.pt/bitstream/10451/48042/1/ulfd145961_tese.pdf. Acesso em: 6 ago. 2022. p. 9.

constitucional.[156] Nesse contexto, o termo faz referência à "[...] causa final do Estado, a razão da sua existência".[157] Assim, pode-se dizer que se trata de uma noção basilar de segurança, que fundamenta a própria criação do Estado e sua caracterização como democrático e de direito.

Já no artigo 5º, que garante a inviolabilidade da segurança aos brasileiros e estrangeiros residentes no país, trata-se de uma referência a um direito individual, uma liberdade pública. De acordo com Santin:

> As liberdades públicas são os direitos do homem, originários do direito natural, convertidos em direitos humanos ou direitos e garantias fundamentais, por normatização pelo ordenamento jurídico moara proteção do cidadão em face do Estado, sendo exemplos tradicionais o direito à vida, à liberdade, à incolumidade pessoal, as garantias processuais e o direito de ação.[158]

Constitui, sob essa perspectiva, uma limitação do poder do Estado, protegendo a pessoa de arbitrariedades do Poder Público. Ademais, pode ser percebido como um conjunto de garantias,[159] que estão distribuídas em diversos incisos do mesmo artigo, assegurando a concretização de outros direitos individuais ou prevendo sub-categorias de segurança (segurança das relações jurídicas, do domicílio, das comunicações etc.).

Finalmente, no artigo 6º, encontra-se o direito social à segurança, também protegido no artigo 144 da Constituição, que diz que a segurança pública é "dever do Estado, direito e responsabilidade de todos" e tem como finalidade a preservação da ordem pública.[160]. Nesse sentido, o direito social resguardado no artigo 6º consiste no direito à segurança pública, como explica Silva:

> Como direito social, a segurança é especialmente a obtenção de uma convivência social que permita o gozo de direitos e o exercício de

---

156 BRASIL. **Constituição Federal**. [Constituição (1988)]. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 ago. 2022.

157 BUONAMICI, Sergio Claro. Direito fundamental social à segurança pública. **Revista de Estudos Jurídicos da UNESP**, [*s. l.*], v. 15, n. 21, 2011. Disponível em: https://doi.org/10.22171/rej.v15i21.341. Acesso em: 1 ago. 2022.

158 SANTIN, Valter Foleto. Segurança pública e sua política. *In*: **Controle judicial da segurança pública**: eficiência do serviço na prevenção e repressão do crime. 2. ed. São Paulo: Verbatim, 2013. p. 47. *E-book*.

159 SILVA, José Afonso da. **Comentário contextual à Constituição**. 6. ed. São Paulo: Malheiros, 2009.

160 BRASIL. **Constituição Federal**. [Constituição (1988)]. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 ago. 2022.

> atividades sem perturbação de outrem. Vale dizer, direito à segurança, no artigo 6º, prende-se ao conceito de segurança pública.[161]

A extensão e os limites desse direito à segurança pública dependem da concepção de ordem pública, que não é pacífica. Para Lopes Jr., trata-se de um conceito "[...] vago, impreciso, indeterminado e despido de qualquer referencial semântico [...]", frequentemente utilizado para justificar ações autoritárias.[162] Por outro lado, há quem defenda a noção de ordem pública como referência "[...] à preservação da paz, à inexistência de desordem e/ou conflitualidade e à garantia dos direitos individuais".[163] Como aponta Cabral:

> Tal obrigação geral de proteção é uma consequência primária da atribuição, ao Estado, do monopólio da utilização da força, o que garante a existência da sociedade enquanto ordem de paz, na qual a autodefesa dos particulares é, em princípio, vedada, donde decorre que, em contrapartida, aquele Estado tem de garantir a protecção dos seus cidadãos contra agressões ou ameaças de terceiros. É exactamente essa perspectiva – a do direito à segurança como garantia de direitos fundamentais e um dos pilares fundamentais do Estado de Direito – que suscita a necessidade de uma relação equilibrada entre segurança e democracia, ou entre segurança e direitos fundamentais.[164]

Nesse sentido, a segurança, na Constituição Federal, é valor e fundamento do Estado, sendo também direito individual e direito social. Assim, submete o Estado a um dever de concretização da segurança em diversas dimensões,[165] ao passo que também estabelece limites ao poder estatal.

---

161 SILVA, José Afonso da. **Comentário contextual à Constituição**. 6. ed. São Paulo: Malheiros, 2009. p. 187.

162 LOPES JÚNIOR, Aury. **Direito processual penal**. 19. ed. São Paulo: Saraiva Jur, 2022. *E-book*. p. 293.

163 DIAS, Manuel Domingos Antunes. **Liberdade, cidadania e segurança**. Coimbra: Almedina, 2001. p. 90.

164 CABRAL, José Santos. Do direito à segurança à segurança do direito. **Julgar**, Lisboa, p. 3, 2012. Disponível em: http://julgar.pt/wp-content/uploads/2014/07/JOS%C3%89SANTOSCABRAL-DODIREITO%C3%80SEGURAN%C3%87A%C3%80SEGURAN%C3%87ADODIREITO.pdf. Acesso em: 7 ago. 2022.

165 AVELINE, Paulo Vieira. **Segurança pública como direito fundamental**. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2009. Disponível em: https://tede2.pucrs.br/tede2/handle/tede/4073. Acesso em: 1 ago. 2022. p. 12.

O poder em questão é o Poder de Polícia, que a Administração Pública detém, em potencialidade, para garantir a segurança.[166] Esse poder sofre limitações, pois, como explicam Minini e Donato:

> [...] deve existir um equilíbrio razoável entre as exigências da segurança geral da sociedade e a proteção dos direitos fundamentais dos cidadãos, visto que isso implica a busca de uma harmonia dos poderes e atributos que a polícia necessita para realizar suas atividades com vista ao respeito das pessoas, evitando possíveis abusos de poder.[167]

Enquanto direito fundamental social, assim como outros direitos dessa natureza, o direito a segurança possui duas dimensões: subjetiva, inerente ao espaço de existência do indivíduo, pela afirmação de sua essencialidade; e objetiva, no sentido de haver um dever de garantia da segurança por parte do Estado e da sociedade, por meio de imposição legal ou prestações.[168] Não se trata, porém, de garantir a segurança a qualquer custo, mas de o fazer com observação aos demais preceitos consagrados no texto constitucional, especialmente outros direitos e garantias fundamentais. Esse ponto é especialmente relevante porque, como bem resumem Azevedo e Basso:

> O Estado tem o dever de propiciar segurança aos cidadãos, contendo a violência e garantindo a paz pública. Por essa razão, a segurança pública, na atualidade, converteu-se em argumento político e constitucional para a legitimação da força estatal. Para tanto, fortaleceu-se o aparato penal com o objetivo de se obter o controle da criminalidade.[169]

Assim, há um ideal, positivado constitucionalmente, de preservação do direito fundamental à segurança. Entretanto, sabe-se que há uma dificuldade de concretização desse direito, dentro de um contexto geral de entraves ao ideal do Estado Social, como consequência de uma variedade de crises.

---

166 LAZZARINI, Álvaro. Limites do poder de polícia. **Revista de Direito Administrativo**, Rio de Janeiro, v. 198, p. 69–83, 1994. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/46412. Acesso em: 28 ago. 2022.

167 MININI, Édis; DONATO, Roberto dos Santos. O exercício do poder de polícia, pela Polícia Militar, como instrumento de proteção e promoção dos direitos humanos, à luz da Constituição Federal de 1988. *In*: GORCZEVSKI, Clovis; LEAL, Mônia larissa Heninng (org.). **Constitucionalismo contemporâneo**: novos desafios. Curitiba: Multideia, 2012. p. 275.

168 CANOTILHO, Joaquim José Gomes. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra: Almedina, 2003.

169 AZEVEDO, Rodrigo Ghiringhelli de; BASSO, Maura. Segurança pública e direitos fundamentais. **Direito e Justiça**, Porto Alegre, v. 34, n. 2, p. 28, 2008.

Dentre diversas leituras da contemporaneidade, destaca-se a análise de Streck e Morais, no sentido de que o modelo de Estado moderno (e suas evoluções) enfrenta uma série de crises interconectadas, que o transformam e exaurem.[170] O Estado contemporâneo – que no Brasil sequer chegou a se concretizar em sua modalidade social[171] – passa por crises de natureza conceitual, estrutural, institucional, funcional e política.[172]

Além disso, há uma crise financeira – ou de financiamento – que normalmente é posta como a origem de todas as demais crises.[173] Historicamente, verificam-se diversas crises econômicas em nível global, como a crise de 29 e a de 2008, assim como a mais recente (cujos efeitos ainda estão em curso), decorrente de variados fatores, como a pandemia da Covid-19 e a Guerra da Ucrânia. Todas elas impactam o funcionamento do Estado, especialmente sua capacidade de garantir os direitos e instituições que o compõem.

Portanto, sob justificativa de déficit financeiro para manutenção do Estado e de seu correto funcionamento, instaura-se uma crise de confiança no modelo de gestão estatal. O Estado que não conseguiu resolver carências sociais, agora precisa lidar com um contexto de riscos difusos.[174] Com valores fundamentais perdendo força e a ascensão de um modelo de sociedade cada vez mais fluido,[175] individualista e tecnológico, os velhos moldes de Estado não parecem dar conta da complexidade do contemporâneo.

Enquanto direito social, o direito à segurança pública também sofre as influências dessas crises. Como afirma Morais, "[...] vemo-nos confrontados com uma

---

[170] STRECK, Lenio Luiz; MORAIS, José Luis Bolzan de. **Ciência política e teoria do estado**. 7. ed. Porto Alegre: Livraria do Advogado, 2010.

[171] MORAIS, José Luis Bolzan de. Estado, função social e (os obstáculos da) violência. Ou: do "mal-estar" na civilização à síndrome do medo da barbárie! *In*: CALLEGARI, André Luís (org.). **Política criminal, Estado e democracia**: homenagem aos 40 anos do curso de Direito e aos 10 anos do curso de pós-graduação em Direito da Unisinos. Rio de Janeiro: Lumen Juris, 2007. p. 69–80.

[172] STRECK, Lenio Luiz; MORAIS, José Luis Bolzan de. **Ciência política e teoria do estado**. 7. ed. Porto Alegre: Livraria do Advogado, 2010.

[173] STRECK, Lenio Luiz; MORAIS, José Luis Bolzan de. **Ciência política e teoria do estado**. 7. ed. Porto Alegre: Livraria do Advogado, 2010. p. 151.

[174] MORAIS, José Luis Bolzan de. Estado, função social e (os obstáculos da) violência. Ou: do "mal-estar" na civilização à síndrome do medo da barbárie! *In*: CALLEGARI, André Luís (org.). **Política criminal, Estado e democracia**: homenagem aos 40 anos do curso de Direito e aos 10 anos do curso de pós-graduação em Direito da Unisinos. Rio de Janeiro: Lumen Juris, 2007. p. 69–80.

[175] Como aponta Bauman, ao falar em modernidade líquida. Nesse sentido, atualmente existe um deslocamento nos "poderes de derretimento", que detém aqueles que podem "derreter os sólidos" – que neste momento de modernidade fluida seriam "[...] os elos que entrelaçam as escolhas individuais em projetos e ações coletivas – os padrões de comunicação e coordenação entre as políticas de vida conduzidas individualmente, de um lado, e as ações políticas de coletividades humanas, de outro". BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Zahar, 2001. p. 12.

nova síndrome que, não sendo fenômeno isolado, mostra-se como uma incapacidade das fórmulas modernas em responder às novas formas, faces e fenômenos de/da violência".[176] Ademais, nas palavras de Cabral:

> Estamos agora no epicentro de uma crise económica de dimensão planetária e não é preciso grande rasgo criminológico para vaticinar a dependência entre o ciclo económico recessivo, o desemprego entre os grupos mais vulneráveis e a desigualdade social, actuando como incentivos de actividade ilícita. Tal facto é potenciado pelos estímulos de um modelo de sociedade baseado num consumismo que já não é sustentável económica e socialmente.[177]

Paralelamente, e potencializando os impactos dessa crise do Estado, há uma crise específica na segurança pública. A violência não é mais a mesma. Suas novas formas passam por uma proliferação de crimes já conhecidos, mas também pela

> [...] emergência de *novas formas*, como aquelas desenvolvidas pela macrocriminalidade, aqui entendida como aquela criminalidade que ultrapassa a ação individual, bem como se desvincula de ambientes demarcáveis geograficamente, tornando-se, ela também, global, constituindo-se como uma economia que se dilui no próprio contexto das práticas financeiras globais [...].[178]

É nesse sentido que Morais destaca que não há apenas uma "violência tradicional maximizada", mas também "novas economias delitivas".[179] Estes novos modelos de violência surgem como uma resposta às crises do Estado, na medida em que se apresentam como uma alternativa "fácil" à função provedora do Estado,[180] ao passo que também aprofundam essas crises.

---

[176] MORAIS, José Luis Bolzan de. Estado, função social e (os obstáculos da) violência. Ou: do "mal-estar" na civilização à síndrome do medo da barbárie! *In*: CALLEGARI, André Luís (org.). **Política criminal, Estado e democracia**: homenagem aos 40 anos do curso de Direito e aos 10 anos do curso de pós-graduação em Direito da Unisinos. Rio de Janeiro: Lumen Juris, 2007. p. 74.

[177] CABRAL, José Santos. Do direito à segurança à segurança do direito. **Julgar**, Lisboa, p. 5, 2012. Disponível em: http://julgar.pt/wp-content/uploads/2014/07/JOS%C3%89SANTOSCABRAL-DODIREITO%C3%80SEGURAN%C3%87A%C3%80SEGURAN%C3%87ADODIREITO.pdf. Acesso em: 7 ago. 2022.

[178] MORAIS, José Luis Bolzan de. Estado, função social e (os obstáculos da) violência. Ou: do "mal-estar" na civilização à síndrome do medo da barbárie! *In*: CALLEGARI, André Luís (org.). **Política criminal, Estado e democracia**: homenagem aos 40 anos do curso de Direito e aos 10 anos do curso de pós-graduação em Direito da Unisinos. Rio de Janeiro: Lumen Juris, 2007. p. 74.

[179] MORAIS, José Luis Bolzan de. Estado, função social e (os obstáculos da) violência. Ou: do "mal-estar" na civilização à síndrome do medo da barbárie! *In*: CALLEGARI, André Luís (org.). **Política criminal, Estado e democracia**: homenagem aos 40 anos do curso de Direito e aos 10 anos do curso de pós-graduação em Direito da Unisinos. Rio de Janeiro: Lumen Juris, 2007. p. 69–80.

[180] Como exemplifica o autor, a criminalidade "emprega" muitas pessoas. O Estado não teria condições de absorver toda essa mão de obra, a fim de garantir a mínima subsistência aos indivíduos – e esta é uma de suas funções sociais. MORAIS, José Luis Bolzan de. Estado, função social e (os

A resposta ao aumento da criminalidade é acompanhada de "[...] um olhar discriminador e assujeitador. O Direito, a lei e o cárcere parecem a resposta mais rápida e 'eficaz' para algo que se apresenta como o grande perigo contemporâneo".[181] Assim, intensifica-se o fenômeno da expansão do direito penal,[182] pois, como explicam Callegari e Motta:

> [...] visualiza-se o Direito Penal como único instrumento eficaz de psicologia político-social, como mecanismo de socialização, de civilização, mas a consequência é a sua incontida expansão, submetendo-o a cargas que não pode suportar. Enquanto outros ramos do Direito vivem momentos de adaptação constitucional, revogação de leis ou apenas regulamentação administrativa, no âmbito do Direito Penal se verifica o contrário: há cada vez mais tipos penais intangíveis e abstratos; [...] a redução de determinadas garantias processuais [...].[183]

Diretamente relacionada a esta expansão do penalismo encontra-se a noção de direito penal do inimigo, que sempre esteve presente na sociedade, mas que se agrava com a situação de crise do Estado. Nas palavras de Zaffaroni,

> [...] o *inimigo da sociedade* ou *estranho*, quer dizer, o ser humano considerado como *ente perigoso ou daninho* e não como *pessoa com autonomia ética*, de acordo com a teoria política, só é compatível com um modo de Estado absoluto e que, consequentemente, as concessões do penalismo têm sido, definitivamente, obstáculos absolutistas que a doutrina penal colocou como pedras no caminho da realização dos Estados constitucionais de direito.[184]

A consequência, nesse sentido, é um aumento do controle para fins de prevenção da criminalidade, sem que necessariamente sejam observadas garantias fundamentais constitucionalmente firmadas. Também há uma desproporção na

---

obstáculos da) violência. Ou: do "mal-estar" na civilização à síndrome do medo da barbárie! *In*: CALLEGARI, André Luís (org.). **Política criminal, Estado e democracia**: homenagem aos 40 anos do curso de Direito e aos 10 anos do curso de pós-graduação em Direito da Unisinos. Rio de Janeiro: Lumen Juris, 2007. p. 69–80.

[181] MORAIS, José Luis Bolzan de. Estado, função social e (os obstáculos da) violência. Ou: do "mal-estar" na civilização à síndrome do medo da barbárie! *In*: CALLEGARI, André Luís (org.). **Política criminal, Estado e democracia**: homenagem aos 40 anos do curso de Direito e aos 10 anos do curso de pós-graduação em Direito da Unisinos. Rio de Janeiro: Lumen Juris, 2007. p. 75.

[182] SILVA SÁNCHEZ, Jesús-María. **A expansão do direito penal**: aspectos da política criminal nas sociedades pós-industriais. 3. ed. rev. e atual.ed. São Paulo: Revista dos Tribunais, 2013.

[183] CALLEGARI, André Luís; MOTTA, Cristina Reindolff da. Estado e política criminal: a expansão do direito penal como forma simbólica de controle social. *In*: CALLEGARI, André Luís (org.). **Política criminal, Estado e democracia**: homenagem aos 40 anos do curso de Direito e aos 10 anos do curso de pós-graduação em Direito da Unisinos. Rio de Janeiro: Lumen Juris, 2007. p. 3.

[184] ZAFFARONI, Eugenio Raul. **O inimigo no direito penal**. 3. ed. Rio de Janeiro: Revan, 2011. p. 12.

punição e a intensificação do direito penal do autor.[185] Tudo isso agrava ainda mais a condição de crise do Estado Social, pois enfraquece toda uma variedade de instituições e direitos previstos na Constituição.

Este cenário de crises do Direito e do Estado é, em variadas medidas, uma realidade global. Enfrenta-se um avanço do neoliberalismo, o crescimento da criminalidade (e do medo,[186] especialmente com o terrorismo e os delitos virtuais), um recrudescimento de medidas de segurança – como o controle de fronteiras, e a implementação de novas tecnologias de policiamento preditivo, por exemplo. Ademais, nas palavras de Azevedo:

> O problema da segurança pública tem sido colocado como uma das principais demandas da chamada 'opinião pública', muitas vezes amplificada por via da atuação dos meios de comunicação de massa. O 'sentimento de insegurança' é crescente, com o aumento da percepção pública a respeito das diversas esferas da criminalidade [...]. A resposta estatal é insistentemente cobrada [...].[187]

Portanto, esse contexto é utilizado como justificativa para medidas de prevenção e repressão penal, que nem sempre considera seus impactos sobre outros direitos fundamentais. No caso específico aqui tratado, as inovações tecnológicas são vistas como promessa de garantia da segurança pública – entretanto, isso "[...] mascara as perspectivas de controle político e obtenção de vantagens econômicas oriundas das práticas de vigilância e monitoramento de comunicações digitais".[188]

Tem-se uma visão utilitarista, de que essas práticas são essenciais para repressão e prevenção de incidentes. Porém, como explica Pinheiro, "[...] o aumento do vigilantismo leva a esse perigoso senso de que não importam mortos, feridos, ou direitos revogados, tudo é colateral para se alcançar o resultado, a Justiça está apenas nos olhos que observam fixos o monitor".[189]

---

185 ZAFFARONI, Eugenio Raul. **O inimigo no direito penal**. 3. ed. Rio de Janeiro: Revan, 2011.

186 AZEVEDO, Rodrigo Ghiringhelli de; BASSO, Maura. Segurança pública e direitos fundamentais. **Direito e Justiça**, Porto Alegre, v. 34, n. 2, p. 21–32, 2008.

187 AZEVEDO, Rodrigo Ghiringhelli. Tendências do controle penal na época contemporânea: reformas penais no Brasil e na Argentina. **São Paulo em Perspectiva**, São Paulo, v. 18, n. 1, p. 39 2004.

188 BEZERRA, Arthur Coelho. Privacidade como ameaça à segurança pública: uma história de empreendedorismo moral. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2, p. 233, 2016. Disponível em: https://revista.ibict.br/liinc/article/view/3720. Acesso em: 30 ago. 2022.

189 PINHEIRO, Patrícia Peck. **Direito digital**. 6. ed. rev., atual. e ampl. São Paulo: Saraiva, 2016. p. 482.

Ferramentas como reconhecimento facial, compartilhamento intragovernamental de dados, coleta de DNA para criação de perfis, obtenção de registros de acesso à Internet e de geolocalização... Todos são celebrados como benéficos em um cenário marcado por altas taxas de criminalidade e que tende ao expansionismo penal. Porém, todos esses recursos oferecem riscos a outros direitos.

Antes do reconhecimento da existência, no Brasil, de um direito fundamental à proteção de dados pessoais, a discussão cingia-se à contraposição do direito à segurança pública e o resguardo da privacidade.[190] Inclusive, alguns autores já defendiam o reconhecimento implícito do direito à proteção de dados na Constituição, justamente por deduzir sua aplicação de

> [...] alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam – aqui nos termos da CF –, os direitos à privacidade e à intimidade, no sentido do que alguns também chamam de uma 'intimidade informática'.[191]

O direito à privacidade situa-se no seio da tutela da personalidade. Ele permite que a pessoa determine "o nível de relação da própria personalidade com as outras pessoas e com o mundo exterior",[192] garantindo o fortalecimento de uma esfera privada individual, "na qual seja possível a construção da individualidade e o livre desenvolvimento da personalidade sem a pressão indevida de mecanismos de controle social".[193]

Em outras palavras, é dizer que o direito à privacidade garante a existência de um espaço privado individual a cada pessoa simplesmente por ser pessoa, permitindo que o próprio indivíduo controle suas informações pessoais (que fornece ou recebe),

---

[190] A esse respeito, por exemplo: OLIVEIRA, Débora Martins. **A (in) constitucionalidade das prisões por reconhecimento facial via câmeras de vídeo**: conflito entre o direito à privacidade e o direito à segurança pública? 30 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Faculdade Três Pontas - Grupo UNIS, Três Pontas, 2020. Disponível em: http://repositorio.unis.edu.br/handle/prefix/1767. Acesso em: 27 jul. 2022. PINHEIRO, Patrícia Peck. **Direito digital**. 6. ed. rev., atual. e ampl. São Paulo: Saraiva, 2016.

[191] SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados pessoais. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book* (não paginado).

[192] 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, 2020.

[193] 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, 2020.

não apenas mediante o resguardo delas ao âmbito do segredo, mas também pelo domínio da circulação dessas informações.[194] Portanto, como esclarece Leonardi:

> [...] parece haver um consenso doutrinário e jurisprudencial a respeito da necessidade de sua tutela [da privacidade] do modo mais amplo possível, ante a caracterização da privacidade como *direito de personalidade* e como *direito fundamental*, cuja base é o princípio da dignidade da pessoa humana, consagrado pela Constituição Federal de 1988 como um dos fundamentos da República [...].[195]

A privacidade é amplamente resguardada pelo ordenamento pátrio. Na Constituição Federal, encontra-se disposto que "a intimidade, a vida privada, a honra e a imagem das pessoas"[196] são invioláveis. Já o Código Civil, quando trata dos direitos da personalidade, entre os artigos 11 e 21,[197] dilui diversas disposições de proteção à privacidade.

Entretanto, os debates travados com relação à privacidade no contexto da Quarta Revolução Industrial, hiperconectado, evoluíram para o reconhecimento de um direito à proteção de dados pessoais.[198] Como explica Mendes:

> Já existe uma rica experiência institucional em curso, há mais de duas décadas, que reconhece a evolução do conceito de privacidade, de modo a abarcar a proteção dos dados pessoais do cidadão no nosso ordenamento jurídico, o que pode ser percebido, para além da evolução da jurisprudência do STF [...], também a partir de inúmeras leis setoriais que garantem a proteção de dados pessoais – Código de Defesa do Consumidor, Lei do Cadastro Positivo, Lei de Acesso à Informação e Marco Civil da Internet – e cujo ápice foi a recente sanção da Lei Geral de Proteção de Dados (Lei nº 13.709/2018).[199]

A doutrina também teve papel fundamental no delineamento dessa evolução do direito à privacidade para o seu desdobramento em um direito à proteção de dados

---

194 LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

195 LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012. p. 90.

196 É parte da redação do inciso X do artigo 5º. BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/ constituicao/constituicao.htm. Acesso em: 12 abr. 2022.

197 BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Presidência da República: Brasília, DF Disponível em: http:// www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm. Acesso em: 11 abr. 2022.

198 LEONARDI, Marcel. Marco Civil da Internet e proteção de dados pessoais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**. São Paulo: Quartier Latin, 2015. t. 1: Marco Civil da Internet (Lei n. 12.965/2014). p. 518.

199 MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 201, 2018. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 30 ago. 2022.

pessoais. Schreiber divide a “problemática da privacidade” em duas dimensões: 1) procedimental, preocupada com o modo com os dados são obtidos e tratados; 2) substancial, focada no uso que se faz do dado pessoal. A primeira, tem uma preocupação com o modo como ocorre a coleta dos dados e com a impressão equivocada de que o fornecimento do dado implica em sua alienação. Por outro lado, segundo o autor:

> Para além da dimensão procedimental, vinculada ao tratamento dispensado ao dado pessoal desde sua coleta até a sua eliminação, a privacidade possui uma dimensão substancial, vinculada ao próprio emprego da informação obtida. Toda pessoa tem direito a controlar a representação de si mesma que é construída a partir de seus dados pessoais. É direito de toda pessoa exigir que tal representação reflita a realidade, impedindo que seu uso assuma caráter discriminatório.[200]

Essas dimensões, hoje, são atribuídas ao direito à proteção de dados pessoais. Isso não quer dizer, porém, que a relação do titular com seus dados seja de propriedade. Como explica Menke, a partir das lições do ordenamento alemão:

> [...] o direito da proteção de dados não regula a propriedade, mas sim consiste num ordenamento sobre a informação e a comunicação a eles relacionada, determinando quem, em qual relação, e em que situação, está autorizado a lidar com os modelos de uma determinada pessoa de uma determinada maneira.[201]

O foco da proteção, nesse sentido, está no poder que o indivíduo tem de tomar decisões sobre os dados que dizem respeito a si – a autodeterminação informacional, ou informativa. Ela pode ser definida como “o direito de cada indivíduo poder controlar e determinar (ainda não de modo absoluto) o acesso e o uso de seus dados pessoais”.[202] Esse direito foi inicialmente concebido da noção de dignidade humana, passando pela personalidade, até consolidar-se como direito autônomo.[203] Ele é o

---

[200] SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2011. p. 133.

[201] 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. (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 213.

[202] SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados pessoais. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book* (não paginado).

[203] CUNHA, Anita Spies Da. **O fortalecimento da dimensão objetiva do direito fundamental à proteção de dados como caminho para sua efetividade**. 105 f. Dissertação (Mestrado em Direito) - Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, 2022.

elemento central do direito fundamental à proteção de dados pessoais, embora com ele não se confunda.[204]

Isso porque o direito à proteção de dados pessoais "[...] regula uma ordem de informação e comunicação, que é na sua essência multidimensional, na medida em que busca equilibrar os variados interesses de usos e os direitos de proteção, de defesa e de participação do indivíduo nos processos comunicativos".[205] Assim, o direito à autodeterminação informacional integra seu núcleo, mas a proteção de dados é mais ampla.[206]

Doneda considera adequado falar em um direito à proteção de dados pessoais, porque nessa expressão "[...] podemos depreender a problemática da privacidade e igualmente a da informação, que teria como ponto de referência os direitos da personalidade e estaria isenta de uma acepção patrimonialista ou meramente conceitual, ao mesmo tempo que não remonta ao direito à liberdade em uma acepção demasiado ampla".[207] De maneira semelhante, Sarlet explica que o uso da expressão "autodeterminação informativa" possui limitações e sofre críticas. Nesse sentido, mais adequada a utilização do termo "proteção de dados pessoais" para o direito, que:

> [...] guarda maior sintonia com a ordem jurídico-constitucional brasileira, dando conta, pela sua abrangência, tanto da essencial vinculação de tal proteção com salvaguarda da privacidade e da intimidade (de onde, em termos gerais, foi deduzida a proteção de dados pessoais na seara da jurisprudência e da doutrina), quanto da sua conexão com o direito ao livre desenvolvimento da personalidade.[208]

Após décadas de debate em torno da existência e dos contornos desse direito, em fevereiro de 2022 foi aprovada a Emenda Constitucional (EC) nº 115, que incluiu o inciso LXXIX no artigo 5º da Constituição Federal, que diz que "é assegurado, nos

---

[204] SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados pessoais. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book* (não paginado).

[205] MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 204, 2018. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 30 ago. 2022.

[206] SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados pessoais. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book* (não paginado).

[207] 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, 2020.

[208] SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Saraiva, 2015. p. 465.

termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".[209] Parte-se do pressuposto de que os dados pessoais são projeções da personalidade, influenciando na representação da pessoa na sociedade, com potencial de violação de seus direitos fundamentais. Por isso, de acordo com Mendes:

> O bem jurídico protegido por esse direito é duplo. Ele visa proteger, por um lado, a integridade moral da pessoa, como componente essencial da dignidade humana, e, por outro, as liberdades em sentido amplo (como a liberdade de comunicação, de trabalho, de locomoção, de informação, entre outras).[210]

Ademais, como explicam Cunha e Schiocchet, "[...] o indivíduo intimidado, que não sabe quais informações do Estado detém sobre si, irá evitar certas atitudes, o que implicará diretamente no livre desenvolvimento e a livre expressão de sua personalidade, parte essencial da dignidade humana".[211] Assim, a proteção não diz respeito somente aos dados em si, mas principalmente ao processo de "coleta, armazenamento, utilização ou transferência, a partir do qual são extraídas informações pessoais a serem utilizadas em um determinado contexto para determinados fins".[212]

O direito à proteção de dados pessoais tem dupla dimensão, subjetiva e objetiva, assim como ocorre com outros direitos fundamentais,[213] inclusive o direito à segurança pública. Sob a perspectiva subjetiva, assume caráter defensivo, criando uma "esfera de liberdade individual que não pode sofrer intervenção do poder estatal

---

209 BRASIL. **Constituição Federal**. [Constituição (1988)]. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 ago. 2022.

210 MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 204, 2018. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 30 ago. 2022.

211 CUNHA, Anita Spies da; SCHIOCCHET, Taysa. A constitucionalidade do DNA na persecução penal: o direito à autodeterminação informativa e o critério de proporcionalidade no Brasil e na Alemanha. **Revista de Investigações Constitucionais**, Curitiba, v. 8, p. 529–554, 2021. Disponível em: https://revistas.ufpr.br/rinc/article/view/74420. Acesso em: 30 ago. 2022.

212 MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 204, 2018. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 30 ago. 2022.

213 SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados pessoais. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book* (não paginado).

ou privado".[214] No âmbito objetivo, o direito se configura como um dever de atuação do Estado para sua garantia, mediante prestações de natureza fática ou normativa.[215]

De acordo com Sarlet, o direito à proteção de dados pessoais abarca um conjunto de "posições jurídicas subjetivas", subdivisões de exigências de proteção que podem ser feitas por um indivíduo no âmbito do direito. São elas:

> (a) o direito ao acesso e ao conhecimento dos dados pessoais existentes em registros (bancos de dados) públicos ou privados; (b) o direito ao não conhecimento, tratamento e utilização e difusão de determinados dados pessoais pelo Estado ou por terceiros, aqui incluído um direito de sigilo quanto aos dados pessoais; (c) o direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; (d) o direito ao conhecimento da finalidade da coleta e da eventual utilização dos dados; (e) o direito à retificação e, a depender do caso, à exclusão de dados pessoais armazenados em bancos de dados.[216]

Apesar da ampla proteção, porém, assim como ocorre com outros direitos fundamentais, a proteção de dados pessoais não é um direito absoluto.[217] Comporta limitações e restrições, especialmente quando relacionado às demais garantias constitucionalmente estabelecidas, pois, "[...] todo direito fundamental possui um âmbito de proteção (um campo de incidência normativa ou suporte fático, como preferem outros) e todo direito fundamental, ao menos em princípio, está sujeito a intervenções neste âmbito de proteção".[218] Porém, o ponto decisivo está na medida dessa limitação.

Na teoria do direito constitucional, distinguem-se duas teorias acerca da restringibilidade e limitação[219] dos direitos fundamentais: interna e externa. Para a

---

214 MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 205, 2018. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 30 ago. 2022.

215 SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados pessoais. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book* (não paginado).

216 SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Saraiva, 2015. p. 466.

217 CUNHA, Anita Spies da. **O fortalecimento da dimensão objetiva do direito fundamental à proteção de dados como caminho para sua efetividade**. 105 f. Dissertação (Mestrado em Direito) - Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, 2022.

218 SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Saraiva, 2015. p. 376.

219 Sabe-se da distinção realizada por alguns autores, como Alexy, a respeito da diferença entre restrição e limite dos direitos fundamentais. Entretanto, considerando as traduções e incorporações da teoria no contexto brasileiro, para fins deste trabalho, adota-se o uso de ambos os termos para o fenômeno jurídico aqui abordado, na linha do que faz Sarlet. ALEXY, Robert.

teoria interna, "[...] não existem duas coisas, o direito e suas restrições, mas apenas uma: o direito com um determinado conteúdo",[220] havendo "limites imanentes" a cada direito, que se justificariam:

> [...] em virtude da existência de 'limites originários ou primitivos' que se imporiam a todos os direitos: (i) 'limites constituídos por direitos dos outros'; (ii) limites imanentes da ordem social; (iii) limites eticamente imanentes. Haveria, pois, uma 'cláusula da comunidade' nos termos da qual os direitos, liberdades e garantias estariam sempre 'limitados' desde que colocassem em perigo bens jurídicos necessários à existência da comunidade.[221]

Por outro lado, para a teoria externa, as restrições impostas aos direitos fundamentais com eles não se confundem, destacando-se a relevância da identificação precisa dos contornos de cada direito.[222] Nesse sentido, haveria uma "limitação horizontal", realizada por meio de uma ponderação entre bens jurídico-constitucionais,[223] gerando limitações para um direito fundamental – que, por sua vez, também devem observar outros limites, que tem sido chamados de "limites dos limites".[224] Como explica Sarlet:

> Em virtude de ser pautada pela referida distinção entre posições jurídicas *prima facie* e definitivas, a teoria externa acaba sendo mais apta a propiciar a reconstrução argumentativa das colisões de direitos fundamentais, tendo em conta a necessidade de imposição de limites a tais direitos, para que possa ser assegurada a convivência harmônica entre seus respectivos titulares no âmbito da realidade social.[225]

Ao tratar da limitação dos direitos fundamentais sob a perspectiva da teoria externa, tem-se duas formas de restrição. Por um lado, há mandados e proibições

---

Teoria de los derechos fundamentales. Madrid: Centro de Estudios Constitucionales, 1993. SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2012.

220 Tradução nossa de "[...] no existen dos cosas, el derecho y sus restricciones, sino sólo una: el derecho con un determinado contenido". ALEXY, Robert. **Teoria de los derechos fundamentales**. Madrid: Centro de Estudios Constitucionales, 1993. p. 268–269.

221 CANOTILHO, Joaquim José Gomes. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra: Almedina, 2003. p. 1280.

222 SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2012.

223 CANOTILHO, Joaquim José Gomes. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra: Almedina, 2003.

224 SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2012.

225 SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Saraiva, 2015. p. 378.

dirigidos aos titulares dos direitos. Por outro, existem normas de competência, que delimitam a possibilidade de o Estado, por meio do legislador, restringir direitos fundamentais[226] – também chamadas de reservas legais.[227]

Pode-se afirmar que há uma reserva legal no texto que garante o direito à proteção de dados pessoais na Constituição, quando diz que este é assegurado “nos termos da lei”.[228] Embora não se identifique disposição semelhante no caso do direito à segurança pública, este também se submete a limites, tendo em vista que a ausência de uma norma de competência limitadora não afasta a possibilidade de colisão entre este direito fundamental e outros.[229] De fato, essa colisão, na realidade social, restou evidente na primeira parte dessa pesquisa, verificando-se uma dificuldade em conciliar o direito à proteção de dados pessoais e o direito à garantia da segurança pública.

Nesse contexto, antecipa-se a relevância de uma norma voltada para a proteção de dados pessoais no âmbito da segurança pública – assunto que será mais amplamente abordado no próximo item, quando for analisado o projeto da LGPD penal. Isso porque, por meio da reserva legal, permite-se a imposição, pelo legislador, de limitações à proteção de dados para garantia do interesse público na prevenção e repressão penal. Entretanto, cabe destacar que as restrições também possuem limites – os “limites dos limites”.

Essas limitações à restringibilidade de direitos fundamentais relacionam-se à compatibilidade das restrições, formal e materialmente, à Constituição. Sob a perspectiva formal, observa-se o procedimento, a competência e a forma utilizados pelo Estado para limitar um direito. No âmbito material, o controle constitucional da limitação se dá por meio de atendimento à proporcionalidade e razoabilidade, bem como pelo respeito ao núcleo essencial do direito.[230]

---

[226] ALEXY, Robert. **Teoria de los derechos fundamentales**. Madrid: Centro de Estudios Constitucionales, 1993.

[227] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2012.

[228] BRASIL. **Constituição Federal**. [Constituição (1988)]. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 ago. 2022.

[229] Como também ocorre com os direitos à liberdade de expressão, à intimidade, à vida privada, à honra e à imagem. SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Saraiva, 2015.

[230] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2012.

A proporcionalidade possui dupla função, servindo de proibição ao excesso, mas também à proteção insuficiente. Ela se desdobra em três elementos, apresentados no seguinte quadro:

Quadro 5 – Elementos da proporcionalidade

Adequação ou conformidade	Deve ser possível que os meios escolhidos atinjam os fins a que se propõem alcançar
Necessidade ou exigibilidade	Deve-se optar pela restrição menos gravosa para o direito. Duas etapas: • Verificar a igualdade de adequação dos meios – outros meios promovem o mesmo fim? • Identificar o meio menos restritivo
Proporcionalidade em sentido estrito	Prezar pelo equilíbrio entre os meios e os fins, dentro da razoabilidade

Fonte: elaborado pela autora com base em Sarlet.[231]

Com relação ao núcleo essencial de um determinado direito fundamental, observa-se que não há uma fórmula para sua definição em abstrato e por antecipação.[232] Seria equivocado, nesse sentido, identificar o núcleo inviolável de um direito fundamental com categorias como o mínimo existencial, ou com a medida da influência da dignidade humana sobre o direito em questão.[233]

No caso da proteção de dados pessoais, como explica Mendes, as limitações ao direito fundamental:

> [...] devem ser estabelecidas na legislação e têm de ser precedidas por requisitos de intervenção proporcionais à gravidade da intervenção, além do estabelecimento de medidas de segurança e de organização para a proteção desse direito. Como se percebe, as limitações do direito fundamental à proteção de dados podem se confundir com a própria delimitação do seu âmbito de proteção, tendo em vista a natureza desse direito, que pode ser entendido como um direito em que há necessidade de conformação jurídica.[234]

---

231 SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Saraiva, 2015.

232 SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2012.

233 SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Saraiva, 2015.

234 MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v.

Assim, delimitar o núcleo essencial do direito fundamental à proteção de dados pessoais é tarefa que se confunde com a determinação do que são dados sensíveis, relacionados a aspectos da vida íntima, mais ligados ao âmago da proteção. Por outro lado, há direitos mais distantes desse núcleo, já de certa forma maculados pela publicidade, como o nome, a filiação etc.[235] No tocante ao núcleo essencial do direito à segurança pública, pode-se afirmar que corresponde ao objetivo de garantir a ordem pública – embora essa concepção se mostre demasiadamente ampla, mas restrita pelo dever de respeito às liberdades públicas.

Não se pode esquecer que, no universo de possibilidades de utilização de dados pessoais para finalidade de prevenção e repressão penal, eventual lei pode não dar conta de todos os possíveis desdobramentos. Portanto, a análise de proporcionalidade, bem como a consideração do núcleo essencial dos direitos à proteção de dados e à garantia da segurança pública, enquanto direitos fundamentais conflitantes, são de extrema relevância. Assim, pode-se falar na restrição limitada desses direitos, com garantia da segurança jurídica necessária, mas ser pretensão de esgotamento de todas as possibilidades da prática social.

Atualmente, há alguns dispositivos legais que se aplicam ao uso de dados pessoais para garantia da segurança pública (*lato sensu*). Há, também, um projeto de lei – já apresentado à Câmara dos Deputados – que pretende regular a temática. A questão é em que medida a legislação, vigente e prospectiva, consegue realizar um equilíbrio entre esses direitos fundamentais. É o que se verá no item a seguir.

3.2 A proteção de dados pessoais na esfera penal: legislação vigente e prospectiva aplicável

Considerando a reserva legal relativa ao direito fundamental à proteção de dados, discute-se a regulação do tema. É preciso ter em mente que se trata de matéria em constante modificação, diante dos acelerados avanços tecnológicos. Nesse sentido:

12, n. 39, p. 213, 2018. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 30 ago. 2022.

[235] SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados pessoais. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book* (não paginado).

> Em termos de regulação, discutem-se duas estratégias: uma regulação baseada em regras e uma regulação baseada em princípios. Esta última possibilitaria maior flexibilidade na regulação, correspondendo aos 'programas teleológicos' luhmanianos, em que importa assegurar certos resultados, mas se deixa margem quanto à escolha dos meios. Estamos ao nível de 'tipos-ideais', pelo que, na realidade, confrontamo-nos, não raro, com modelos mistos, sendo certo que a própria densificação de princípios pode levar a níveis de concretização que se aproximam das regras.[236]

Ainda assim, não se pode depender tão somente de princípios para a proteção de um direito fundamental. Como explicam Limberger e Bunchhaft:

> [...] é importante que o mundo virtual tenha sua normatização, sob pena de se transformar em um verdadeiro *far west* informático. Outrossim, o ciberespaço se constitui – ou pode se constituir – um espaço para o exercício dos direitos humanos e para a participação, inspirando o controle social, a partir da informação disponibilizada em rede, de seu acesso e de seu compartilhamento.[237]

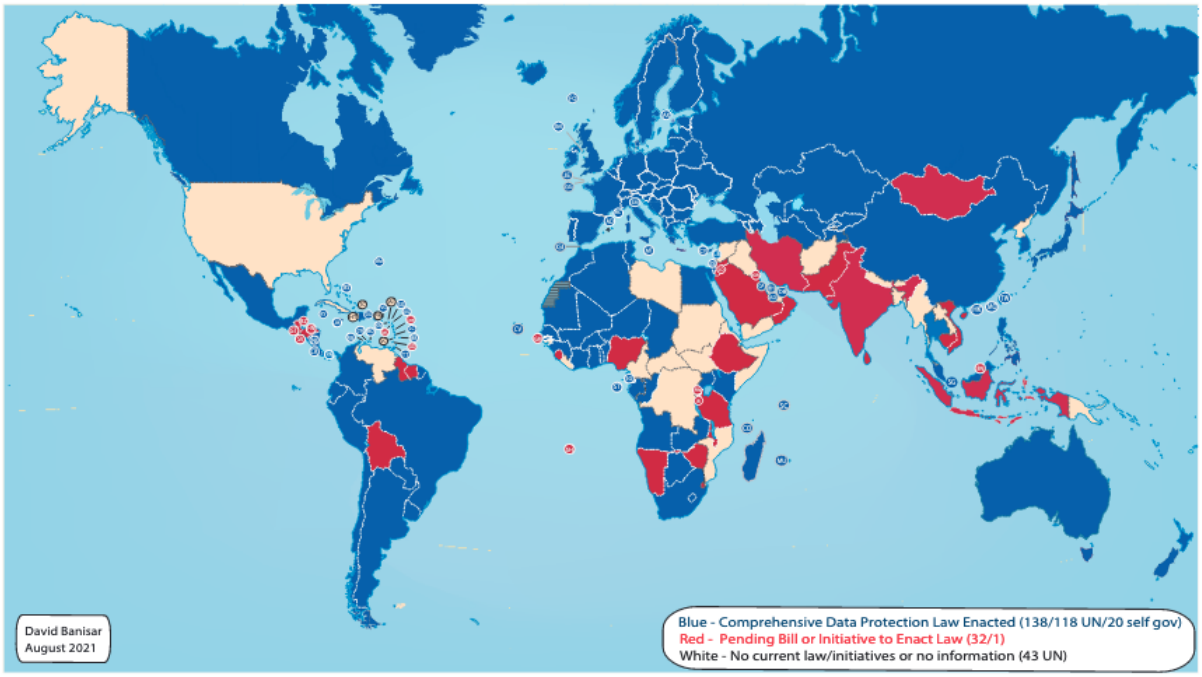
Quando se fala em proteção de dados pessoais, por meio de legislação infraconstitucional, o destaque está nas leis gerais – LGPD no Brasil, GDPR no contexto europeu, especialmente. Em agosto de 2021, aproximadamente 140 países e jurisdições independentes já possuíam leis gerais de proteção de dados ou de privacidade, e outros 30 projetos de leis ou iniciativas pendentes, ou seja, em processo de elaboração. A situação, pelo mundo, pode ser visualizada no mapa:

---

[236] LOUREIRO, João Carlos. Constituição, tecnologia e risco(s): entre medo(s) e esperança(s). *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 68–69.

[237] LIMBERGER, Têmis; BUNCHAFT, Maria Eugenia. Novas tecnologias e direitos humanos: uma reflexão à luz da concepção de esfera pública. **Espaço Jurídico Journal of Law**, [*s. l.*], v. 17, n. 3, p. 864, 2016. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/7578. Acesso em: 30 ago. 2022.

Figura 9 – Mapa da proteção de dados no mundo



Fonte: Banisar.[238]

A doutrina identifica quatro gerações de leis de proteção de dados pessoais, com início na década de 1970, que, segundo Doneda, “partem desde um enfoque mais técnico e restrito até a abertura mais recente a técnicas mais amplas e condizentes com a profundidade da tecnologia adotada para o tratamento de dados, em busca de uma tutela mais eficaz e também vinculando a matéria aos direitos fundamentais”.[239] Desse modo, considerando que a Europa investiu na regulamentação do uso de dados pessoais já muito cedo,[240] o que permitiu com que seu sistema de proteção evoluísse no tempo em prol de uma tutela eficaz e da proteção de direitos humanos. Por isso, é considerada modelo quanto à proteção de dados pessoais para diversos países que buscam a regulamentação do tema.

---

238 BANISAR, David. **National comprehensive data protection/privacy laws and bills 2021**. Rochester: SSRN, 2021. Disponível em: https://papers.ssrn.com/abstract=1951416. Acesso em: 29 ago. 2022.

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

240 Os primeiros documentos que reconheceram a proteção de dados pessoais como direito fundamental no bloco europeu foram o Tratado de Lisboa, que alterou o Tratado a União Europeia e o Tratado que institui a Comunidade Europeia, em 2007, e a Carta dos Direitos Fundamentais da União Europeia, de 2000. UNIÃO EUROPEIA. **Tratado de Lisboa**: que altera o Tratado da União Europeia e o Tratado que Institui a Comunidade Europeia (2007/C 306/01). Lisboa, 2007. Disponível em: http://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0018.02/DOC_19. Acesso em: 18 jul. 2022.

A *General Data Protection Regulation* (GDPR) foi aprovada em 2016 e entrou em vigor em 25 de maio de 2018.[241] Com a finalidade de harmonizar a legislação de proteção de dados nos países da União Europeia, a GDPR serviu de modelo para diversos diplomas legais que a sucederam. É o caso da Lei Geral de Proteção de Dados brasileira (LGPD), Lei nº 13.709/2018, que entrou plenamente em vigor em 1º de agosto de 2021.[242]

Tanto a GDPR quanto a LGPD são focadas na regulação do processamento de dados pessoais coletados, de maneira automatizada ou não, por pessoas de direito público ou privado. Porém, ambas excluem de seu âmbito de aplicação o tratamento de dados realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão penal.[243]

Com relação ao tratamento de dados pessoais por entidades públicas, há previsão expressa no sentido de que a LGPD não se aplica o tratamento de dados realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão penal (artigo 4º).[244] Porém, a Lei traz disposições que se aplicam a essas questões, como é o caso do inciso III do artigo 33, que prevê a transferência internacional de dados pessoais entre órgãos públicos de investigação, inteligência e persecução.

Além disso, a norma também é explícita no sentido de que seus princípios devem ser aplicados à prática de tratamento de dados pelo Estado para garantia da

---

241 UNIÃO EUROPEIA. Parlamento Europeu. Conselho da União Europeia. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT%0A. Acesso em: 18 jul. 2022.

242 A *vacatio legis* era, inicialmente, de 24 meses a partir da publicação da Lei. Entretanto, tal prazo foi estendido pela Lei nº 14.010/2020 e pela Medida Provisória nº 959/2020. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 jul. 2022.

243 UNIÃO EUROPEIA. Parlamento Europeu. Conselho da União Europeia. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT%0A. Acesso em: 18 jul. 2022. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 jul. 2022.

244 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 jul. 2022.

lei. Eles estão previstos no artigo 6º: finalidade; adequação; necessidade; livre acesso; qualidade dos dados, transparência, segurança, prevenção, não discriminação; e responsabilização e prestação de contas.[245]

Desse modo, a LGPD representa importante marco regulatório com relação à proteção de dados pessoais – principalmente em face do tratamento por empresas privadas, mas também pelo uso estatal. O problema é que, mesmo não excluindo totalmente o Estado enquanto controlador, restringe, quase totalmente, sua aplicação quando se trata do problema da segurança pública.

Desse modo, quando se pensa no tratamento de dados pessoais pelo Estado para fins de garantia da segurança pública, porém, não há legislação equivalente à LGPD. Assim, como explica Mendes:

> [...] a LGPD não está apta a proteger o cidadão de outras leis que possam a vir a ser aprovadas pelo Poder Legislativo e que violem a sua privacidade, ao permitir, por exemplo, o processamento de dados abusivos, legitimar práticas de vigilância ou produzir discriminação por meio do processamento de dados. Assim, resta claro que a base legal para o tratamento de dados pessoais, exigido pela LGPD, somente passa a ser um meio para a limitação de abusos, caso a própria base legal fique sob o escrutínio de um direito fundamental à proteção de dados.[246]

Fala-se na necessidade de uma regulação específica desde 2020, tendo sido elaborado anteprojeto de lei[247] com a finalidade de proteção de dados no âmbito da segurança pública.[248] Recentemente, em junho de 2022, foi apresentado o Projeto de Lei (PL) nº 1.515 à Câmara dos Deputados,[249] que possui o texto do anteprojeto como base, mas que trouxe diversas alterações na proposta.

---

245 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 jul. 2022.

246 MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 186, 2018. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 30 ago. 2022.

247 CORDEIRO, Nefi *et al.* **Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal**. Brasília, DF, 2020. Disponível em: https://www.conjur.com.br/dl/anteprojeto-lei-disciplina-protecao.pdf. Acesso em: 28 fev. 2022.

248 COMISSÃO entrega à câmara anteprojeto sobre tratamento de dados pessoais na área criminal. *In*: STJ Notícias, Brasília, DF, 5 nov. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx. Acesso em: 28 fev. 2022.

249 ARMANDO, Coronel. **Projeto de lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de

Ainda na época de apresentação do anteprojeto, Almeida *et al*. Identificavam seis pontos de destaque no texto: 1) o papel do controlador, que é a autoridade que trata os dados; 2) as condições de licitude e legitimidade para o tratamento de dados no âmbito da segurança pública e persecução penal; 3) o sigilo de dados, transparência e acesso à informação, à luz da Diretiva 680/2016 da União Europeia; 4) necessidade de previsão legal específica para uso de tecnologias de monitoramento que limitem direitos, liberdades e garantias, com elevado risco, com exigência de prévio relatório de impacto de vigilância; 5) a transferência internacional de dados; 6) e a autoridade de supervisão do tratamento.[250]

O anteprojeto foi elaborado por uma comissão de juristas composta por grandes pesquisadores contemporâneos da proteção de dados pessoais.[251] Apesar de possuir um texto bastante avançado, aparentemente voltado para a proteção do direito fundamental à proteção de dados, a proposta também recebeu críticas. Nas palavras de Josino:

> No direito público alemão, solidificou-se a necessidade de se proteger a liberdade dos cidadãos e de limitar a atuação do Estado. A partir da correlação entre poder e saber, é essencial que o acesso às informações (o "saber") seja limitado para que não haja abusos de poder. Na finalidade da segurança pública, o estado deve poder saber mais, mas isso por que ele pode atuar menos concretamente contra um indivíduo em específico. Já no setor da persecução penal, em que o estado está autorizado, inclusive, a medidas cautelares pessoais bastante interventivas, concretas e individualizadas contra uma pessoa em especial, o estado deve poder saber menos, por que ele pode mais. Quem tudo sabe, não deve poder tudo; e quem pode quase tudo, não deve saber de tudo. Essa divisão fundante do direito alemão é respirada no anteprojeto, contudo, ela não é levada ao seu termo. Há sempre a identificação de que essa proteção de dados deve ser dar tanto no setor da persecução penal, quanto no da segurança pública, porém não há identificação dos pressupostos autorizativos, que são diversos, para uma ou para outra coleta de dados. Nesse sentido, o projeto está animado por essa distinção fundamental, mas está pendente, ainda, de um aprofundamento quanto a essa questão.

investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 7 jun. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node09wqlrgv9qemi1qa4zbdv699tb12566378.node0?codteor=2182274&filename=Tramitacao-PL+1515/2022. Acesso em: 1 ago. 2022.

250 ALMEIDA, Eloísa Machado de; ESTELLITA, Heloisa (org.). **Dados, privacidade e persecução penal**: cinco estudos. São Paulo: FGV-DIREITO-SP, 2021. *E-book*.

251 COMISSÃO entrega à câmara anteprojeto sobre tratamento de dados pessoais na área criminal. *In*: STJ Notícias, Brasília, DF, 5 nov. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx. Acesso em: 28 fev. 2022.

> O anúncio dessa distinção é importante, mas ele ainda não realiza todos os anseios da reserva de lei no processo penal.[252]

Ocorre que o PL modificou grande parte da proposta do anteprojeto. A comparação completa entre os dois documentos encontra-se no Apêndice A, ao final deste trabalho. Entretanto, alguns pontos merecem destaque, pois permitem a identificação de potenciais desequilíbrios entre a proteção de dados e a garantia da segurança pública. O foco da análise, aqui, estará no PL, que é o texto normativo mais avançado no âmbito da matéria em estudo.

No geral, verifica-se que a redação do PL apresenta diversos problemas, de natureza formal e material. Formalmente, é possível identificar repetições de texto, como no artigo 26, onde se lê que "A prestação de informações e a concessão e acesso a dados pode ser adiada, limitada ou recusada se e enquanto tal for necessário e proporcional para" evitar prejuízo e proteger a defesa nacional duas vezes, nos incisos V e VI.[253] No artigo 28, o §3º há necessidade de observação dos incisos I e II do mesmo artigo – que, de fato, não possui incisos.

O artigo 35 fala em uma "autoridade" competente para dispor sobre o acesso e a guarda dos dados para as finalidades do PL, suprimindo o termo "nacional" que antes acompanhava o anteprojeto (artigo 30) e que determina qual autoridade pode dispor sobre o acesso e tempo de guarda dos dados, gerando ambiguidade. Apesar de ser possível deduzir que a autoridade mencionada se trata da autoridade nacional de proteção de dados, que, de acordo com a LGPD possui a responsabilidade de "zelar, implementar e fiscalizar a proteção de dados em todo o território nacional",[254] mas que foi excluída do rol do artigo 3º do PL, não é difícil confundi-la com a autoridade competente, nos termos do PL:

---

[252] JOSINO, Clarissa Nogueira. **Dados pessoais, segurança pública e investigação criminal**: um panorama da proteção de dados e seus desafios regulatórios no Brasil. 2021. 53 f. Monografia (Graduação em Direito) - Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2021. Disponível em: https://repositorio.ufc.br/handle/riufc/58510. Acesso em: 30 ago. 2022.

[253] ARMANDO, Coronel. **Projeto de lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 7 jun. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node09wqlrgv9qemi1qa4zbdv699tb12566378.node0?codteor=2182274&filename=Tramitacao-PL+1515/2022. Acesso em: 1 ago. 2022.

[254] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Presidência da República: Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jun. 2022.

> autoridade pública, órgão ou entidade do Poder Público responsável pelas atividades de segurança do Estado, de defesa nacional, e pela prevenção, detecção, investigação ou repressão de atos infracionais e infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, ou qualquer outro órgão ou entidade que, nos termos da lei, exerça autoridade ou execute políticas públicas para os referidos efeitos, total ou parcialmente.[255]

Para além das questões formais, no entanto, o que mais chama a atenção são algumas disposições de conteúdo. Já no artigo 1º há um problema. Ele prevê que a LGPD Penal "dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública e de atividades de investigação e repressão de infrações penais".[256] Como visto na primeira parte deste trabalho, é possível a utilização – na prevenção e repressão penal – de dados pessoais coletados e tratados originariamente para outras finalidades, pelo Poder Público ou por particulares. Portanto, a norma já nasceria deficitária.

O primeiro artigo também deixa clara uma ênfase na proteção da segurança, visando assegurar a eficiência dos órgãos que devem garanti-la e permitindo o intercâmbio de dados. A eficiência das atividades de segurança também foi incluída como fundamento da disciplina da proteção de dados pessoais na prevenção e repressão penal (artigo 2º, IV). Ao mesmo tempo, foram removidos dos fundamentos a autodeterminação informacional, a confidencialidade e a integridade dos sistemas informáticos pessoais. Outra demonstração de prevalência da segurança sobre a proteção dos dados é verificável na inclusão, no princípio da finalidade (artigo 4º, II), do objetivo de subsidiar as atividades de segurança pública dos órgãos dela incumbidos.

---

[255] ARMANDO, Coronel. **Projeto de lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 7 jun. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node09wqlrgv9qemi1qa4zbdv699tb12566378.node0?codteor=2182274&filename=Tramitacao-PL+1515/2022. Acesso em: 1 ago. 2022.

[256] ARMANDO, Coronel. **Projeto de lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 7 jun. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node09wqlrgv9qemi1qa4zbdv699tb12566378.node0?codteor=2182274&filename=Tramitacao-PL+1515/2022. Acesso em: 1 ago. 2022.

Na apresentação de conceitos-chave para o processamento de dados na segurança pública no anteprojeto (artigo 5º), tinha-se a noção de dados sigilosos, que não foi incluída no texto do PL (artigo 3º). O mesmo ocorre com o conceito de tecnologia de vigilância. Por outro lado, o PL expande a noção de "atividade de segurança pública", ampliando seu âmbito de proteção, ultrapassado a garantia da ordem pública para alcançar a incolumidade das pessoas e do patrimônio. Além disso, cria o conceito de dados cadastrais, como dados apresentados para fins de cadastro, junto ao Poder Público ou a entidade particular, não sujeitos a sigilo. De acordo com o § 1º, podem ser "[…] referentes à qualificação pessoal, dados biométricos, filiação, endereço, nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão, identificação de usuário ou código de acesso que tenha sido atribuído no momento da conexão".[257]

Nos princípios que devem ser observados no tratamento de dados pessoais para finalidade de exercício de atividades de segurança pública (em sentido amplo), destaca-se que os princípios da proporcionalidade, do livre acesso e da transparência, que constavam no anteprojeto, não foram mencionados no PL. Ademais, coloca como princípio a "supremacia do interesse público: prevalência do interesse público em conflito sobre um interesse particular".[258]

No anteprojeto, estavam incluídas somente as atividades de processamento de dados para fins de garantia da segurança pública e da persecução criminal. O PL ampliou sua aplicação para o uso de dados pessoais para as atividades de inteligência, de segurança do Estado e defesa nacional. Ou seja, em todos estes âmbitos deve prevalecer, indiscriminadamente, o interesse público – consubstanciado na garantia da segurança pública, que, para o PL, diz respeito à manutenção da ordem pública, da incolumidade de pessoas e patrimônio. Nesse sentido, parece violar a

---

[257] ARMANDO, Coronel. **Projeto de lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 7 jun. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node09wqlrgv9qemi1qa4zbdv699tb12566378.node0?codteor=2182274&filename=Tramitacao-PL+1515/2022. Acesso em: 1 ago. 2022.

[258] ARMANDO, Coronel. **Projeto de lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 7 jun. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node09wqlrgv9qemi1qa4zbdv699tb12566378.node0?codteor=2182274&filename=Tramitacao-PL+1515/2022. Acesso em: 1 ago. 2022.

proporcionalidade necessária entre os direitos fundamentais à proteção de dados pessoais e à segurança pública, com uma valorização muito maior do segundo.

Acerca das categorias de titulares dos dados, o anteprojeto (artigo 7º) previa e o PL (artigo 5º) manteve a necessidade de, quando possível, realizar uma distinção entre eles. O problema está na supressão de um termo de um texto para o outro: o anteprojeto fala em pessoas com relação às quais se tem “indícios suficientes” de cometimento de uma infração, passada ou iminente; o PL suprimiu o termo “suficientes”, bastando, nesta proposta, qualquer indício. Nesse ponto, verifica-se um problema com relação ao abuso de poder sobre os dados, também amparado na justificativa de suprir o interesse público de garantia da segurança.

No §2º do artigo 9º do PL, inclui-se a possibilidade de tratamento de dados sensíveis para prevenção e repressão penal quando for necessário para cumprimento de obrigação legal, execução de políticas públicas, proteção da vida ou incolumidade física do titular, de terceiro ou da coletividade, ou, ainda, para resguardar direitos dos titulares. Nesse sentido, não oferece nenhum tipo de salvaguarda especial aos dados sensíveis, facilitando que a Administração Pública os utilize – embora sejam o núcleo central do direito fundamental à proteção de dados pessoais.

De acordo com o artigo 10º do PL, dados anonimizados não são considerados dados pessoais. Isso é um problema porque, como visto, no contexto atual, é possível combinar dados, que deixam de ser anonimizados e permitem a extração de informações relativas às pessoas. Além disso, o artigo 16 do anteprojeto previa o descarte imediato dos dados quando constatadas a obtenção e o tratamento de dados excessivos ou irrelevantes – determinação de exclusão que foi suprimida no PL.

Todo esse cenário, de prevalência do suposto interesse público na segurança, que tem seu âmbito essencial de aplicação ilegitimamente ampliado pelo PL, é agravado pela possibilidade de compartilhamento dos dados. O artigo 13 permite a troca de dados controlados pela Administração Pública com pessoas jurídicas de direito privado, como medida excepcional, mas com base tão somente em razões de interesse público motivadas em ato administrativo. Não esclarece, no entanto, quais seriam os requisitos e os limites dessa motivação – que, na verdade, por ser colocada na esfera das decisões da administração, sujeitam-se a um certo grau de discricionariedade.

Ademais, o artigo 17 do anteprojeto restringia a guarda de dados que já se terminou de tratar ao cumprimento de obrigação ou para uso por órgãos de pesquisa.

No artigo 22 do PL, esta última ressalva foi substituída pela genérica autorização de compartilhamento dos dados com “terceiros”.

Quanto aos direitos do titular dos dados, o anteprojeto previa que qualquer restrição a eles deveria ser limitada no tempo (artigo 19). O PL retirou essa limitação temporal (artigo 23). Aliás, os direitos reconhecidos – em ambas as propostas – são: liberdade, intimidade e privacidade. Não há menção a um direito fundamental à proteção de dados, o que era de se esperar ao menos na proposta do PL, que é posterior ao reconhecimento constitucional explícito do direito.

O anteprojeto previa, dentre os direitos específicos dos titulares dos dados no âmbito de proteção da norma, as possibilidades de anonimização, bloqueio ou eliminação de dados excessivos, desnecessários ou tratados de forma ilegal, bem como o direito de informação a respeito das entidades públicas e privadas com as quais os dados foram compartilhados (artigo 20). O PL não abordou essas possibilidades.

O PL também é problemático porquanto retira a possibilidade de uso dos registros cronológicos de uso dos dados para exercício do poder disciplinar. Com isso, fragiliza a possibilidade de responsabilização administrativa por consulta e divulgação ilegal de dados. Ademais, reduz o prazo mínimo de manutenção desses registros de 5 anos para 6 meses.

O anteprojeto previa expressamente a necessidade de documentação das transferências internacionais de dados. No §2º do artigo 52, lia-se que deveriam ser feitos registros “sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos”.[259] Isso foi cortado do texto do PL. O mesmo ocorre com os §§ 2º e 3º do artigo 54 do anteprojeto.

Há diversos outros pontos que poderiam ser abordados a respeito da proposta do PL. Entretanto, cabe observar que se trata de projeto recentemente apresentado, que ainda não passou pelas comissões da Câmara e ainda não sofreu as modificações que certamente receberá. Por enquanto, é relevante destacar que a forma como se pretende regular a temática da proteção de dados pessoais no seu

[259] ARMANDO, Coronel. **Projeto de lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 7 jun. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node09wqlrgv9qemi1qa4zbdv699tb12566378.node0?codteor=2182274&filename=Tramitacao-PL+1515/2022. Acesso em: 1 ago. 2022.

uso para garantia da segurança pública (*lato sensu*) valoriza muito pouco o direito fundamental à proteção de dados, priorizando o suposto interesse público à segurança pública – sem, de fato, atentar-se ao conteúdo deste último, que visa a ordem pública, mas com respeito às demais garantias e liberdades fundamentais.

Enquanto não se tem uma lei geral relativa ao uso de dados pessoais na segurança pública, já se veem outras normas que tratam dessa possibilidade. É o caso do Decreto nº 10.046/2019,[260] que visa a criação de um Cadastro Base do Cidadão e a possibilidade de compartilhamento de dados entre órgãos públicos. Nesse Cadastro, o Decreto prevê a inclusão de atributos biográficos, biométricos e genéticos, que assim define:

> Art. 2º Para fins deste Decreto, considera-se:
> I - atributos biográficos - dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios;
> II - atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar; [...]
> IV - atributos genéticos - características hereditárias da pessoa natural, obtidas pela análise de ácidos nucleicos ou por outras análises científicas; [...][261]

Destaca-se a possibilidade de tratamento de dados relacionados não apenas ao registro civil, havendo uma ampliação muito grande para a coleta de registros dos olhos, da voz e até mesmo maneira de andar. Todos esses dados poderão ser compartilhados "[...] entre os órgãos e as entidades da administração pública federal direta, autárquica e fundacional e os demais Poderes da União" (artigo 1º).[262] Com esse tratamento massivo e com o compartilhamento facilitado, o Decreto cria possibilidades de potencializar ações de vigilância tecnológica.[263]

---

[260] BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Brasília, DF: Presidência da República, 9 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 28 fev. 2022.

[261] BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Brasília, DF: Presidência da República, 9 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 28 fev. 2022.

[262] BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Brasília, DF: Presidência da República, 9 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 28 fev. 2022.

[263] Justamente diante da ameaça à proteção de dados pessoais a OAB ingressou com Ação Direta de Inconstitucionalidade (ADI nº 6.649) no Supremo Tribunal Federal, questionando a

O chamado Pacote Anticrime (Lei nº 13.964/2019) modificou a Lei de Identificação Criminal (nº 12.037/2009), autorizando a criação de um Banco Nacional Multibiométrico e de Impressões Digitais. O objetivo desse banco é de "armazenar dados de registros biométricos, de impressões digitais e, quando possível, de íris, face e voz, para subsidiar investigações criminais federais, estaduais ou distritais" (§2º do artigo 7º-C).[264]

O artigo que o prevê possui 11 parágrafos, que são toda a regulação a respeito do tema. O único indício de preocupação com a proteção de dados pessoais, embora não explicitamente nestes termos, está no §8º, que diz que os dados terão caráter sigiloso. Ainda assim, não há uma clara delimitação a respeito do uso desses dados, mais uma vez ficando evidente um desequilíbrio em que pondera uma justificativa de garantia da segurança.

Inclusive, a LGPD prevê a possibilidade de processamento de dados biométricos para identificação e autenticação[265] no artigo 11, inciso II, alínea "g", com a observação de que não podem ser utilizados quando prevalecer o direito à proteção de dados do titular.[266] Porém, diante da exclusão do processamento de dados para garantia da segurança pública do âmbito de proteção da LGPD, há uma identificação entre a prática e a norma, mas não se pode dizer que ela é plenamente aplicável

---

constitucionalidade do Decreto. GROSSMANN, Luís Osvaldo. **Governo revoga compartilhamento de dados entre Serpro e Abin**. *In*: CONVERGÊNCIA Digital, [*s. l.*], 25 jun. 2020. Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=54011&sid=18. Acesso em: 28 fev. 2022.

264 BRASIL. **Lei nº 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. Brasília, DF: Presidência da República, 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12037.htm. Acesso em: 30 ago. 2022.

265 De acordo com Colombo e Goulart: "[...] os efeitos ou objetivos específicos a serem alcançados, na biometria são: 'identificação, verificação/autenticação ou categorização'. Na 'identificação biométrica' comparam-se os dados biométricos de uma pessoa (quando da inscrição) com 'um determinado número de modelos armazenados na base de dados', é o que se denomina de 'um para muitos'. Na 'autenticação', compara-se os dados de uma única pessoa com um único modelo no dispositivo. E, por último, na 'categorização/separação', o essencial não é a sua identificação, mas classificar a pessoa em um determinado grupo. Por exemplo, separar entre homens e mulheres, crianças e adultos". COLOMBO, Cristiano; GOULART, Guilherme Damasio. Novo perímetro do corpo e a biometria como dado pessoal: princípios da finalidade e da necessidade aplicados e recomendações para o caso do metrô de São Paulo. *In*: COLOMBO, Cristiano; ENGELMANN, Wilson; FALEIROS JÚNIOR, José Luiz de Moura (org.). **Tutela jurídica do corpo eletrônico**: novos desafios ao direito digital. Indaiatuba: Foco, 2022. p. 431.

266 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 ago. 2022.

nesses casos. Mais uma vez, verifica-se a importância de uma lei geral de proteção voltada especificamente para a área criminal.

Não se poderia deixar de mencionar, ainda com relação às normas que autorizam a coleta e tratamento de dados para garantia de segurança pública, a Lei nº 12.654/2012, que criou os bancos de perfis genéticos para fins de persecução penal, também por meio de uma alteração na Lei de Identificação Criminal. O uso de material genético para criação de perfis das pessoas possui diversos desdobramentos e tem recebido críticas desde antes da aprovação da lei.[267] Conforme explicam Cunha e Schiocchet:

> No Brasil, a implementação e regulação do uso de DNA para fins de persecução penal teve como pano de fundo legitimador esse argumento de combate à criminalidade, influenciado pelo "efeito CSI", que, inserido em uma ainda incipiente cultura de proteção de dados, como é a brasileira, levou à aprovação da Lei 12.654/12, que, com apenas quatro artigos, passou a permitir a coleta, manutenção e utilização de dados genéticos para fins de persecução penal, sem regular adequadamente seu funcionamento, sendo omissa em vários aspectos. Como consequência, exatamente 4 anos depois de sua promulgação, a Lei teve sua constitucionalidade questionada, e atualmente o Recurso Extraordinário (RE) nº 973.837/MG está concluso para julgamento, com a repercussão geral reconhecida (Tema 905 - Constitucionalidade da inclusão e manutenção de perfil genético de condenados por crimes violentos ou por crimes hediondos em banco de dados estatal).[268]

Atualmente, com o reconhecimento de um direito fundamental à proteção de dados pessoais, tem-se mais um direito individual em risco com o uso de perfis genéticos para persecução criminal. Nesse sentido, a criação de uma lei geral de proteção de dados na esfera da segurança pública pode afetar, também, a identificação genética nesse âmbito.

---

[267] Não é objetivo deste trabalho aprofundar a polêmica da utilização de DNA para fins de persecução penal. Recomenda-se a leitura, dentre outros, de: SCHIOCCHET, Taysa (org.). **Bancos de perfis genéticos para fins de persecução criminal**. Brasília, DF: Ministério da Justiça, 2012. (Série Pensando o Direito, v. 43).*E-book*. SCHIOCCHET, Taysa; CUNHA, Anita Spies da; LAZZARETTI, Bianca Kaini. Bancos de perfis genéticos para fins de persecução criminal: implicações jurídicas à privacidade, intimidade e estigmatização genéticas. *In*: REUNIÃO DE ANTROPOLOGIA DA CIÊNCIA E DA TECNOLOGIA, 5., Porto Alegre. **Direitos e Ciências interfaces entre saberes especializados**. Porto Alegre: REACT, 2015. Disponível em: https://ocs.ige.unicamp.br/ojs/react/article/view/1355. Acesso em: 29 ago. 2022.

[268] CUNHA, Anita Spies da; SCHIOCCHET, Taysa. A constitucionalidade do DNA na persecução penal: o direito à autodeterminação informativa e o critério de proporcionalidade no Brasil e na Alemanha. **Revista de Investigações Constitucionais**, Curitiba, v. 8, p. 532, 2021. Disponível em: https://revistas.ufpr.br/rinc/article/view/74420. Acesso em: 30 ago. 2022.

Por fim, destaca-se que a compatibilização entre um direito fundamental à proteção de dados pessoais e àquele que garante a segurança pública é medida necessária, também, para que se atinjam os Objetivos do Desenvolvimento Sustentável, traçados pela Organização das Nações Unidas. Trata-se de uma questão de sustentabilidade.

Frequentemente associado a questões de Direito Ambiental, eis que é nessa área que se concentram os maiores riscos à vida futura digna na Terra, o princípio da sustentabilidade é, na realidade, mais amplo e precisa ser aplicado também a outras áreas do Direito. Nas palavras de Freitas, a sustentabilidade, em nível constitucional:

> [...] determina, com eficácia direta e imediata, a responsabilidade do Estado e da sociedade pela concretização solidária do desenvolvimento material e imaterial, socialmente inclusivo, durável e equânime, ambientalmente limpo, inovador, ético e eficiente, no intuito de assegurar, preferencialmente de modo preventivo e precavido, no presente e no futuro, o direito ao bem-estar.[269]

Como se vê em sua definição, a sustentabilidade traduz-se em princípio que orienta o Direito para o futuro, com a finalidade de garantir o bem-estar do ser humano no planeta em diversas áreas. Assim, é possível afirmar que se pretende um desenvolvimento sustentável nas áreas ambiental, econômica, social e tantas outras.

Nesse espírito, desde o ano 2000 a Organização das Nações Unidas (ONU) vem traçando recomendações para que o desenvolvimento nesses diversos setores seja realizado de maneira sustentável em um nível internacional. Naquele ano, foram lançados os oito Objetivos de Desenvolvimento do Milênio, com 21 metas a serem buscadas pelos 191 Estados membros da ONU na época.[270]

Posteriormente, em setembro de 2015, os 193 países da ONU adotaram uma nova programação para os próximos 15 anos: a Agenda 2030, que conta com 17 Objetivos de Desenvolvimento Sustentável (ODS), especificados em 169 metas.[271] Os Objetivos da Agenda 2030 são os seguintes:

---

[269] FREITAS, Juarez. Sustentabilidade: conceito. *In*: FREITAS, Juarez. **Sustentabilidade**: direito ao futuro. 3. ed. Belo Horizonte: Fórum, 2016. p. 43.

[270] CAL, Carla Monteaperto. Histórico ODM. *In*: SECRETARIA DE GOVERNO DA PRESIDÊNCIA DA REPÚBLICA. **Objetivos de Desenvolvimento Sustentável**: ODS. [*S. l.*], 16 dez. 2019. Disponível em: http://www4.planalto.gov.br/ods/assuntos/copy_of_historico-odm. Acesso em: 15 ago. 2022.

[271] CAL, Carla Monteaperto. Histórico ODM. *In*: SECRETARIA DE GOVERNO DA PRESIDÊNCIA DA REPÚBLICA. **Objetivos de Desenvolvimento Sustentável**: ODS. [*S. l.*], 16 dez. 2019. Disponível em: http://www4.planalto.gov.br/ods/assuntos/copy_of_historico-odm. Acesso em: 15 ago. 2021.

> Objetivo 1. Acabar com a pobreza em todas as suas formas, em todos os lugares; Objetivo 2. Acabar com a fome, alcançar a segurança alimentar e melhoria da nutrição e promover a agricultura sustentável; Objetivo 3. Assegurar uma vida saudável e promover o bem-estar para todos, em todas as idades; Objetivo 4. Assegurar a educação inclusiva e equitativa de qualidade, e promover oportunidades de aprendizagem ao longo da vida para todos; Objetivo 5. Alcançar a igualdade de gênero e empoderar todas as mulheres e meninas; Objetivo 6. Assegurar a disponibilidade e gestão sustentável da água e saneamento para todos; Objetivo 7. Assegurar o acesso confiável, sustentável, moderno e a preço acessível à energia para todos; Objetivo 8. Promover o crescimento econômico sustentado, inclusivo e sustentável, emprego pleno e produtivo e trabalho decente para todos; Objetivo 9. Construir infraestruturas robustas, promover a industrialização inclusiva e sustentável e fomentar a inovação; Objetivo 10. Reduzir a desigualdade dentro dos países e entre eles; Objetivo 11. Tornar as cidades e os assentamentos humanos inclusivos, seguros, resistentes e sustentáveis; Objetivo 12. Assegurar padrões de produção e de consumo sustentáveis; Objetivo 13. Tomar medidas urgentes para combater a mudança do clima e seus impactos; Objetivo 14. Conservar e usar sustentavelmente dos oceanos, dos mares e dos recursos marinhos para o desenvolvimento sustentável; Objetivo 15. Proteger, recuperar e promover o uso sustentável dos ecossistemas terrestres, gerir de forma sustentável as florestas, combater a desertificação, deter e reverter a degradação da terra e deter a perda de biodiversidade; Objetivo 16. Promover sociedades pacíficas e inclusivas para o desenvolvimento sustentável, proporcionar o acesso à justiça para todos e construir instituições eficazes, responsáveis e inclusivas em todos os níveis; Objetivo 17. Fortalecer os meios de implementação e revitalizar a parceria global para o desenvolvimento sustentável.[272]

Além das metas globais estabelecidas na Agenda 2030, espera-se que os países que a adotaram fixem metas nacionais e indicadores próprios para avaliação de seu progresso.[273] Assim, trata-se de verdadeiro compromisso voltado para a efetivação de mudanças necessárias para o alcance de um futuro sustentável.

Ao pensar os impactos da vigilância penal tecnológica no futuro da vida em sociedade, questiona-se em que medida essa prática pode contribuir ou atrapalhar um desenvolvimento sustentável. Nesse sentido, verifica-se que pelo menos dois ODS

---

[272] ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Transformando nosso mundo**: a Agenda 2030 para o Desenvolvimento Sustentável. Rio de Janeiro: Centro de Informação das Nações Unidas para o Brasil, 2015. Disponível em: http://www.itamaraty.gov.br/images/ed_desenvsust/Agenda2030-completo-site.pdf. Acesso em: 13 ago. 2022. p. 15.

[273] INDICADORES brasileiros para os Objetivos de Desenvolvimento Sustentável. *In*: INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE); SECRETARIA ESPECIAL DE ARTICULAÇÃO SOCIAL. **Objetivos de Desenvolvimento Sustentável**. [*S. l.*], 2021. Disponível em: https://odsbrasil.gov.br/home/agenda. Acesso em: 13 ago. 2022.

da Agenda 2030 são alcançados por ações como as narradas no capítulo anterior deste artigo: o ODS 10 e o ODS 16.

O ODS 10, focado na redução das desigualdades dentro dos países e entre eles. Ele inclui metas globais que visam: aumento da renda da população; inclusão independente de idade, gênero, deficiência, raça, etnia, origem, religião, condição econômica etc.; eliminação de normas e políticas discriminatórias; adoção de políticas sociais em busca da igualdade; regulamentação de mercados financeiros; aumento do protagonismo de países em desenvolvimento nas instituições econômicas globais; implementação de políticas migratórias adequadas.

Com relação a práticas de tecnovigilância, a meta que é mais potencialmente afetada é a 10.3, descrita no seguinte enunciado: "Garantir a igualdade de oportunidades e reduzir as desigualdades de resultados, inclusive por meio da eliminação de leis, políticas e práticas discriminatórias e da promoção de legislação, políticas e ações adequadas a este respeito".[274] Isso porque, como visto anteriormente, já é possível verificar usos da tecnologia que se tenta incorporar em leis e em políticas públicas que abrem margem para um aumento da discriminação, especialmente racial.

Além disso, o último Relatório Luz acerca da Agenda 2030 no Brasil indica – sem considerar os impactos de novas tecnologias expressamente – que essa meta está em retrocesso. Há uma grande dificuldade em obter dados sobre violência contra grupos vulneráveis (com relação à discriminação) junto a órgãos públicos. Inclusive, uma das recomendações do Relatório acerca do ODS 10 diz respeito à necessidade de "Garantir a produção de dados públicos em direitos humanos e disponibilizá-los".[275] Justamente a falta de informações e transparência sobre o uso de dados dos cidadãos para garantia da segurança pública é um dos problemas que já pôde ser verificado na prática, principalmente no tocante à população negra.[276]

---

[274] ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Redução das desigualdades. *In*: NAÇÕES Unidas Brasil. Brasília, DF, c2021. Disponível em: https://brasil.un.org/pt-br/sdgs/10. Acesso em: 23 ago. 2022.

[275] GRUPO DE TRABALHO DA SOCIEDADE CIVIL PARA A AGENDA 2030. **VI Relatório Luz da Sociedade Civil Agenda 2030 de Desenvolvimento Sustentável Brasil**. [*S. l.: s. n.*], 2022. Disponível em: https://brasilnaagenda2030.files.wordpress.com/2022/07/pt_rl_2022_final_web-1.pdf. Acesso em: 19 ago. 2022. p. 63.

[276] REDE DE OBSERVATÓRIOS DA SEGURANÇA. **Retratos da violência: cinco meses de monitoramento, análises e descobertas**. [*S. l.*]: CESEC, 2019. Disponível em: http://observatorioseguranca.com.br/wp-content/uploads/2019/11/1relatoriorede.pdf. Acesso em: 2 fev. 2022.

Outro Objetivo potencialmente afetado por práticas de tecnovigilância é o ODS 16, que busca a paz, a justiça e instituições eficazes. Dentre suas metas, estão: a redução da violência; proteção das crianças em face de abusos e violências de diversas naturezas; promoção do Estado de Direito e do acesso à justiça; combate ao crime organizado; redução da corrupção; desenvolvimento de instituições eficazes, responsáveis e transparentes; aumento da representatividade na tomada de decisões; fortalecimento de países em desenvolvimento em instituições globais; identificação populacional integral; garantia de acesso à informação pública; fortalecimento de instituições para combate ao crime; promoção de políticas não discriminatórias.[277] São diversas as metas impactadas pela tecnovigilância nesse ODS.

A primeira é a meta 16.3, que busca "Promover o Estado de Direito, em nível nacional e internacional, e garantir a igualdade de acesso à justiça para todos". A meta 16.b, que diz que se objetiva "Promover e fazer cumprir leis e políticas não discriminatórias para o desenvolvimento sustentável" é afetada de maneira semelhante.[278] Como visto, o uso de tecnologias de vigilância pode aprofundar a desigualdade e a discriminação na justiça brasileira.

Ademais, com práticas como a coleta irrestrita de dados, cria-se um desequilíbrio informacional que aumenta o poder estatal e pode impactar negativamente no que se espera do Estado de Direito. Como aponta o Relatório Luz de 2021:

> [...] diminuíram a transparência e circulação de informações públicas, com o aparelho estatal sendo usado contra pessoas que criticam o governo. [...] As informações sobre ações de promoção do estado de direito e garantia de igualdade de acesso à justiça são escassas e não há previsão sobre a realização de pesquisas nacionais para superar essa lacuna. Os últimos dados sobre a proporção de vítimas de violência no país que reportaram às autoridades competentes ou a outros organismos de resolução de conflitos são de 2010 e a realização de novos levantamentos pelo IBGE está indefinida pelos

[277] ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Paz, Justiça e Instituições Eficazes. *In*: NAÇÕES Unidas Brasil. Brasília, DF, c2021. Disponível em: https://brasil.un.org/pt-br/sdgs/16. Acesso em: 23 ago. 2022.

[278] ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Paz, Justiça e Instituições Eficazes. *In*: NAÇÕES Unidas Brasil. Brasília, DF, c2021. Disponível em: https://brasil.un.org/pt-br/sdgs/16. Acesso em: 23 ago. 2022.

> cortes de orçamento. Também os dados do INFOPEN atual sofreram alterações significativas pelo atual governo.[279]

Também nesse sentido é o risco à meta 16.6, que prevê "Desenvolver instituições eficazes, responsáveis e transparentes em todos os níveis".[280] A coleta de dados muitas vezes é realizada sem a devida transparência acerca dos meios e finalidades, além de ser feita de maneira irresponsável, sem nenhuma prévia previsão legal – especialmente no tocante aos atores envolvidos, as técnicas utilizadas etc.

Além dessas, a meta 16.10 também está especialmente ameaçada. Ela diz que é necessário "Assegurar o acesso público à informação e proteger as liberdades fundamentais, em conformidade com a legislação nacional e os acordos internacionais". Retoma-se o problema de acesso à informação, já mencionado acima.

Por fim, a meta 16.a merece especial atenção. Ela dispõe que é necessário:

> Fortalecer as instituições nacionais relevantes, inclusive por meio da cooperação internacional, para a construção de capacidades em todos os níveis, em particular nos países em desenvolvimento, para a prevenção da violência e o combate ao terrorismo e ao crime.[281]

A grande dificuldade está em como fortalecer as instituições para o combate à violência e ao crime sem permitir que sejam violados direitos fundamentais. As tecnologias que oferecem novas ferramentas a essas instituições muitas vezes são adotadas sem uma preocupação com esses direitos, focando tão somente nos possíveis benefícios. Para que essa meta seja alcançada sem prejuízo às demais, é necessário que se regule propriamente as inovações tecnológicas aplicadas à garantia da segurança pública, sem permitir que a esperança de um processo penal efetivo obscureça o potencial totalitário e discriminatório da vigilância.

---

[279] GRUPO DE TRABALHO DA SOCIEDADE CIVIL PARA A AGENDA 2030. **V Relatório Luz da Sociedade Civil**: Agenda 2030 de Desenvolvimento Sustentável Brasil. [*S. l.*]: GTSC A2030, 2021. p. 94.

[280] ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Paz, Justiça e Instituições Eficazes. *In*: NAÇÕES Unidas Brasil. Brasília, DF, c2021. Disponível em: https://brasil.un.org/pt-br/sdgs/16. Acesso em: 23 ago. 2022.

[281] ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Paz, Justiça e Instituições Eficazes. *In*: NAÇÕES Unidas Brasil. Brasília, DF, c2021. Disponível em: https://brasil.un.org/pt-br/sdgs/16. Acesso em: 23 ago. 2022.

4 CONSIDERAÇÕES FINAIS

No mundo hiperconectado contemporâneo, marcado pelos impactos da Quarta Revolução Industrial, a extração e circulação de dados pessoais adquiriu caráter massivo como nunca visto. Esse contexto de expansão do tratamento de dados gera crescente preocupação no mundo jurídico, assim como outros debates travados na seara das relações entre Direito e tecnologia. São diversos os fatores que despertam atenção na temática, destacando-se os atores envolvidos, os potenciais usos e a agilidade com que a tecnologia avança e se difunde.

Este trabalho abordou a utilização de dados pessoais para a garantia da segurança pública em sentido amplo. Essa concepção abrange a prevenção (segurança pública em sentido estrito), a repressão penal (investigação e persecução), as atividades de defesa nacional (essencialmente militares) e de segurança do Estado (relacionadas às ações de inteligência). Em todos estes espaços, o uso de dados pessoais não tem regulação, visto que o artigo 4º, III, da LGPD – que é a lei geral de proteção a esses dados no país – expressamente os exclui de seu âmbito de aplicação.

A análise foi dividida em duas partes, consistentes nos capítulos 2 e 3 da dissertação. A primeira parte, de caráter exploratório, pretendeu apresentar os contornos da problemática sob uma perspectiva transdisciplinar. Assim, no item 2.1 explicou-se o que são, afinal, dados pessoais, elencando seus tipos. Observou-se a massificação da coleta de dados, mediada pela Internet das coisas. Diferenciou-se dados de informações, conceituando, também, os dados pessoais sensíveis.

No mesmo tópico, abordou-se o tratamento de dados. A esse respeito, mencionaram-se a importância dos algoritmos, que utilizam inteligência artificial e suas evoluções – como o *machine learning* e o *deep learning* – no processamento de dados pessoais. Também se abordou o conceito e os atributos do *Big Data*, destacando o grande volume de dados tratados no contexto atual e como isso pode ser feito sob um ponto de vista técnico. Tratou-se do *Big Data Analytics*, distinguindo as análises descritiva, preditiva e prescritiva. Apresentou-se exemplos de utilização de inteligência artificial no setor público, dentre os quais se encontra o processamento para fins de garantia da segurança pública.

No item 2.2, realizou-se a investigação sobre as práticas sociais de uso de dados pessoais para prevenção e repressão penal, sem pretensão de exaurir todas

as possibilidades, mas para compreender os riscos e benefícios relacionados. Para isso, delimitou-se a noção de segurança em sentido amplo. Em seguida, apresentou-se a classificação dos dados colhidos: (a) por órgãos estatais, (a.1) originalmente coletados para atividades de segurança ou (a.2) para finalidades diversas; e (b) obtidos por entidades privadas, com (b.1) finalidade originária de garantia da segurança (pública ou privada), ou (b.2) para outros fins. Além disso, foram fornecidos exemplos de meios de coleta de dados em todas estas possibilidades.

Em seguida, foram trabalhados alguns casos relacionados ao tratamento de dados pessoais na segurança pública (*lato sensu*), indicando as promessas de benefícios e os desdobramentos negativos das práticas. Tratou-se do espelhamento da tela do *WhatsApp Web* pela polícia para monitoramento das comunicações de um suspeito; do caso Marielle Franco, em que foram requisitadas informações de acesso à Internet de pessoas que realizaram determinadas pesquisas em período anterior ao crime, bem como dados de geolocalização; da revogação da decisão *Roe vs. Wade* nos Estados Unidos, que já se antecipa ter impactos na proteção de dados sensíveis; do caso *Snowden*, em que foi denunciado o monitoramento massivo de comunicações em diversos países pelo governo norte-americano; do monitoramento, pela ABIN, de redes sociais pelo Governo Federal brasileiro; do acordo de cooperação da mesma agência de inteligência com a Serpro para acesso a dados pessoais de condutores no país; da Medida Provisória que garantia, ao IBGE, acesso a dados de usuários de telecomunicações; do caso da Boate Kiss, em que houve acesso a dados de apenados e pessoas com quem tiveram contato; do reconhecimento facial; da criação de equipamentos de vigilância baseados em Internet das coisas; das previsões policiais da Geolitica; e das *risk assessment practices*.

Verificou-se que essas práticas raramente apresentam resultados que comprovem efetivos benefícios à garantia da segurança pública, visto que dificilmente a eficácia das medidas vem desacompanhada de ameaça a algum direito fundamental. Em suma, esses casos deixam evidente uma série de problemas relacionados à presunção de inocência, à responsabilização pelo tratamento dos dados, à privacidade, ao consentimento para o tratamento de dados, à proporcionalidade das medidas, ao compartilhamento indiscriminado de dados entre entidades governamentais, à paridade de armas no processo penal, a presença de vieses algorítmicos, a imprecisão dos resultados apurados pelas tecnologias preditivas, à transparência e muitos outros.

O que se identifica, na verdade, é uma celebração da técnica e da tecnologia enquanto soluções para a satisfação de “necessidades privatizadas”. A utilização de novas tecnologias no contexto da garantia da segurança pública frequentemente está acompanhada da falácia de neutralidade dos recursos técnicos. Porém, se o mero uso dessas ferramentas já modifica o ser humano e a vida em sociedade, a utilização inadequada tem potencial devastador. Constata-se, portanto, o papel do Estado como garantidor de uma evolução sustentável, com a imposição de normas constitucionais e infraconstitucionais de proteção. É sobre esse ponto que versa a segunda parte do trabalho.

No item 3.1, apresentaram-se dois direitos fundamentais que são o centro da questão abordada neste trabalho: a proteção de dados pessoais e a segurança pública. Começando pelo segundo, explicou-se que a noção de segurança, na Constituição brasileira, é polissêmica. É utilizada com relação à seguridade social, às garantias processuais, à segurança alimentar... No preâmbulo, consta como valor supremo; no artigo 5º, caracteriza-se como direito individual, corolário de diversas outras perspectivas de segurança (do domicílio e das relações jurídicas, por exemplo).

É nos artigos 6º e 144 que se tem a noção de segurança pública invocada como bem a ser protegido nas práticas de utilização de dados pessoais, que se identifica como um direito social de natureza difusa e que visa à manutenção da ordem pública. Observou-se que é indispensável que a realização desse direito fundamental deve respeitar o espaço de aplicação de outros direitos da mesma natureza, servindo como dever de concretização, mas também como limitação às atividades do Estado.

Há uma dificuldade de efetivação desse direito fundamental, relacionada às crises do Estado, que fazem surgir novas formas de violência, a sensação de impunidade e o medo da comunidade social. Isso desencadeia um processo de expansão do penalismo, com o direcionamento para um direito penal do inimigo. Por sua vez, esses fenômenos são o contexto propício para a busca cada vez maior de recursos que punam mais, que possam identificar culpados a qualquer custo.

Por isso, em seguida, abordou-se o direito fundamental à proteção de dados pessoais, previsto no inciso LXXIX do artigo 5º da Constituição, pois eles são cada vez mais utilizados para finalidade de garantia da segurança pública – como demonstrado na primeira parte da dissertação. Verificou-se que tal direito surge da noção de privacidade, passando pela construção daquilo que se chama de autodeterminação informacional e que hoje é o núcleo de sua proteção. Nesse

sentido, pode-se concluir que o direito à proteção de dados pessoais resguarda a autodeterminação informativa, mas também a privacidade, a intimidade e o livre desenvolvimento da personalidade.

Apontou-se que nenhum direito fundamental é absoluto, não sendo possível um deles ser aplicado com prejuízo aos demais. Em situações de colisão entre direitos dessa natureza, é possível que um se restrinja para que outro prevaleça. Porém, esses limites que vão ser impostos a um determinado direito fundamental também possuem restrições, os “limites dos limites”, nomeadamente: proporcionalidade e respeito ao núcleo essencial do direito.

Da análise do conteúdo dos direitos fundamentais em estudo, conclui-se que o núcleo essencial da proteção de dados pessoais é a salvaguarda dos dados sensíveis. Por outro lado, o cerne da garantia da segurança pública é a manutenção da ordem pública. Na ponderação entre qual deve prevalecer quando se fala no uso de dados para finalidades de repressão e prevenção penal, é preciso considerar que o acesso aos dados não pode ser irrestrito e sobretudo não pode ser justificado pela manutenção da ordem quando for possível realizar o objetivo da segurança pública por meios menos gravosos.

Tendo essa concepção como base, no último item do trabalho (3.2) descreveu-se a proposta de regulação infraconstitucional da problemática. Destacou-se o papel das leis gerais de proteção de dados e as iniciativas legislativas no âmbito penal, especialmente o anteprojeto elaborado por comissão de juristas designada pela Câmara dos Deputados em 2020 e o PL nº 1.515, de 2022, apresentado à mesma casa legislativa.

Verificou-se que o anteprojeto já sofria algumas críticas, especialmente com relação ao papel do controlador dos dados, ao sigilo e à transparência, às condições de licitude e legitimidade do tratamento de dados, o tratamento de dados “de elevado risco”, a transferência internacional e autoridade de supervisão do processamento dos dados. Realizando uma análise comparativa entre as duas propostas, verificou-se que o PL é bastante problemático.

Retoma-se, aqui, o problema de pesquisa que esta dissertação pretendeu responder: em que medida a proposta da LGPD penal (Projeto de Lei nº 1.515 de 2022) limita e garante o direito fundamental à proteção de dados pessoais dentro do contexto da garantia da segurança pública em sentido amplo? Conclui-se que o PL limita em excesso o direito fundamental à proteção de dados pessoais, com uma

supervalorização da garantia da segurança pública. O texto examinado busca, em última análise, legitimar práticas de vigilância tecnológica e de utilização de dados pessoais – inclusive sensíveis – como promessa não apenas de proteção da ordem pública, núcleo central do direito à segurança, mas ampliando para a incolumidade física de indivíduos ou proteção de outros direitos dos titulares.

Outras normas, já vigentes, que tratam do uso de dados pessoais no âmbito penal não oferecem perspectiva mais animadora: a Lei de Identificação Criminal permite o uso de dados sensíveis, com pouquíssimas disposições sobre a proteção desses dados. Nesse sentido, tem-se um cenário de poucos avanços e de alguns retrocessos na concretização das metas traçadas pela comunidade global, e ratificadas pelo Brasil, como é o caso dos Objetivos do Desenvolvimento Sustentável.

REFERÊNCIAS

“BIG BROTHER Rio”: reconhecimento facial usado no carnaval será ampliado. *In*: TILT Uol. [*S. l.*], 30 mar. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/03/30/big-brother-rio-reconhecimento-facial-usado-no-carnaval-sera-ampliado.htm. Acesso em: 19 ago. 2022.

22 ESTADOS dos EUA devem banir aborto com revisão de Roe vs Wade. *In*: PODER 360. [*S. l.*], 25 jun. 2022. Disponível em: https://www.poder360.com.br/internacional/22-estados-dos-eua-devem-banir-aborto-com-revisao-de-roe-vs-wade/. Acesso em: 21 ago. 2022.

ABIN monta rede para monitorar internet. *In:* ÉPOCA Negócios, São Paulo, 14 jul. 2013. Disponível em: https://epocanegocios.globo.com/Informacao/Acao/noticia/2013/06/abin-monta-rede-para-monitorar-internet.html. Acesso em: 18 ago. 2022.

ABREU, Jacqueline de Souza. Tratamento de dados pessoais para segurança pública: contornos do regime jurídico pós-LGPD. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book*.

ABRUSIO, Juliana *et al.* Dados de geolocalização e a investigação do caso Marielle. **Consultor Jurídico**, São Paulo, 7 jul. 2020. Disponível em: https://www.conjur.com.br/2020-jul-07/direito-digital-dados-geolocalizacao-investigacao-marielle. Acesso em: 31 jul. 2022.

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA (ABIN). **Atividade de inteligência no Brasil**. Brasília, DF: ABIN, 2020. v. 5: Cadernos de legislação da ABIN. *E-book*.

ALEXY, Robert. **Teoria de los derechos fundamentales**. Madrid: Centro de Estudios Constitucionales, 1993.

ALMEIDA, Eloísa Machado de; ESTELLITA, Heloisa (org.). **Dados, privacidade e persecução penal**: cinco estudos. São Paulo: FGV-DIREITO-SP, 2021. *E-book*.

ALMEIDA, Guilherme Alberto Almeida de; MENEZES, José Henrique Videira. Inteligência artificial e inovação no setor público. *In*: VAINZOF, Rony; GUTIERREZ, Andriei (org.). **Inteligência artificial**: sociedade, economia e Estado. São Paulo: Thomson Reuters Brasil, 2021. p. 569–602.

ANGWIN, Julia. **Dragnet nation**: a quest for privacy, security, and freedom in a world of relentless surveillance. New York: Times Books, Henry Holt and Company, 2014. *E-book* (não paginado).

ANTEPROJETO de lei disciplina proteção de dados em investigações criminais. **Consultor Jurídico**, São Paulo, 31 out. 2020. Disponível em: https://www.conjur.com.br/2020-out-31/anteprojeto-disciplina-protecao-dados-investigacoes-criminais. Acesso em: 28 fev. 2022.

ANTHES, Emily. The race to create “insect cyborgs”. **The Observer**, [*s. l.*], 17 fev. 2013. Science. Disponível em: https://www.theguardian.com/science/2013/feb/17/race-to-create-insect-cyborgs. Acesso em: 12 ago. 2022.

ARCENO, Taynara Silva. **Inteligência artificial no Tribunal de Justiça do Rio Grande do Sul**: desafios e possibilidades no atual estado da arte. 155 f. Dissertação (Mestrado em Direito) - Universidade do Vale do Rio dos Sinos, São Leopoldo, 2021. Disponível em: http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/9861/Taynara%20Silva%20Arceno_.pdf?sequence=1&isAllowed=y. Acesso em: 12 ago. 2022.

AREOSA, João. A globalização dos riscos sociais e os acidentes tecnológicos. **Pensamiento Americano**, Barranquilla, v. 9, n. 17, p. 151-176, jul./dez. 2016.

ARMANDO, Coronel. **Projeto de lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 7 jun. 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node09wqlrgv9qemi1qa4zbdv699tb12566378.node0?codteor=2182274&filename=Tramitacao-PL+1515/2022. Acesso em: 1 ago. 2022.

AVELINE, Paulo Vieira. **Segurança pública como direito fundamental**. Dissertação (Mestrado em Direito) - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2009. Disponível em: https://tede2.pucrs.br/tede2/handle/tede/4073. Acesso em: 1 ago. 2022.

AZEVEDO, Rodrigo Ghiringhelli de; BASSO, Maura. Segurança pública e direitos fundamentais. **Direito e Justiça**, Porto Alegre, v. 34, n. 2, p. 21–32, 2008.

AZEVEDO, Rodrigo Ghiringhelli. Tendências do controle penal na época contemporânea: reformas penais no Brasil e na Argentina. **São Paulo em Perspectiva**, São Paulo, v. 18, n. 1, p. 39–48, 2004.

BACKYARD BRAINS. **The RoboRoach Bundle**. Ann Arbor: Backyard Brains, [2022?]. Disponível em: https://backyardbrains.com/products/roboroach. Acesso em: 19 ago. 2022.

BANISAR, David. **National comprehensive data protection/privacy laws and bills 2021**. Rochester: SSRN, 2021. Disponível em: https://papers.ssrn.com/abstract=1951416. Acesso em: 29 ago. 2022.

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Zahar, 2001.

BENBOUZID, Bilel. To predict and to manage: predictive policing in the United States. **Big Data & Society**, [*s. l.*], v. 6, n. 1, 2019. Disponível em: https://journals.sagepub.com/doi/pdf/10.1177/2053951719861703. Acesso em: 30 ago. 2022.

BEZERRA, Arthur Coelho. Privacidade como ameaça à segurança pública: uma história de empreendedorismo moral. **Liinc em Revista**, Rio de Janeiro, v. 12, n. 2,

p. 231–242, 2016. Disponível em: https://revista.ibict.br/liinc/article/view/3720. Acesso em: 30 ago. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BOEING, Daniel Henrique Arruda; ROSA, Alexandre Morais da. **Ensinando um robô a julgar**: pragmática, discricionariedade e vieses no uso de aprendizado de máquina no Judiciário. Florianópolis: Emais, 2020.

BRAGA, Carolina. Discriminação nas decisões por algoritmos: polícia preditiva. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito**: ética, regulação e responsabilidade. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 671–696.

BRASIL. **Constituição Federal**. [Constituição (1988)]. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 7 ago. 2022.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Brasília, DF: Presidência da República, 9 out. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 28 fev. 2022.

BRASIL. **Decreto nº 8.793, de 29 de junho de 2016**. Fixa a Política Nacional de Inteligência. Brasília, DF: Presidência da República, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Decreto/D8793.htm. Acesso em: 18 ago. 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Presidência da República: Brasília, DF. Disponível em: http:// www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm. Acesso em: 11 abr. 2022.

BRASIL. **Lei nº 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. Brasília, DF: Presidência da República, 2009. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2009/Lei/L12037.htm. Acesso em: 30 ago. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 ago. 2022.

BRASIL. **Medida Provisória nº 954, de 17 de abril de 2020**. Dispõe 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, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: Presidência da República, 2020. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 18 ago. 2022.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Recurso em Habeas Corpus nº 99.735 Santa Catarina**. Recurso ordinário em habeas corpus. Penal e processo penal. Tráfico de drogas e associação ao tráfico. Autorização judicial de espelhamento, via whatsapp web, das conversas realizadas pelo investigado com terceiros. [...]. Recorrentes: A C DA C, D C DA C. Recorrido: Ministério Público do Estado de Santa Catarina. Relatora: Ministra Laurita Vaz, 27 de novembro de 2018. Disponível em: https://cutt.ly/YcmT6m3. Acesso em: 3 abr. 2022.

BUONAMICI, Sergio Claro. Direito fundamental social à segurança pública. **Revista de Estudos Jurídicos da UNESP**, [*s. l.*], v. 15, n. 21, 2011. Disponível em: https://doi.org/10.22171/rej.v15i21.341. Acesso em: 1 ago. 2022.

BUY IPHONE 13. *In*: APPLE, [*S. l.*, 2022?]. Disponível em: https://www.apple.com/shop/buy-iphone/iphone-13. Acesso em: 13 ago. 2022.

CABRAL, José Santos. Do direito à segurança à segurança do direito. **Julgar**, Lisboa, 2012. Disponível em: http://julgar.pt/wp-content/uploads/2014/07/JOS%C3%89SANTOSCABRAL-DODIREITO%C3%80SEGURAN%C3%87A%C3%80SEGURAN%C3%87ADODIREITO.pdf. Acesso em: 7 ago. 2022.

CAL, Carla Monteaperto. Histórico ODM. *In*: SECRETARIA DE GOVERNO DA PRESIDÊNCIA DA REPÚBLICA. **Objetivos de Desenvolvimento Sustentável**: ODS. [*S. l.*], 16 dez. 2019. Disponível em: http://www4.planalto.gov.br/ods/assuntos/copy_of_historico-odm. Acesso em: 15 ago. 2022.

CALLEGARI, André Luís; MOTTA, Cristina Reindolff da. Estado e política criminal: a expansão do direito penal como forma simbólica de controle social. *In*: CALLEGARI, André Luís (org.). **Política criminal, Estado e democracia**: homenagem aos 40 anos do curso de Direito e aos 10 anos do curso de pós-graduação em Direito da Unisinos. Rio de Janeiro: Lumen Juris, 2007. p. 1-22.

CANOTILHO, Joaquim José Gomes. **Direito constitucional e teoria da constituição**. 7. ed. Coimbra: Almedina, 2003.

CANTARINI, Paola. Marco legal da IA (PL 21/20): análise comparativa à luz da regulamentação europeia (AI Act) e a questão da proteção do segredo industrial. *In*: COLOMBO, Cristiano; ENGELMANN, Wilson; FALEIROS JÚNIOR, José Luiz de Moura (org.). **Tutela jurídica do corpo eletrônico**: novos desafios ao direito digital. Indaiatuba: Foco, 2022. p. 703–722.

CISCO. **Cisco global cloud index**: forcast and methodology, 2016-2021. San Jose: Cisco Systems, 2018. Disponível em: https://virtualization.network/Resources/Whitepapers/0b75cf2e-0c53-4891-918e-b542a5d364c5_white-paper-c11-738085.pdf. Acesso em: 13 ago. 2022.

COMISSÃO entrega à câmara anteprojeto sobre tratamento de dados pessoais na área criminal. *In*: STJ Notícias, Brasília, DF, 5 nov. 2020. Disponível em:

https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx. Acesso em: 28 fev. 2022.

COPACABANA e Maracanã ganham sistema de câmeras de reconhecimento facial. *In*: SEGURANÇA Eletrônica. [*S. l.,* 2017c]. Disponível em: https://revistasegurancaeletronica.com.br/copacabana-e-maracana-ganham-sistema-de-cameras-de-reconhecimento-facial/. Acesso em: 22 nov. 2021.

CORDEIRO, Nefi *et al.* **Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal**. Brasília, DF, 2020. Disponível em: https://www.conjur.com.br/dl/anteprojeto-lei-disciplina-protecao.pdf. Acesso em: 28 fev. 2022.

CUNHA, Anita Spies da; SCHIOCCHET, Taysa. A constitucionalidade do DNA na persecução penal: o direito à autodeterminação informativa e o critério de proporcionalidade no Brasil e na Alemanha. **Revista de Investigações Constitucionais**, Curitiba, v. 8, p. 529–554, 2021. Disponível em: https://revistas.ufpr.br/rinc/article/view/74420. Acesso em: 30 ago. 2022.

CUNHA, Anita Spies da. **O fortalecimento da dimensão objetiva do direito fundamental à proteção de dados como caminho para sua efetividade**. 105 f. Dissertação (Mestrado em Direito) - Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, 2022.

DIAS, Manuel Domingos Antunes. **Liberdade, cidadania e segurança**. Coimbra: Almedina, 2001.

DIAS, Tatiana; MARTINS, Rafael Moro Martins. Documentos vazados mostram que Abin pediu ao Serpro dados e fotos de todas as CNHs do país. *In*: THE INTERCEPT, [*s. l.*], 6 jun. 2020. Disponível em: https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/. Acesso em: 28 fev. 2022.

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

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, 2020.

DONEDA, Danilo. Prefácio. *In*: COLOMBO, Cristiano; ENGELMANN, Wilson; FALEIROS JÚNIOR, José Luiz de Moura (org.). **Tutela jurídica do corpo eletrônico**: novos desafios ao direito digital. Indaiatuba: Foco, 2022. p. IX–XI.

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC). **Liberty at risk, pre-trial risk assessment tools in the U.S**. Washington, DC: EPIC, 2021. Disponível em: https://archive.epic.org/LibertyAtRiskReport.pdf. Acesso em: 16 jun. 2022.

ENGELMANN, Wilson; FRÖHLICH, Afonso Vinício Kirschner. Inteligência artificial aplicada à decisão judicial: o papel dos algoritmos no processo de tomada de decisão. **Revista Jurídica**, Blumenau, v. 24, n. 54, e8274, mai./ago. 2020.

Disponível em: https://proxy.furb.br/ojs/index.php/juridica/issue/view/474. Acesso em: 9 jan. 2022.

ERTHAL, Carolina Naciff de Andrade. **A segurança pública como direito fundamental e como tarefa estatal na Constituição brasileira de 1988**. 228 f. Dissertação (Mestrado em Direito e Ciência Jurídica) - Universidade de Lisboa, Lisboa, 2020. Disponível em: https://repositorio.ul.pt/bitstream/10451/48042/1/ulfd145961_tese.pdf. Acesso em: 6 ago. 2022.

FERGUSON, Andrew G. **The rise of big data policing**: surveillance, race, and the future of law enforcement. New York: New York University Press, 2017. *E-book*.

FLO. **Política de privacidade**. [*S. l.*]: Flo, 6 out. 2020. Disponível em: https://flo.health/pt/politica-de-privacidade. Acesso em: 21 ago. 2022.

FLORIDI, Luciano. Semantic Conceptions of Information. *In*: ZALTA, Edward (ed.). **The Stanford Encyclopedia of Philosophy**. [Stanford: Stanford University], Winter 2019. Disponível em: https://plato.stanford.edu/entries/information-semantic/. Acesso em: 15 jun. 2022.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. 27. ed. [*S. l.*]: Petrópolis, 1987.

FREITAS, Juarez. Sustentabilidade: conceito. *In*: FREITAS, Juarez. **Sustentabilidade**: direito ao futuro. 3. ed. Belo Horizonte: Fórum, 2016.

GABRIEL, Markus. **O sentido do pensar**: a filosofia desafia a inteligência artificial. Petrópolis: Vozes, 2021.

GABRIEL, Martha. **Você, eu e os robôs**: pequeno manual do mundo digital. São Paulo: Atlas, 2018.

GALIMBERTI, Umberto. O ser humano na era da técnica. **Cadernos IHU Ideais**, São Leopoldo, v. 13, n. 218, 2015.

GALIMBERTI, Umberto. **Psiche e techne: o homem na idade da técnica**. São Paulo: Paulus, 2006.

GEOLITICA. **Company**. Santa Cruz: Geolitica, [2022?]. Disponível em: https://geolitica.com/company/. Acesso em: 21 ago. 2022.

GEOLITICA. **Using Geolitica to implement DDACTS**. Santa Cruz: Geolitica, [2022?]. Disponível em: https://geolitica.com/blog/using-geolitica-to-implement-ddacts/. Acesso em: 21 ago. 2022.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2018. *E-book* (não paginado). Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597012934/cfi/6/10!/4/8@0:53.2. Acesso em: 25 jul. 2022.

GROSSMANN, Luís Osvaldo. **Governo revoga compartilhamento de dados entre**

Serpro e Abin. *In*: CONVERGÊNCIA Digital, [*s. l.*], 25 jun. 2020. Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=54011&sid=18. Acesso em: 28 fev. 2022.

GRUPO DE TRABALHO DA SOCIEDADE CIVIL PARA A AGENDA 2030. **V Relatório Luz da Sociedade Civil**: Agenda 2030 de Desenvolvimento Sustentável Brasil. [*S. l.*]: GTSC A2030, 2021.

GRUPO DE TRABALHO DA SOCIEDADE CIVIL PARA A AGENDA 2030. **VI Relatório Luz da Sociedade Civil Agenda 2030 de Desenvolvimento Sustentável Brasil**. [*S. l.: s. n.*], 2022. Disponível em: https://brasilnaagenda2030.files.wordpress.com/2022/07/pt_rl_2022_final_web-1.pdf. Acesso em: 19 ago. 2022.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Tereza Fonseca; NICÁCIO, Camila Silva. **(Re)pensando a pesquisa jurídica**: teoria e prática. 5. ed. rev., ampl. atual. São Paulo: Almedina, 2020.

HABERMAS, Jürgen. **Técnica e ciência como "ideologia"**. 1. ed. Lisboa: Edições 70, 2011.

HAN, Byung-Chul. **Sociedade da transparência**. Petrópolis: Vozes, 2017.

HOFFMANN-RIEM, Wolfgang. **Teoria geral do direito digital**: transformação digital: desafios para o direito. Rio de Janeiro: Forense, 2021.

HOHENDORFF, Raquel von. **A contribuição do *safe by design* na estruturação autorregulatória da gestão dos riscos nanotecnológicos**: lidando com a improbabilidade da comunicação inter-sistêmica entre o direito e a ciência em busca de mecanismos para concretar os objetivos de sustentabilidade do milênio. 478 p. Tese (Doutorado em Direito) – Universidade do Vale do Rio dos Sinos. Programa de Pós-Graduação em Direito, São Leopoldo, 2018. p. 28-29. Disponível em: http://www.repositorio.jesuita.org.br/handle/UNISINOS/7055. Acesso em: 22 jul. 2022.

HOHENDORFF, Raquel Von. Revolução nanotecnológica, riscos e reflexos no Direito: os aportes necessários da Transdisciplinaridade. *In*: ENGELMANN, Wilson; WITTMANN, Cristian (org.). **Direitos humanos e novas tecnologias**. Jundiaí: Paco Editorial, 2015. p. 9–48.

INDICADORES brasileiros para os Objetivos de Desenvolvimento Sustentável. *In*: INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE); SECRETARIA ESPECIAL DE ARTICULAÇÃO SOCIAL. **Objetivos de Desenvolvimento Sustentável**. [*S. l.*], 2021. Disponível em: https://odsbrasil.gov.br/home/agenda. Acesso em: 13 ago. 2022.

INSTITUTO IGARAPÉ. Reconhecimento facial no Brasil. *In*: INSTITUTO Igarapé. [Rio de Janeiro], 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 12 jul. 2022.

INTELIGÊNCIA artificial vai agilizar a tramitação de processos no STF. *In*: SUPREMO TRIBUNAL FEDERAL (STF). **Notícias STF**. Brasília, DF, 30 maio 2018.

Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=380038. Acesso em: 9 jan. 2022.

JOH, Elizabeth E. The new surveillance discretion: automated suspicion, big data, and policing symposium: policing in America on the 50th anniversary of Miranda v. Arizona. **Harvard Law & Policy Review**, [*s. l.*], v. 10, n. 1, p. 15–42, 2016.

JOSINO, Clarissa Nogueira. **Dados pessoais, segurança pública e investigação criminal**: um panorama da proteção de dados e seus desafios regulatórios no Brasil. 2021. 53 f. Monografia (Graduação em Direito) - Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2021. Disponível em: https://repositorio.ufc.br/handle/riufc/58510. Acesso em: 30 ago. 2022.

JÚRI DA Boate Kiss é anulado pelo Tribunal de Justiça do RS. *In*: DIÁRIO Catarinense, [*s. l.*], 3 ago. 2022. Disponível em: https://www.nsctotal.com.br/noticias/juri-da-boate-kiss-e-anulado-pelo-tribunal-de-justica-do-rs. Acesso em: 19 ago. 2022.

KIRA, Beatriz; TAMBELLI, Clarice Nassar. **Data protection in Brazil**: critical analysis of the Brazilian legislation. São Paulo: InternetLab, 2016. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2017/03/Legal-Framework-Analysis-Brazil.pdf. Acesso em: 20 out. 2022.

KORN, Jennifer; DUFFY, Clare. Como dados pessoais podem ser usados para fazer cumprir leis antiaborto nos EUA. *In:* CNN Brasil, Nova Iorque, 25 jun. 2022. Disponível em: https://www.cnnbrasil.com.br/tecnologia/como-dados-pessoais-podem-ser-usados-para-fazer-cumprir-leis-antiaborto-nos-eua/. Acesso em: 21 ago. 2022.

LAZZARETTI, Bianca Kaini; FORTIN, Eleonora Jotz Pacheco. O espelhamento via *WhatsApp Web* e direitos fundamentais em risco: como a licitude da prova é justificada nos tribunais. *In*: ENCONTRO VIRTUAL DO CONPEDI, 3., 2021, Florianópolis. **Direito penal, processo penal e constituição II**. Florianópolis: CONPEDI, 2021. Disponível em: http://site.conpedi.org.br/publicacoes/276gsltp/3b53n985/9dZHOuAi3hOVaDy7.pdf. Acesso em: 22 jun. 2022.

LAZZARETTI, Bianca Kaini; HOHENDORFF, Raquel Von. O uso de inteligência artificial na tomada de decisões judiciais: uma análise sob a perspectiva da Crítica Hermenêutica do Direito. **RDUno**: Revista do Programa de Pós-Graduação em Direito da Unochapecó, Chapecó, v. 3, n. 4, p. 15–32, 2021. Disponível em: https://bit.ly/3Q0D3d1. Acesso em: 29 ago. 2022.

LAZZARINI, Álvaro. Limites do poder de polícia. **Revista de Direito Administrativo**, Rio de Janeiro, v. 198, p. 69–83, 1994. Disponível em: https://bibliotecadigital.fgv.br/ojs/index.php/rda/article/view/46412. Acesso em: 28 ago. 2022.

LEE, Kai-Fu; QIUFAN, Chen. **2041**: como a inteligência artificial vai mudar sua vida nas próximas décadas. Rio de Janeiro: Globo Livros, 2022.

LEONARDI, Marcel. Marco Civil da Internet e proteção de dados pessoais. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (Coord.). **Direito & Internet III**. São Paulo: Quartier Latin, 2015. t. 1: Marco Civil da Internet (Lei n. 12.965/2014). p. 517-538.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

LIMBERGER, Têmis; BUNCHAFT, Maria Eugenia. Novas tecnologias e direitos humanos: uma reflexão à luz da concepção de esfera pública. **Espaço Jurídico Journal of Law**, [*s. l.*], v. 17, n. 3, p. 843–868, 2016. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/7578. Acesso em: 30 ago. 2022.

LINDOSO, Maria Cristine Branco. **Discriminação de gênero no tratamento automatizado de dados pessoais**: como a automatização incorpora vieses de gênero e perpetua a discriminação de mulheres. Rio de Janeiro: Processo, 2021. *E-book*.

LOPES JÚNIOR, Aury. **Direito processual penal**. 19. ed. São Paulo: Saraiva Jur, 2022. *E-book*.

LOUREIRO, João Carlos. Constituição, tecnologia e risco(s): entre medo(s) e esperança(s). *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 33–84.

LOUREIRO, Maria Fernanda Battaglin; CARNEIRO, João Víctor Vieira. Problematizando o direito à privacidade e à proteção de dados pessoais em face da vigilância biométrica. **Teknokultura**: Revista de Cultura Digital y Movimientos Sociales, Madrid, v. 17, n. 2, p. 204–213, 2020. Disponível em: https://revistas.ucm.es/index.php/TEKN/article/view/69479. Acesso em: 30 ago. 2022.

LYON, David. **El ojo electrónico**: el auge de la sociedad de la vigilancia. Madrid: Alianza, 1995.

MAGRANI, Eduardo. **Entre dados e robôs**: ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MAGRANI, Eduardo. **Internet das coisas**. Rio de Janeiro: FGV, 2018. *E-book*.

MARGETH, Ana Lara; CARNEIRO, Giovana. Caminhos para a proteção de dados pessoais na segurança pública e investigação criminal: lições do Seminário Internacional da Comissão de Juristas. *In*: ITS Rio, [*s. l.*], 11 ago. 2020. Disponível em: https://bit.ly/3dX6n6P. Acesso em: 4 ago. 2022.

MEDINA, José Miguel Garcia; MARTINS, João Paulo Nery dos Passos. A era da inteligência artificial: as máquinas poderão tomar decisões judiciais? **Revista dos Tribunais**, [*s. l.*], v. 1020/2020, p. 1-22, out. 2020. Disponível em: https://cutt.ly/0knyKSP. Acesso em: 15 jan. 2022.

MELO, Pedro Raphael Vieira. **Reconhecimento facial automatizado para fins de**

segurança pública e seus riscos aos titulares dos dados biométricos. 31 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Instituto Brasileiro de Ensino Desenvolvimento e Pesquisa (IDP), Brasília, DF, 2020. Disponível em: https://repositorio.idp.edu.br//handle/123456789/3523. Acesso em: 26 jul. 2022.

MENDES, Gilmar Ferreira; PINHEIRO, Jurandi Borges. Interceptações e privacidade: novas tecnologias e a Constituição. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 231–250.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados de uma mesma moeda. **Revista Brasileira de Direitos Fundamentais & Justiça**, Belo Horizonte, v. 12, n. 39, p. 185–216, 2018. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/655. Acesso em: 30 ago. 2022.

MENEZES NETO, Elias Jacob de; MORAIS, Jose Luis Bolzan de; BEZERRA, Tiago José de Souza Lima. O projeto de lei de proteção de dados pessoais (PL 5276/2016) no mundo do big data: o fenômeno da dataveillance em relação à utilização de metadados e seu impacto nos direitos humanos. **Revista Brasileira de Políticas Públicas**, Brasília, DF, v. 7, n. 3, p. 184–198, 2017. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/4840. Acesso em: 30 ago. 2022.

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. (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 205–230.

MININI, Édis; DONATO, Roberto dos Santos. O exercício do poder de polícia, pela Polícia Militar, como instrumento de proteção e promoção dos direitos humanos, à luz da Constituição Federal de 1988. *In*: GORCZEVSKI, Clovis; LEAL, Mônia larissa Heninng (org.). **Constitucionalismo contemporâneo: novos desafios**. Curitiba: Multideia, 2012. p. 263–285.

MISURACA, Gianluca; NOORDT, Colin van. **AI watch**: artificial Intelligence in public services: overview of the use and impact of AI in public services in the EU: Science for Policy Report. Luxembourg: European Commission, 2020. Disponível em: https://bit.ly/3TsZ6vV. Acesso em: 14 ago. 2022.

MOLINARO, Carlos Alberto; SARLET, Ingo Wolfgang. Apontamentos sobre direito, ciência e tecnologia na perspectiva de políticas públicas sobre regulação em ciência e tecnologia. *In*: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (org.). **Direito, inovação e tecnologia**. São Paulo: Saraiva, 2015. p. 85–122.

MORAIS, José Luis Bolzan de. Estado, função social e (os obstáculos da) violência. Ou: do “mal-estar” na civilização à síndrome do medo da barbárie! *In*: CALLEGARI, André Luís (org.). **Política criminal, Estado e democracia**: homenagem aos 40 anos do curso de Direito e aos 10 anos do curso de pós-graduação em Direito da Unisinos. Rio de Janeiro: Lumen Juris, 2007. p. 69–80.

MP QUE obrigava operadoras a compartilhar dados com o IBGE perde validade. *In*: CÂMARA dos Deputados, Brasília, DF, 18 ago. 2020. Disponível em: https://www.camara.leg.br/noticias/685115-mp-que-obrigava-operadoras-a-compartilhar-dados-com-o-ibge-perde-validade/. Acesso em: 18 ago. 2022.

NASCIMENTO, Heloisa Kreutz do. **O que são Atos no SAJ Tribunais?** *In*: QUÍRON. [*S. l.*], 22 jan. 2021. Disponível em: https://quiron.softplan.com.br/hc/pt-br/articles/360016031993-O-que-s%C3%A3o-Atos-no-SAJ-Tribunais-. Acesso em: 3 fev. 2022.

NUNES, Pablo. Novas ferramentas, velhas práticas: reconhecimento facial e policiamento no Brasil. *In*: REDE OBSERVATÓRIOS DA SEGURANÇA. **Retratos da violência**: cinco meses de monitoramento, análises e descobertas. [*S. l.*]: CESEC, 2019.

O'NEIL, Cathy. **Algoritmos de destruição em massa**. 1. ed. Santo André: Rua do Sabão, 2020.

OECD. **Exploring the economics of personal data**: a survey of methodologies for measuring monetary value: OECD Digital Economy Papers. [*S. l.*]: OECD, 2013. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en. Acesso em: 13 ago. 2022.

OLIVEIRA, Débora Martins. **A (in) constitucionalidade das prisões por reconhecimento facial via câmeras de vídeo**: conflito entre o direito à privacidade e o direito à segurança pública? 30 f. Trabalho de Conclusão de Curso (Graduação em Direito) - Faculdade Três Pontas - Grupo UNIS, Três Pontas, 2020. Disponível em: http://repositorio.unis.edu.br/handle/prefix/1767. Acesso em: 27 jul. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Paz, Justiça e Instituições Eficazes. *In*: NAÇÕES Unidas Brasil. Brasília, DF, c2021. Disponível em: https://brasil.un.org/pt-br/sdgs/16. Acesso em: 23 ago. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Redução das desigualdades. *In*: NAÇÕES Unidas Brasil. Brasília, DF, c2021. Disponível em: https://brasil.un.org/pt-br/sdgs/10. Acesso em: 23 ago. 2022.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Transformando nosso mundo**: a Agenda 2030 para o Desenvolvimento Sustentável. Rio de Janeiro: Centro de Informação das Nações Unidas para o Brasil, 2015. Disponível em: http://www.itamaraty.gov.br/images/ed_desenvsust/Agenda2030-completo-site.pdf. Acesso em: 13 ago. 2022.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2014.

PEREIRA, Mariana Araújo *et al*. **Framework de Big Data**. 1. ed. Porto Alegre: SAGAH, 2019. *E-book*.

PINHEIRO, Patrícia Peck. **Direito digital**. 6. ed. rev., atual. e ampl. São Paulo: Saraiva, 2016.

PORTINARI, Natália. Planalto usa dados de agência para monitorar política em

redes sociais. *In*: FOLHA de São Paulo, São Paulo, 11 abr. 2017. Disponível em: http://www1.folha.uol.com.br/poder/2017/04/1874399-planalto-usa-dados-de-agencia-de-sp-para-monitorar-redes-sociais.shtml. Acesso em: 18 ago. 2022.

PUGA, Sandra; FRANÇA, Edson; GOYA, Milton. **Banco de dados**: implementação em SQL, PL/SQL e Oracle 11g. 1. ed. São Paulo: Pearson Education do Brasil, 2013. *E-book*.

RIO GRANDE DO SUL, Ministério Público. **Acordo de Cooperação Técnica SR/PF/RS e MP/RS nº 01/2022**. Acordo de cooperação técnica que entre si celebram a união, por intermédio da Polícia Federal, com a interveniência da Superintendência Regional da Polícia Federal no Rio Grande do Sul - SR/PF/RS e o Ministério Público do estado do Rio Grande do Sul, por intermédio da Procuradoria-Geral de Justiça, para os fins que especifica. Porto Alegre: Procuradoria-Geral de Justiça, 2022. Disponível em: https://transparencia.mprs.mp.br/media/convenios/convenio/Acordo_de_Coopera%C3%A7%C3%A3o_T%C3%A9cnica_JRb6QGx.pdf. Acesso em: 19 ago. 2022.

ROCHA, Leonel Severo. **Epistemologia jurídica e democracia**. 2. ed. São Leopoldo: UNISINOS, 2003

RUSSELL, Stuart; NORVIG, Peter. **Inteligência artificial**. Rio de Janeiro: Elsevier, 2013. *E-book* (não paginado).

SANTIN, Valter Foleto. Segurança pública e sua política. *In*: **Controle judicial da segurança pública**: eficiência do serviço na prevenção e repressão do crime. 2. ed. São Paulo: Verbatim, 2013. p. 47. *E-book*.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Saraiva, 2015.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2012.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: o direito fundamental à proteção de dados pessoais. *In*: MENDES, Laura Schertel *et al.* (org.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021. *E-book* (não paginado).

SARLET, Ingo Wolfgang. Mais uma vez o caso da boate Kiss: a proteção de dados pessoais. **Consultor Jurídico**, São Paulo, 2022. Disponível em: https://www.conjur.com.br/2022-ago-12/direitos-fundamentais-vez-boate-kiss-protecao-dados-pessoais. Acesso em: 19 ago. 2022.

SCHIOCCHET, Taysa (org.). **Bancos de perfis genéticos para fins de persecução criminal**. Brasília, DF: Ministério da Justiça, 2012. (Série Pensando o Direito, v. 43). *E-book*.

SCHIOCCHET, Taysa; CUNHA, Anita Spies da; LAZZARETTI, Bianca Kaini. Bancos de perfis genéticos para fins de persecução criminal: implicações jurídicas à privacidade, intimidade e estigmatização genéticas. *In*: REUNIÃO DE

ANTROPOLOGIA DA CIÊNCIA E DA TECNOLOGIA, 5., Porto Alegre. **Direitos e Ciências interfaces entre saberes especializados**. Porto Alegre: REACT, 2015. Disponível em: https://ocs.ige.unicamp.br/ojs/react/article/view/1355. Acesso em: 29 ago. 2022.

SCHIOCCHET, Taysa. O humano entre o direito e a genética: pressupostos para o debate legislativo acerca das implicações jurídicas concernentes à criação de bancos de perfis genéticos para fins de persecução criminal no Brasil. *In*: SCHIOCCHET, Taysa (org.). **Bancos de perfis genéticos para fins de persecução criminal**: análise interdisciplinar e em direito comparado. Rio de Janeiro: Multifoco, 2015. p. 29–59.

SCHREIBER, Anderson. **Direitos da personalidade**. São Paulo: Atlas, 2011.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. 1. ed. São Paulo: EDIPRO, 2019. *E-book* (não paginado).

SECURITY and the internet of things. *In*: COMPUTER Science Zone, [*s. l.*], 2015. Disponível em: https://www.computersciencezone.org/security-internet-of-things/. Acesso em: 14 ago. 2022.

SILVA SÁNCHEZ, Jesús-María. **A expansão do direito penal**: aspectos da política criminal nas sociedades pós-industriais. 3. ed. rev. e atual. São Paulo: Revista dos Tribunais, 2013.

SILVA, José Afonso da. **Comentário contextual à Constituição**. 6. ed. São Paulo: Malheiros, 2009.

SIQUEIRA, Deborah. A tecnologia de reconhecimento facial aplicada à segurança pública. *In*: JOTA Info, [*s. l.*], 23 jul. 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/a-tecnologia-de-reconhecimento-facial-aplicada-a-seguranca-publica-23072019. Acesso em: 19 ago. 2022.

SISTEMA de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. *In*: G1, [*s. l.*], 11 jul. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 19 ago. 2022.

SOUSA, Weslei Gomes De. **Inteligência artificial e celeridade processual no Judiciário**: mito, realidade ou necessidade? Dissertação (Mestrado em Administração) – Universidade de Brasília, Brasília, DF, 2020. Disponível em: https://repositorio.unb.br/bitstream/10482/38772/1/2020_WesleiGomesdeSousa.pdf. Acesso em: 4 fev. 2022.

SOUZA, Sartorelli Venâncio de. Criminalização e proteção de dados: análise do caso Roe vs Wade. **Consultor Jurídico**, São Paulo, 26 jul. 2022. Disponível em: https://www.conjur.com.br/2022-jul-26/flora-sartorelli-criminalizacao-protecao-dados. Acesso em: 21 ago. 2022.

STF vai julgar acordo de compartilhamento de dados entre Serpro e ABIN. *In*: CONVERGÊNCIA Digital, [*s. l.*], 19 jun. 2020. Disponível em: https://www.convergenciadigital.com.br/Seguranca/STF-vai-julgar-acordo-de-

compartilhamento-de-dados-entre-Serpro-e-ABIN-53978.html?UserActiveTemplate=site. Acesso em: 28 fev. 2022.

STRECK, Lenio Luiz; MORAIS, José Luis Bolzan de. **Ciência política e teoria do estado**. 7. ed. Porto Alegre: Livraria do Advogado, 2010.

STUCKE, Maurice E.; GRUNES, Allen P. **Big data and competition policy**. Oxford: Oxford University Press, 2016.

SULOCKI, Victoria de. Novas tecnologias, velhas discriminações: ou da falta de reflexão sobre o sistema de algoritmos na Justiça Criminal. *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 651–670.

SUPREMO começa a julgar compartilhamento de dados de usuários de telefonia com o IBGE. *In*: NOTÍCIAS STF, Brasília, DF, 6 maio 2020. Disponível em: http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442823. Acesso em: 4 jul. 2022.

TACCA, Adriano; ROCHA, Leonel Severo. Inteligência artificial: reflexos no sistema do direito. **Revista do Programa de Pós-Graduação em Direito da UFC**, Fortaleza, v. 38, n. 2, p. 53–68, jul./dez. 2018. Disponível em: www.periodicos.ufc.br/nomos/article/ download/20493/95963. Acesso em: 15 jan. 2022.

UNIÃO EUROPEIA. Parlamento Europeu. Conselho da União Europeia. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT%0A. Acesso em: 18 jul. 2022.

UNIÃO EUROPEIA. **Tratado de Lisboa**: que altera o Tratado da União Europeia e o Tratado que Institui a Comunidade Europeia (2007/C 306/01). Lisboa, 2007. Disponível em: http://publications.europa.eu/resource/cellar/688a7a98-3110-4ffe-a6b3-8972d8445325.0018.02/DOC_19. Acesso em: 18 jul. 2022.

VALENTE, Fernanda. MP 954 não define como e para que serão usados dados coletados, diz Rosa Weber. **Consultor Jurídico**, São Paulo, 2020. Disponível em: https://www.conjur.com.br/2020-mai-06/mp-954-nao-define-finalidade-dados-coletados-rosa-weber. Acesso em: 18 ago. 2022.

WERNECK, Antônio. Reconhecimento facial falha em segundo dia, e mulher inocente é confundida com criminosa já presa. *In*: O GLOBO, [*s. l.*], 11 jul. 2019. Disponível em: https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913. Acesso em: 19 ago. 2022.

WITZEL anuncia reconhecimento facial no Maracanã e Santos Dumont: serão instaladas 140 câmeras na capital do estado do Rio de Janeiro; projeto piloto, no

Carnaval, fez com que fossem cumpridos oito mandados de prisão. *In*: VEJA, São Paulo, 29 mar. 2019. Disponível em: https://veja.abril.com.br/politica/witzel-anuncia-reconhecimento-facial-no-maracana-e-santos-dumont/. Acesso em: 22 mar. 2022.

WORLDOMETER. **Real time world statistics**. [*S. l.*]: Worldometer, [2022?]. Disponível em: http://www.worldometers.info/. Acesso em: 13 ago. 2022.

YU, Yipeng *et al.* Automatic training of rat cyborgs for navigation. **Computational Intelligence and Neuroscience**, [*s. l.*], v. 2016, p. e6459251, 2016. Disponível em: https://www.hindawi.com/journals/cin/2016/6459251/. Acesso em: 30 ago. 2022.

ZAFFARONI, Eugenio Raul. **O inimigo no direito penal**. 3. ed. Rio de Janeiro: Revan, 2011.

APÊNDICE A – QUADRO COMPARATIVO ENTRE O ANTEPROJETO DE LGPD PENAL E O PROJETO DE LEI Nº 1.515/2022

Anteprojeto de LGPD Penal, de 2020	Projeto de Lei nº 1.515, de 2022
CAPÍTULO I DISPOSIÇÕES PRELIMINARES Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes para atividades de segurança pública e persecução penal, 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.	CAPÍTULO I DISPOSIÇÕES PRELIMINARES Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais realizado por autoridades competentes **para fins exclusivos** de segurança do Estado, de defesa nacional, de segurança pública e de atividades de investigação e repressão de infrações penais, previstas no inciso III do artigo 4º da Lei nº 13.709, de 14 de agosto de 2018, com os objetivos de: I - proteger os direitos fundamentais de **segurança**, liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural; II - **assegurar a eficiência da atuação dos órgãos incumbidos das atividades mencionadas no caput deste artigo**; e III - **possibilitar o intercâmbio de dados pessoais entre autoridades competentes no exercício das atividades referidas no caput deste artigo**. § 1º As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. § 2º Esta lei **aplica-se**, ainda, **às atividades de inteligência realizadas pelas autoridades competentes no cumprimento de suas competências mencionadas no caput deste artigo, sem prejuízo de leis específicas que regulamentam tais atividades**.
Art. 2º A disciplina da proteção de dados pessoais em atividades de segurança pública e persecução penal tem como fundamentos: I – a dignidade, os direitos humanos, o livre desenvolvimento da personalidade, e o exercício da cidadania pelas pessoas naturais; II – **a autodeterminação informativa**; III – o respeito à vida privada e à intimidade; IV – a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e de opinião; V – a presunção de inocência; **VI – confidencialidade e integridade dos sistemas informáticos pessoais; e** VII – garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal.	Art. 2º A disciplina da proteção de dados pessoais em atividades de segurança pública e de persecução penal tem como fundamentos: I - a dignidade, os direitos humanos, o livre desenvolvimento da personalidade, e o exercício da cidadania pelas pessoas naturais; II - o respeito à vida privada e à intimidade; III - a liberdade de manifestação do pensamento, de expressão, de informação, de comunicação e de opinião; IV - a presunção de inocência; V - garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal; e **VI - o dever estatal de eficiência nas atividades de segurança do Estado e de defesa nacional e de garantia do direito à segurança pública, por meio da instituição de mecanismos que otimizem a prevenção, investigação e repressão de infrações penais.**

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por autoridades competentes em atividades segurança pública e persecução penal.	
Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado.	
Art. 5º Para os fins desta Lei, considera-se: [incisos I a XIX, exceto o III, estão na LGPD] 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 dado biométrico; **III - dado pessoal sigiloso: dado pessoal constitucionalmente protegido por sigilo, como aquele relativo a operações financeiras, registros e conteúdo de comunicações privadas, geolocalização, atividades e documentos físicos ou digitais em ambientes privados, fontes jornalísticas e segredo estatístico;** IV - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; V - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; VI - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: autoridade competente responsável pelas decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); IX - agentes de tratamento: o controlador e o operador; X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, uso compartilhado, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; XI - anonimização: 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;	Art. 3º Para os fins desta Lei, considera-se:

XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organização internacional; XVI - uso compartilhado de dados: divulgação por transmissão, comunicação, transferência, difusão ou qualquer forma de disponibilização, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; XIX - autoridade nacional de proteção de dados: órgão da administração pública responsável por zelar, implementar e fiscalizar a proteção de dados em todo o território nacional;	
XX - autoridade competente: autoridade pública, órgão ou entidade do Poder Público responsável **pela prevenção, detecção, investigação ou repressão de atos infracionais e infrações penais ou execução de sanções penais**, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, ou qualquer outro órgão ou entidade que, nos termos da lei, exerça autoridade ou execute políticas públicas para os referidos efeitos, total ou parcialmente; XXI - atividade de segurança pública: toda e qualquer atividade exercida para a preservação da ordem pública e para prevenção e detecção de infrações penais, inclusive aquelas de inteligência policial e financeira, por autoridades competentes; XXII – atividade de persecução penal: toda e qualquer atividade exercida para a investigação, apuração, persecução e repressão de infrações penais e execução de penas, por autoridades competentes; **XXIII - tecnologia de vigilância: equipamento, programa de computador ou sistema informático que possa ser usado ou**	I - autoridade competente: autoridade pública, órgão ou entidade do Poder Público responsável **pelas atividades de segurança do Estado, de defesa nacional, e pela prevenção, detecção, investigação ou repressão de atos infracionais e infrações penais ou execução de sanções penais**, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, ou qualquer outro órgão ou entidade que, nos termos da lei, exerça autoridade ou execute políticas públicas para os referidos efeitos, total ou parcialmente; **II - atividade de segurança do Estado: toda e qualquer atividade que vise à preservação do território, das instituições, do povo e da soberania nacionais.** **III - atividade de defesa nacional: é a atividade exercida, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas.** IV - atividade de segurança pública: toda e qualquer atividade exercida para a preservação da

implementado para tratamento de dados pessoais captados ou analisados em vídeo, imagem ou áudio.	ordem pública**, da incolumidade das pessoas e do patrimônio,** e para prevenção de infrações penais, realizada por autoridades competentes previstas no artigo 144 da Constituição Federal; V - **atividade de investigação e repressão de infrações penais:** toda e qualquer atividade exercida para a investigação, apuração, persecução e repressão de infrações penais e execução de penas, por autoridades competentes para a finalidade de persecução penal; **VI - dados cadastrais: são os dados apresentados pelo titular para realização ou manutenção do cadastro perante particular ou poder público, não sujeitos a sigilo constitucional ou legal.** **§ 1º Os dados cadastrais a que se refere o inciso VI do caput deste artigo podem incluir informações referentes à qualificação pessoal, dados biométricos, filiação, endereço, nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão, identificação de usuário ou código de acesso que tenha sido atribuído no momento da conexão.** **§ 2º Aplicam-se a esta lei as definições estabelecidas no art. 5º da Lei nº 13.709, de 14 de agosto de 2018 [LGPD].**
Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I – licitude: embasamento do tratamento de dados pessoais em hipótese legal, nos termos do Capítulo II desta Lei; II - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades III - adequação: pertinência e relevância do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento; IV - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; **V – proporcionalidade: compatibilidade do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento;** **VI - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a**	Art. 4º As atividades de tratamento e compartilhamento de dados pessoais em matéria de segurança do Estado, de defesa nacional, de segurança pública e de persecução penal deverão observar a boa-fé e os seguintes princípios: I - licitude: embasamento do tratamento de dados pessoais em hipótese legal, nos termos do Capítulo II desta Lei; II - finalidade: coletados para fins determinados, explícitas e legítimas, e não tratados de uma forma incompatível com essas finalidades, **de modo a subsidiar a atuação dos órgãos incumbidos das atividades de segurança pública, investigação e repressão de infrações penais, em conformidade com suas atribuições legais;** III - adequação: pertinência e relevância do tratamento com os objetivos pretendidos, de acordo com o contexto do tratamento; IV - necessidade: limitação do tratamento ao necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

duração do tratamento, bem como sobre a integralidade de seus dados pessoais; VII - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; **VIII - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;** IX - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; X - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; XI - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; **XII - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.**	V - segurança da informação: utilização de medidas **físicas**, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VI - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais **VII - supremacia do interesse público: prevalência do interesse público em conflito sobre um interesse particular;** VIII - qualidade dos dados: garantia de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; **X - auditabilidade: a tomada de medidas que viabilizem a verificação e a checagem do tratamento, bem como o controle do acesso à informação, sempre que tecnicamente possível.**
Art. 7º No tratamento de dados pessoais, o responsável pelo tratamento deve, na medida do possível, fazer uma distinção clara entre as diferentes categorias de titulares dos dados, especialmente: I – pessoas em relação às quais existem indícios **suficientes** de que cometeram uma infração penal; II – pessoas em relação às quais indícios **suficientes** de que estão prestes a cometer uma infração penal; III – pessoas processadas pela prática de infração penal; IV – pessoas condenadas definitivamente por uma infração penal; V – vítimas de uma infração penal ou pessoas em relação às quais certos fatos indicam que podem ser vítimas de uma infração penal; e VI – outras pessoas, tais como testemunhas, pessoas que possam fornecer informações, ou contatos ou associados das pessoas referidas nos incisos I a V.	Art. 5º No tratamento de dados pessoais, o responsável pelo tratamento deve, na medida do possível, fazer distinção clara entre as diferentes categorias de titulares dos dados, especialmente: I - pessoas em relação às quais existem indícios de que cometeram uma infração penal; II - pessoas em relação às quais existem indícios de que estão prestes a cometer uma infração penal; III - pessoas processadas pela prática de infração penal; IV - pessoas condenadas definitivamente pela prática de infração penal; V - vítimas de uma infração penal ou pessoas em relação às quais certos fatos indicam que podem ser vítimas de uma infração penal; VI - outras pessoas, tais como testemunhas, pessoas que possam fornecer informações, ou contatos ou associados das pessoas referidas nos incisos I a V; e

	VII - pessoas em relação às quais existem indícios de que cometeram ou estão prestes a cometer ações que atentem contra a segurança do Estado.
Art. 8º No tratamento de dados, o responsável deve distinguir, na medida do possível, os dados pessoais baseados em fatos dos dados pessoais baseados em avaliações pessoais. [Art. 10º no Capítulo II - Do tratamento de dados pessoais, Seção I - Dos Requisitos para o Tratamento de Dados Pessoais] Art. 10º. É vedado o tratamento de dados pessoais para atividades de segurança pública e persecução penal por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional, sem prejuízo de outras exigências legais.	Art. 6º No tratamento de dados, o responsável deve distinguir os dados pessoais baseados em fatos dos dados pessoais baseados em avaliações pessoais. **§ 1º Caso o responsável verifique que tratou dados pessoais inexatos ou que tratou dados pessoais de forma ilícita, os dados pessoais devem ser retificados ou apagados.** § 2º É vedado o tratamento dos dados a que se refere o art. 1º desta lei por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo. **§ 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no art. 1º desta lei e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.** **§ 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o art. 1º desta lei poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público.**
CAPÍTULO II DO TRATAMENTO DE DADOS PESSOAIS **Seção I** **Dos Requisitos para o Tratamento de Dados Pessoais**	CAPÍTULO II DO TRATAMENTO DE DADOS PESSOAIS **SEÇÃO I** **DO TRATAMENTO DE DADOS PESSOAIS EM ATIVIDADES DE SEGURANÇA DO ESTADO E DE DEFESA NACIONAL**
	Art. 7º O tratamento de dados pessoais para atividades de segurança do Estado e de defesa nacional poderá ser realizado desde que haja previsão legal específica. **§ 1º A previsão legal de que trata o caput deste artigo se consubstanciará nas competências legais dos órgãos incumbidos das atividades mencionadas no caput deste artigo e nos diplomas legais exarados pelo Ministro de Estado Chefe do Gabinete de Segurança Institucional da Presidência da República, pelo Ministro de Estado da Defesa, pelo Diretor Geral da Agência Brasileira de Inteligência e pelos Comandantes das Forças Armadas.** **§ 2º O compartilhamento de dados pessoais para os fins de segurança do Estado e de defesa nacional poderá ser realizado entre os órgãos incumbidos dessas atividades, com o objetivo de proporcionar eficácia às ações daqueles órgãos, devendo ser observados,**

	para tanto, os princípios descritos no art. 4º desta lei. **§ 3º As atividades a serem regulamentadas nos diplomas legais mencionados no §1º constituem-se, dentre outras, naquelas referentes à inteligência de Estado; à garantia da lei e da ordem (GLO); às de emergência e de ajuda humanitária; às missões de paz: à segurança de grandes eventos; aos exercícios ou operações militares; e aos casos de emprego real das Forças Armadas, na forma da lei.**
	Art. 8º Os órgãos incumbidos das atividades mencionadas no art. 7º deverão estar em condições de fornecer à Autoridade Nacional de Proteção de Dados, a qualquer tempo, informações sobre o tratamento de dados pessoais que realizam.
Art. 9º O tratamento de dados pessoais para atividades de segurança pública e persecução penal somente poderá ser realizado nas seguintes hipóteses: I - quando necessário para o cumprimento de atribuição legal de autoridade competente, na persecução do interesse público, na forma de lei ou regulamento, observados princípios gerais de proteção, os direitos do titular e os requisitos do Capítulo VI desta Lei; II - para execução de políticas públicas previstas em lei, na forma de regulamento, observados os princípios gerais de proteção, os direitos do titular e os requisitos do Capítulo VI desta Lei; III - para a proteção da vida ou da incolumidade física do titular ou de terceiro, contra perigo concreto e iminente.	DO TRATAMENTO DE DADOS PESSOAIS EM ATIVIDADES DE SEGURANÇA PÚBLICA Art. 9º O tratamento de dados pessoais para atividades de segurança pública poderá ser realizado nas seguintes hipóteses: I - quando necessário para o cumprimento de atribuição legal de autoridade competente, na garantia do interesse público, observados os princípios gerais de proteção e os direitos dos titulares na forma desta lei; II - para execução de políticas públicas, observados os princípios gerais de proteção, e os direitos dos titulares na forma desta lei; e III - para a proteção da vida ou da incolumidade física do titular ou de terceiro, contra perigo concreto e iminente. **§ 1º As autoridades competentes poderão tratar os dados pessoais coletados no contexto da prevenção, investigação ou repressão de infrações penais específicas a fim de obter melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detectadas.** **§ 2º O tratamento de dados pessoais sensíveis para atividades de segurança pública poderá ser realizado nas seguintes hipóteses:** **I - cumprimento de obrigação legal;** **II - execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;** **III - proteção da vida ou da incolumidade física do titular, de terceiro ou da coletividade; e** **IV - resguardar direitos relacionados aos titulares dos dados pessoais sensíveis.**
	Art. 10. 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.
	Art. 11. O acesso de autoridades competentes a dados pessoais e a bancos de dados controlados por órgãos e entidades da Administração Pública, para fins de segurança pública, inclusive de inteligência policial, observará as seguintes diretrizes: I - os dados pessoais poderão ser compartilhados por órgãos e entidades federais, distritais, estaduais e municipais, observadas as restrições legais, os requisitos de segurança da informação e comunicações e o disposto na presente Lei; 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 de segurança pública para facilitar a execução de políticas públicas orientadas por dados e o exercício de suas atribuições legais; IV - os órgãos e entidades colaborarão para a redução dos custos de acesso a dados no âmbito da administração pública, inclusive, mediante o reaproveitamento de recursos de infraestrutura e de sistemas por múltiplos órgãos e entidades.
Art. 11. O acesso de autoridades competentes a dados pessoais controlados por pessoas jurídicas de direito privado somente ocorrerá mediante previsão legal específica, respeitados os princípios desta Lei e as obrigações regulatórias aplicáveis ao setor privado e ressalvadas as possibilidades de cooperação voluntária. **§ 1º. Toda e qualquer requisição administrativa ou judicial indicará o fundamento legal de competência expressa para o acesso e a motivação concreta para o pedido, incluindo sua adequação, necessidade e proporcionalidade, sendo vedados pedidos que sejam genéricos ou inespecíficos.** **§2º. A pessoa jurídica de direito privado que não coletar ou já não possuir os dados pessoais solicitados deverá informar tal fato à autoridade solicitante, ficando desobrigada de fornecer tais dados.** **§3º. É lícita a adoção de criptografia ponta-a-ponta ou outro recurso tecnológico que torne tecnicamente impossível a produção de dados requisitados pela autoridade competente, salvo nos casos em que sua implementação se destine principalmente a permitir ou facilitar a prática de ilícitos penais, ou para ocultar a identidade de seus autores**	Art. 12. O acesso de autoridades competentes a dados pessoais e a bancos de dados controlados por pessoas jurídicas de direito privado se dará: I - mediante previsão legal; II - por cooperação voluntária por parte do particular, quando em conformidade com a Lei nº 13.709, de 2018 [LGPD]; III - por meio de contrato, acordo de cooperação ou instrumento congênere.

§4º. É vedada a proibição genérica de notificação dos titulares de dados cujos dados pessoais forem fornecidos em razão de requisição administrativa ou judicial sigilosa, devendo a autoridade competente informar prazo mínimo para possibilidade de notificação.	
Art. 12. A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às operações de tratamento e deverá solicitar às autoridades competentes responsáveis relatórios de impacto à proteção de dados pessoais.	
	Art. 13. O **compartilhamento de dados pessoais controlados pelos órgãos incumbidos de atividades de segurança pública com pessoas jurídicas de direito privado** se dará excepcionalmente, quando presentes razões de interesse público devidamente motivadas em ato administrativo, devendo ser adotadas medidas para garantir um nível de proteção adequado.
Seção II Do Tratamento de Dados Pessoais Sensíveis Art. 13. O tratamento de dados pessoais sensíveis somente poderá ser realizado por autoridades competentes se estiver previsto em lei, observadas as salvaguardas desta Lei. Parágrafo único. A autoridade competente responsável pelo tratamento de dados pessoais sensíveis elaborará relatório de impacto à proteção de dados pessoais e informará a autoridade nacional de proteção de dados.	
Seção III Do Tratamento de Dados Pessoais Sigilosos Art. 14. O tratamento de dados pessoais sigilosos somente poderá ser realizado se estiver previsto em lei e para atividades de persecução penal. §1º. O acesso a dados pessoais sigilosos por meio de ferramentas de investigação e medidas cautelares de obtenção de prova deve observar a legislação especial aplicável. §2º. O acesso a dados pessoais sigilosos controlados por pessoas jurídicas de direito privado será específico a pessoas investigadas e dependerá de ordem judicial prévia baseada em indícios de envolvimento dos titulares de dados afetados em infração penal e na demonstração de necessidade dos dados à investigação, na forma da lei.	
Seção IV Do Tratamento de Registros Criminais Art. 15. Nos autos de investigação e processo criminal, os dados pessoais de investigados, suspeitos, acusados e condenados sem trânsito em julgado da sentença condenatória terão os seus elementos identificadores protegidos. §1º. É vedado o acesso automatizado e massificado a quaisquer documentos, como provas colhidas,	

peças processuais, laudos periciais e documentos análogos dos autos, salvo aos atos decisórios §2º. O Poder Judiciário, o Ministério Público e as Polícias deverão adotar as medidas de segurança para a proteção de dados das pessoas naturais envolvidas nos processos judiciais. §3º. Regulamentação do Conselho Nacional de Justiça disporá sobre as medidas técnicas e administrativas para a implementação do disposto neste artigo.	
	SEÇÃO III DO TRATAMENTO DE DADOS PESSOAIS EM ATIVIDADES DE INVESTIGAÇÃO E REPRESSÃO DE INFRAÇÕES PENAIS Art. 14. É permitido o tratamento e o compartilhamento de dados pessoais e de dados pessoais sensíveis para finalidades de investigação e repressão de infrações penais, observada a legislação processual penal vigente no que couber.
	Art. 15. O acesso de autoridades competentes, a dados pessoais e a bancos de dados controlados por órgãos e entidades da Administração Pública, para fins de investigação e repressão de infrações penais, observará as diretrizes definidas no artigo 11.
	Art. 16. É permitido o tratamento e o compartilhamento de dados pessoais e de dados pessoais sensíveis para finalidades de inteligência de segurança pública (Decreto nº 3.695/2000), investigação e repressão de infrações penais, observada a legislação vigente no que couber.
	Art. 17. O acesso de autoridades competentes, a dados pessoais e a bancos de dados controlados por órgãos e entidades da Administração Pública, inclusive dos órgãos integrantes do Subsistema e Inteligência de Segurança Pública (SISP) para fins de inteligência de segurança pública, investigação e repressão de infrações penais, observará as diretrizes definidas no artigo 12.
	Art. 18. O acesso, tratamento e compartilhamento, no âmbito de atividades de investigação e repressão de infrações penais e de inteligência de segurança pública a dados pessoais e a bancos de dados controlados por pessoas jurídicas de direito privado dar-se-á por meio de: I - requisição do delegado de polícia ou do membro do Ministério Público, com a respectiva indicação do seu fundamento legal; II - por cooperação voluntária por parte do particular, quando em conformidade com a Lei nº 13.709, de 2018; III - por meio de contrato, acordo de cooperação ou instrumento congênere; ou IV - pelo canal técnico de inteligência de Estado.
	Art. 19. O acesso de autoridades competentes para a investigação e repressão de infrações

	penais a dados pessoais controlados por pessoas jurídicas de direito privado que estejam sujeitos a sigilo legal ou constitucional será regulado pela legislação processual penal vigente, mediante autorização judicial, sem prejuízo do acesso aos dados cadastrais, nos termos do artigo anterior.
	SEÇÃO IV DAS DECISÕES AUTOMATIZADAS Art. 20. É vedada a tomada de decisão realizada exclusivamente com base no tratamento automatizado, incluída a definição de perfis, que produzam efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa.
	Art. 21. A tomada de decisões decorrentes de tratamento automatizado deve garantir o direito de solicitar a intervenção humana do responsável pelo tratamento. § 1º São vedadas as definições de perfis que conduzam à discriminação de titulares de dados, com base em dados pessoais sensíveis. § 2º Os sistemas responsáveis por decisões automatizadas a que se refere o artigo 21 devem ser auditáveis, não discriminatórios e passíveis de comprovação acerca de sua precisão e grau de acurácia. § 3º É vedada a adoção de qualquer medida coercitiva ou restritiva de direitos exclusivamente com base em decisão automatizada.
Seção V Dos Limites e do Término do Tratamento de Dados Art. 16. A autoridade competente deve manter procedimentos para evitar que, no curso de suas atividades, obtenha e trate dados pessoais irrelevantes ou excessivos à finalidade da operação de tratamento, devendo descartá-los imediatamente. Art. 17. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I - verificação de que os dados não são ou deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; II - verificação de que a finalidade foi alcançada; II - fim do período de tratamento; ou III - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. Art. 18. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; ou	[O art. 24, do Cap. III da Seção V, corresponde ao art. 16:] Art. 24. A autoridade competente deve manter procedimentos para evitar que, no curso de suas atividades, obtenha e trate dados pessoais irrelevantes ou excessivos à finalidade da operação de tratamento. SEÇÃO V DOS PRAZOS DE ARMAZENAMENTO DOS DADOS PESSOAIS Art. 22. Os dados pessoais coletados em virtude das atividades escopo desta Lei deverão ser eliminados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou III - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. Parágrafo Único. As autoridades competentes deverão estabelecer prazos para a eliminação dos dados pessoais mencionados no caput deste

II - **estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais**	artigo, inclusive para realização de avaliações periódicas da necessidade de conservar tais dados.
CAPÍTULO III DOS DIREITOS DO TITULAR Art. 19. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei, sendo que qualquer restrição a estes direitos deverá ser proporcional, **limitada no tempo** e necessária para finalidades de atividades de segurança pública e persecução penal.	CAPÍTULO III DOS DIREITOS DO TITULAR Art. 23. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei, sendo que qualquer restrição a estes direitos deverá ser proporcional e necessária para finalidades de atividades de segurança do Estado, de defesa nacional, de segurança pública e de persecução penal.
Art. 20. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, 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; e** **VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.** § 1º. O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional. § 2º. Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento. § 3º. Em caso de impossibilidade de adoção imediata da providência de que trata o § 2º deste artigo, o controlador enviará ao titular resposta em que poderá: I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência. § 4º. O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.	Art. 25. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; e III - correção de dados incompletos, inexatos ou desatualizados. § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a Autoridade Nacional de Proteção de Dados **ou em juízo, quando cabível habeas data.** § 2º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento. § 3º Em caso de impossibilidade de adoção imediata da providência de que trata o § 2º deste artigo, o controlador enviará ao titular resposta em que poderá: I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência. § 4º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.
Art. 21. A prestação de informações e a concessão e acesso a dados pode ser adiada, limitada ou	Art. 26. A prestação de informações e a concessão e acesso a dados pode ser adiada,

recusada se e enquanto tal for necessário e proporcional para: I - evitar prejuízo para investigações, inquéritos ou processos judiciais; II - evitar prejuízo para a prevenção, detecção, investigação ou repressão de infrações penais ou para a execução de sanções penais; III - proteger a segurança do Estado ou a defesa nacional; ou IV - proteger os direitos e garantias de terceiros. §1º. Nos casos previstos, o responsável pelo tratamento deve informar o titular dos dados, por escrito e sem demora injustificada, dos motivos da recusa ou da limitação do acesso §2º. A comunicação pode ser omitida apenas na medida em que a sua prestação possa prejudicar uma das finalidades enunciadas no caput, caso em que o titular deve ser informado da possibilidade de levar o questionamento à autoridade nacional ou de iniciar ação judicial. §3º. O controlador deve disponibilizar à autoridade nacional informação sobre os motivos de fato e de direito que fundamentam a decisão de recusa ou de limitação do direito de acesso, bem como da omissão de informação ao titular dos dados.	limitada ou recusada se e enquanto tal for necessário e proporcional para: I - evitar prejuízo para investigações, inquéritos ou processos judiciais; II - evitar prejuízo para a prevenção, detecção, investigação ou repressão de infrações penais ou para a execução de sanções penais; **III - evitar prejuízo às ações de inteligência;** IV - evitar prejuízo às atividades de defesa nacional; V - proteger a segurança do Estado ou a defesa nacional; ou VI - proteger os direitos e garantias de terceiros. §1º Nos casos previstos, o responsável pelo tratamento deve informar ao titular dos dados, por escrito e sem demora injustificada, dos motivos da recusa ou da limitação do acesso**, bem como indicar quando cessarão os motivos da recusa ou da limitação de acesso;** §2º A comunicação pode ser omitida apenas na medida em que a sua prestação possa prejudicar uma das finalidades enunciadas no caput, caso em que o titular deve ser informado da possibilidade de levar o questionamento à ANPD ou de iniciar ação judicial. §3º O controlador deve disponibilizar à ANPD informação sobre os motivos de fato e de direito que fundamentam a decisão de recusa ou de limitação do direito de acesso, bem como da omissão de informação ao titular dos dados.
Art. 22. O direito à retificação de dados pessoais não alcançará informações baseadas em percepções pessoais colhidas por agentes de autoridades competentes e testemunhas.	Art. 27. O direito à retificação de dados pessoais não alcançará informações baseadas em percepções pessoais colhidas por agentes de autoridades competentes e testemunhas.
Art. 23. A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I - em formato simplificado, imediatamente; ou II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no **prazo de até 15 (quinze) dias**, contado da data do requerimento do titular. §1º. Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso. §2º. As informações e os dados poderão ser fornecidos, a critério do titular: I - por meio eletrônico, seguro e idôneo para esse fim; ou **II - sob forma impressa.** §3º. A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.	Art. 28. O acesso às informações pessoais tratadas no âmbito de atividades de segurança do Estado, de defesa nacional e de segurança pública, pelos titulares, dar-se-á por meio de requerimento às autoridades competentes, que deverão providenciar resposta aos titulares no **prazo de 20 (vinte) dias** da entrada do requerimento. § 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso. § 2º As informações e os dados poderão ser fornecidos por meio de documento eletrônico, desde que inteligível, seguro e idôneo. § 3º A ANPD poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos.

Art. 24. As decisões tomadas com base no tratamento automatizado de dados pessoais que possam produzir efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa, incluídas as decisões destinadas a definir o seu perfil pessoal e o risco de envolvimento em infração penal ou de reincidência, deverão ser autorizadas por lei, que preveja garantias adequadas para os direitos e liberdades do titular, incluído o direito de obter a intervenção humana pelo controlador. §1º. O processo legislativo será instruído de relatório público de impacto à proteção de dados pessoais, que demonstre as garantias para a proteção dos direitos e liberdades do titular requeridas no caput, que deverão ser adequadas à natureza dos dados tratados. §2º. Em qualquer caso, é garantido ao titular obter a intervenção humana do responsável pelo tratamento §3º. O titular será notificado imediatamente da utilização de decisões automatizadas que tiverem influenciado ou fundamentado medida coercitiva ou restritiva de direitos. §4º É vedada a adoção de qualquer medida coercitiva ou restritiva de direitos exclusivamente com base em decisão automatizada. §5º. As decisões a que se refere o caput deste artigo não podem basear-se em dados sensíveis.	
Art. 25. O relatório de impacto à proteção de dados que fundamentar decisões automatizadas nos termos desta lei verificará, entre outros, as medidas tomadas para a garantia da não-discriminação e transparência. §1º. Os parâmetros para verificação da natureza discriminatória contemplarão o peso de dados pessoais sensíveis, bem como aqueles referentes à situação sócio-econômica e os dados demográficos relacionados à residência ou os demais capazes de revelar informações sensíveis. §2º. Os sistemas responsáveis por decisões automatizadas conforme o caput devem ser auditáveis nos termos a serem determinados pela autoridade nacional, que não serão restringidos pelo segredo industrial e comercial. §3º. Os parâmetros a serem considerados na auditoria prevista no § 2º contemplarão, entre outros: a) a precisão, incluindo a taxa de falsos positivos ou falsos negativos; b) a reprodutibilidade e disponibilidade de documentação acerca do seu funcionamento.	
Art. 26. O controlador deve assegurar o direito do titular de dados de realizar denúncias confidenciais a respeito de violações a esta Lei.	
Art. 27. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo,	

individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva	
	Art. 29. O acesso, pelos titulares, às informações pessoais tratadas no âmbito de atividades de investigação e repressão de infrações penais se dará nos termos da legislação processual penal vigente.
	DA SEGURANÇA DOS DADOS PESSOAIS Art. 30. Os agentes de tratamento devem adotar medidas de segurança, físicas, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º A ANPD poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do artigo 4º desta Lei. § 2º Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. § 3º No que se refere ao tratamento automatizado de dados, o controlador deve adotar as seguintes medidas: I - impedir o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento; II - impedir que as mídias de dados sejam lidos, copiados, alterados ou retirados sem autorização; III - impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou apagamento não autorizados de dados pessoais armazenados; IV - impedir que os sistemas de tratamento automatizado sejam utilizados por pessoas não autorizadas; V - assegurar que as pessoas autorizadas a utilizar um sistema de tratamento automatizado só tenham acesso aos dados pessoais abrangidos pela sua autorização de acesso; VI - assegurar que possam ser verificados os dados pessoais que foram ou que possam ser transmitidos ou disponibilizados por meio de equipamento de comunicação de dados; VII - assegurar que possam ser verificados a posteriori quais os dados pessoais introduzidos nos sistemas de tratamento automatizado, quando e por quem; VIII - impedir que, durante as transferências de dados pessoais ou o transporte de mídias de

	dados, os dados pessoais possam ser lidos, copiados, alterados ou suprimidos sem autorização; IX - assegurar que os sistemas utilizados possam ser restaurados em caso de interrupção; e X - assegurar que as funções do sistema operem corretamente, que os erros de funcionamento sejam assinalados e que os dados pessoais armazenados não possam ser corrompidos por mau funcionamento do sistema.
	Art. 31. Os sistemas desenvolvidos, a partir da vigência desta Lei, para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. § 1º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. § 2º O responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir a rastreabilidade e a auditabilidade dos sistemas de informação.
	Art. 32. O controlador deverá comunicar à Autoridade Nacional de Proteção de Dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em prazo a ser regulamentado pela ANPD e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. § 2º A Autoridade Nacional de Proteção de Dados verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente.
CAPÍTULO IV DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS Seção I Do Controlador e do Operador	CAPÍTULO V DOS AGENTES DE TRATAMENTO DE DADOS PESSOAIS SEÇÃO I

Art. 28. É obrigatória a elaboração de relatório de impacto à proteção de dados pessoais para tratamento de dados pessoais sensíveis, sigilosos, ou operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados §1º A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, referente a suas operações de tratamento de dados. **§ 2º Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.**	DO CONTROLADOR E DO OPERADOR Art. 33. É obrigatória a elaboração do relatório de impacto à proteção de dados pessoais, referente ao tratamento de dados pessoais sensíveis, sigilosos, ou em operações que apresentem elevado risco aos direitos, liberdades e garantias dos titulares de dados. **§ 1º O relatório mencionado no caput deste artigo deverá considerar, ao menos:** **I - descrição geral das operações de tratamento previstas;** **II - avaliação dos riscos para os direitos dos titulares de dados;** **III - medidas previstas para fazer face a esses riscos; e** **IV - medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais.** **§ 2º Outras informações podem ser solicitadas e determinadas pela ANPD para inclusão no relatório de impacto à proteção de dados pessoais.** § 3º A ANPD poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, referente a outras hipóteses além daquelas mencionadas no caput deste artigo.
Art. 29. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.	Art. 34. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.
Art. 30. A autoridade **nacional** poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.	Art. 35. A Autoridade poderá dispor sobre aspectos referentes ao acesso aos dados e à segurança, e sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.
	Art. 36. Os agentes de tratamento, no exercício de suas atribuições, devem cooperar com a autoridade nacional.
Seção II. Registos das atividades de tratamento Art. 31. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.	DO REGISTRO DAS ATIVIDADES DE TRATAMENTO Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.
Art. 32. O controlador deve manter registro de todas as categorias de atividades de tratamento sob a sua responsabilidade, o qual conterá: I – o nome e os contatos **de operadores, co-controladores** e encarregados; II – a descrição das categorias de titulares de dados e das categorias de dados pessoais; III – as finalidades das operações de tratamento; IV - a indicação da base legal do tratamento; V – a origem da coleta ou recebimento dos dados e as categorias de destinatários com quais os dados pessoais foram compartilhados; VI – a utilização de técnicas e políticas de agrupamento de titulares em perfis, se for o caso;	Art. 38. O registro das operações de tratamento de que trata o art. 37 deverá conter: I - o nome e o contato do encarregado; II - a descrição das categorias de titulares de dados e das categorias de dados pessoais; III - as finalidades das operações de tratamento; IV - a indicação da base legal do tratamento; V - a origem da coleta ou recebimento dos dados e as categorias de destinatários com quais os dados pessoais foram compartilhados; VI - a utilização de técnicas e políticas de agrupamento de titulares em perfis, se for o caso;

VII – as categorias de transferências de dados pessoais para um país terceiro ou para uma organização internacional, se for caso disso; VIII – os prazos de conservação das diferentes categorias de dados pessoais **ou os procedimentos previstos para revisão periódica da necessidade de conservação;** IX – uma descrição geral das medidas técnicas e organizativas em matéria de segurança referidas no capítulo V **X – os pedidos apresentados pelos titulares dos dados e a respetiva tramitação, bem como as decisões do responsável pelo tratamento com a correspondente fundamentação.**	VII - as categorias de transferências de dados pessoais para um país terceiro ou para uma organização internacional, se for caso disso; VIII - os prazos de armazenamento das diferentes categorias de dados pessoais; e IX - a descrição geral das medidas de segurança referidas no capítulo IV. Parágrafo único. A ANPD poderá indicar outras informações a serem incluídas no registro das operações de tratamento.
	SEÇÃO III DO REGISTRO CRONOLÓGICO Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.
Art. 33. Controladores e operadores devem conservar em sistemas de tratamento automatizado registos cronológicos das seguintes operações de tratamento: de coleta, alteração, consulta, acesso, divulgação, transferências, interconexão, apagamento. §1º. Os registos cronológicos das operações de consulta e de divulgação devem permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados pessoais. §2º. Os registos cronológicos serão **mantidos por no mínimo 5 anos** e poderão utilizados para efeitos de verificação da licitude do tratamento, controle administrativo, **exercício do poder disciplinar**, garantia da integridade e segurança dos dados pessoais, análise da autoridade nacional e instrução de processos penais, inclusive a pedido da defesa.	[O PL não possui art. 38] Art. 39. Controladores e operadores devem conservar em sistemas de tratamento automatizado registros cronológicos das seguintes operações de tratamento: coleta; alteração; consulta; acesso; divulgação; transferências; interconexão, e apagamento. § 1º Os registos cronológicos das operações de consulta e de divulgação devem permitir determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou dados pessoais e, sempre que possível, a identidade dos destinatários desses dados pessoais. § 2º Os registos cronológicos, cuja integridade deve ser observada pelos controladores e operadores, serão **mantidos por no mínimo 6 (seis) meses** e poderão ser utilizados para efeitos de verificação da licitude do tratamento, controle administrativo, garantia da integridade e da segurança dos dados pessoais, e para instrução de processos penais, inclusive a pedido da defesa. § 3º A ANPD poderá: I - solicitar aos controladores e operadores a disponibilização dos registros cronológicos; e II - dispor sobre outros prazos de registro cronológico.
Seção III Do Encarregado pelo Tratamento de Dados Pessoais Art. 34. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. § 2º As atividades do encarregado consistem em:	SEÇÃO IV DO ENCARREGADO Art. 40. O controlador deverá indicar encarregado pelo tratamento de dados pessoais. § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.

I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da autoridade nacional e adotar providências; III - orientar os servidores e funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e **IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.** § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.	§ 2º As atividades do encarregado consistem em: I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; II - receber comunicações da Autoridade Nacional de Proteção de Dados e adotar providências; e III - orientar os servidores e funcionários da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais. § 3º A Autoridade Nacional de Proteção de Dados poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.
CAPÍTULO V DA SEGURANÇA E DO SIGILO DOS DADO Seção I Da Segurança e do Sigilo de Dados Art. 35. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. § 1º. A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei. § 2º. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término. § 3º. As medidas de que trata o caput devem ser adotadas com as seguintes finalidades: a. controle de acesso ao equipamento: impedir o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento; b. controle de suporte de dados: impedir que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização; c. controle da conservação: impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou apagamento não autorizados de dados pessoais conservados; d. controle dos utilizadores: impedir que os sistemas de tratamento automatizado sejam utilizados por	

pessoas não autorizadas por meio de equipamento de comunicação de dados; e. controle do acesso aos dados: assegurar que as pessoas autorizadas a utilizar um sistema de tratamento automatizado só tenham acesso aos dados pessoais abrangidos pela sua autorização de acesso; f. controle da comunicação: assegurar que possa ser verificado e determinado a organismos os dados pessoais foram ou podem ser transmitidos ou facultados utilizando equipamento de comunicação de dados; g. controle da inserção: assegurar que possa ser verificado e determinado a posteriori quais os dados pessoais introduzidos nos sistemas de tratamento automatizado, quando e por quem; h. controle do transporte: impedir que, durante as transferências de dados pessoais ou o transporte de suportes de dados, os dados pessoais possam ser lidos, copiados, alterados ou suprimidos sem autorização; i. recuperação: assegurar que os sistemas utilizados possam ser restaurados em caso de interrupção; j. assegurar que as funções do sistema funcionem, que os erros de funcionamento sejam assinalados (fiabilidade) e que os dados pessoais conservados não possam ser falseados por um mau funcionamento do sistema.	
Art. 36. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas prática e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares. § 1º. As medidas de que trata o caput deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. § 2º. Os dados pessoais serão tornados anônimos ou pseudonimizados o quanto antes, de acordo com a finalidade do processamento. § 3º. O responsável pelo tratamento deve implementar medidas técnicas e organizacionais adequadas para garantir que, por padrão, apenas os dados pessoais necessários para cada finalidade específica do tratamento sejam processados.	
Art. 37. 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. § 1º A comunicação será feita no prazo de 72 (setenta e duas) horas e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos;	

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente. § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.	
CAPÍTULO VI ACESSO À INFORMAÇÃO E TRANSPARÊNCIA Art. 38. As autoridades competentes informarão as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a base legal, a finalidade, os objetivos específicos, os procedimentos e as práticas utilizadas para a execução dessas atividades. §1º. As informações a que se refere este artigo serão pormenorizadas em lei ou regulamento, conforme a base legal, observadas as normas do Capítulo II; § 2º. O acesso facilitado às informações sobre o tratamento de dados se dará em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos, de forma clara, adequada e ostensiva, devendo incluir informações, entre outras previstas em regulamentação para o atendimento do princípio do livre acesso, sobre: I - finalidade específica do tratamento; II - forma, escopo e duração do tratamento; III - políticas de retenção, descarte e acesso; IV- identificação do controlador; V - informações de contato do controlador; VI - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VII - responsabilidades dos agentes que realizarão o tratamento; e VIII - direitos do titular, com menção explícita aos direitos contidos no art.20 desta Lei. §2º. A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento, especialmente tendo em vista a	

garantia da segurança pública e atividades de repressão, investigação e persecução de infrações penais e execução da pena.	
Art. 39. A autoridade máxima de cada autoridade competente publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de dados pessoais sigilosos para atividades de persecução penal, contendo: I - o número de pedidos realizados; II - a natureza dos dados solicitados; III - a listagem das pessoas jurídicas de direito privado aos quais os dados foram requeridos; IV - o número de pedidos deferidos e indeferidos judicialmente; V - o número de titulares afetados por tais solicitações.	
CAPÍTULO VII TECNOLOGIAS DE VIGILÂNCIA E TRATAMENTO DE DADOS DE ELEVADO RISCO Art. 40. A utilização de tecnologias de vigilância ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados por autoridades competentes dependerá de previsão legal específica, que estabeleça garantias aos direitos dos titulares e seja precedida de relatório de impacto de proteção de dados pessoais e vigilância. §1º. O processo legislativo será instruído de relatório público de impacto à proteção de dados pessoais e vigilância que contenha: I – uma descrição do escopo do tratamento e das capacidades da tecnologia de vigilância; II – quaisquer testes ou relatórios relativos aos efeitos do tratamento e da tecnologia de vigilância na saúde e na segurança de pessoas; III – quaisquer impactos potencialmente díspares do tratamento de dados e da tecnologia de vigilância ou de sua política de uso em quaisquer grupos protegidos; IV – as medidas previstas para fazer frente aos riscos mencionados nos incisos anteriores; V – as garantias, as medidas de segurança e os mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade do tratamento com a presente lei; e VI – a política de uso e as garantias dos direitos dos titulares, conforme o disposto no §2º deste artigo. §2º. A lei deve estabelecer política de uso que garanta os direitos dos titulares de dados e contenha: I – regras, processos e diretrizes emitid as pela autoridade competente que regulem o tratamento de dados, incluindo o acesso e o uso interno de tal tecnologia de vigilância; II – salvaguardas ou medidas de segurança destinadas a proteger as informações coletadas por tal tecnologia de vigilância contra o acesso não	

autorizado, incluindo, mas não se limitando à existência de criptografia e mecanismos de controle de acesso; III – políticas e práticas relacionadas à retenção, acesso e uso dos dados tratados; IV – políticas e procedimentos relativos ao acesso ou uso dos dados tratados por meio de tal tecnologia de vigilância por membros do público; V – as hipóteses de uso compartilhado, se admitido VI – se algum treinamento é exigido pela autoridade competente para um indivíduo realizar o tratamento, usar tal tecnologia de vigilância ou acessar informações tratadas; VII – uma descrição da auditoria interna e mecanismos de supervisão dentro da autoridade competente para garantir a conformidade com a política de uso que rege o uso de tal tecnologia de vigilância. §3º. No processo legislativo, o relatório de impacto de proteção de dados pessoais e vigilância deverá ser submetido à consulta pública com ampla participação social. §4º. No âmbito de atividades de segurança pública, é vedada a utilização de tecnologias de vigilância diretamente acrescida de técnicas de identificação de pessoas indeterminadas em tempo real e de forma contínua, quando não houver a conexão com a atividade de persecução penal individualizada e autorizada por lei.	
Art. 41. A autoridade nacional emitirá opiniões técnicas ou recomendações referentes à utilização de tecnologias de vigilância ou o tratamento de dados pessoais que representem elevado risco para direitos, liberdades e garantias dos titulares dos dados. §1º. A autoridade nacional deverá publicar relatório anual acerca do uso de tecnologias de vigilância pelas autoridades competentes no território nacional. §2º. Em caso de denúncia de uso de tecnologia de vigilância em descumprimento a esta Lei, a autoridade nacional realizará auditoria para verificação da base legal, da publicação de relatório de impacto e da implementação das medidas e garantias para preservação do direito dos titulares, sem prejuízo de outros mecanismos de controle e supervisão administrativo e judicial.	
CAPÍTULO VIII COMPARTILHAMENTO DE DADOS Art. 42. Qualquer modalidade de uso compartilhado de dados pessoais entre autoridades competentes somente será possível nas hipóteses previstas em lei, desde que observados os propósitos legítimos e específicos para o tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei.	

§ 1º. É vedado o compartilhamento direto e contínuo de bancos de dados estabelecidos no âmbito de atividades de segurança pública com autoridades competentes para fins de persecução penal, as quais somente terão acesso a dados dessa origem para investigação ou processo criminal específico, observadas as demais disposições deste artigo. § 2º. O acesso de agentes de autoridades competentes a dados pessoais de uso compartilhado entre autoridades competentes dependerá de solicitação ao controlador, devidamente motivada quanto ao contexto específico do pedido, à base legal, finalidade, necessidade e proporcionalidade, devendo o registro de acesso e de uso ser mantido por período de no mínimo 5 anos § 3º. O uso compartilhado de dados pessoais sigilosos entre autoridades competentes, inclusive no âmbito de uma mesma autoridade competente, dependerá de autorização judicial específica e motivada que ateste a pertinência e cabimento do compartilhamento.	
Art. 43. O uso compartilhado de dados pessoais entre uma autoridade competente e outro órgão ou entidade do Poder Público não competente para os fins desta Lei dependerá de autorização legal específica, sendo vedadas hipóteses em que o tratamento posterior seja incompatível com a finalidade original da coleta, em termos de expectativas legítimas de titulares de dados ou de objetivos de políticas públicas que ensejaram a coleta original. Parágrafo único. Nas situações compatíveis, o acesso de agentes de autoridades competentes dependerá de requisição e autorização administrativa devidamente motivada quanto ao contexto específico do pedido, à base legal, à finalidade, necessidade e proporcionalidade, resguardada a reserva de jurisdição para dados pessoais sigilosos e devendo ser mantido o registro de acesso e de uso por período de no mínimo 5 anos.	
Art. 44. É vedado a autoridades competentes praticar quaisquer das modalidades de uso compartilhado de dados pessoais com pessoas jurídicas de direito privado, exceto: I - em casos de execução descentralizada de atividade pública, autorizada em lei, e que exija a transferência, exclusivamente para esse fim específico e determinado, observadas as demais disposições desta Lei; II - nos casos em que os dados forem acessíveis publicamente, observadas as demais disposições desta Lei e da Lei nº 13.709/18.	

III - por aquela que possua capital integralmente constituído pelo poder público e esteja na qualidade de operadora de tratamento de dados.	
Art. 45. É vedado a pessoas jurídicas de direito privado praticar modalidades de uso compartilhado de dados com autoridades competentes, exceto nas hipóteses específicas previstas em lei ou mediante cooperação voluntária, desde que observadas as demais disposições dos Capítulos I e II desta Lei e da Lei nº 13.709/18.	
Art. 46. Toda e qualquer operação de uso compartilhado de dados será informada ao público, nos termos e limites do Capítulo VI, e comunicada à autoridade nacional, que poderá determinar a sua imediata suspensão e posterior adequação, limitação e interrupção se configurada violação a dispositivo desta Lei.	
Art. 47. Os registros a que se referem o artigo 42, §2º e o parágrafo único do artigo 43 incluirão a identificação funcional do agente, o endereço IP, a data e o horário do acesso e poderão ser objeto de análise no âmbito de processos administrativos e judiciais, inclusive por titulares de dados pessoais.	
Art. 48. A autoridade nacional poderá requisitar, a qualquer momento, às autoridades competentes, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico para garantir o cumprimento desta Lei.	
Art. 49. A autoridade nacional poderá estabelecer normas complementares para as atividades de que trata o art. 42.	
CAPÍTULO IX TRANSFERÊNCIA INTERNACIONAL DE DADOS E COOPERAÇÃO INTERNACIONAL Seção I. Hipóteses Art. 50. Sem prejuízo de outras condições exigidas em lei, as autoridades competentes só podem transferir dados pessoais para outro país ou para uma organização internacional, inclusive dados que se destinem a transferências ulteriores para outro país ou outra organização internacional, se: I - a transferência for necessária para atividades de segurança pública ou persecução penal; II - tiver sido adotada uma decisão de adequação, nos termos do disposto no art. 51 ou tiverem sido apresentadas garantias adequadas, nos termos do art. 52, ou forem aplicáveis as derrogações previstas no art. 53; III - os dados pessoais forem transferidos para agente responsável no outro país ou na organização internacional competente para fins de atividades de segurança pública ou persecução penal, sem prejuízo do disposto no art. 54;	CAPÍTULO VI TRANSFERÊNCIA INTERNACIONAL DE DADOS E COOPERAÇÃO INTERNACIONAL SEÇÃO I HIPÓTESES Art. 41. Sem prejuízo de outras condições exigidas em Lei, as autoridades competentes poderão transferir dados pessoais para outro país ou para uma organização internacional, inclusive dados que se destinem a transferências ulteriores para outro país ou outra organização internacional, se: I - a transferência for necessária para atividades de **segurança do Estado, de defesa nacional**, de segurança pública ou de persecução penal; II - tiverem sido apresentadas garantias adequadas, nos termos do artigo 45, ou forem aplicáveis as derrogações previstas no artigo 46; **e** III - os dados pessoais forem transferidos para agente no outro país ou na organização internacional com atribuições de segurança do Estado, de defesa nacional, de segurança pública ou de persecução penal, sem prejuízo do disposto no artigo 47.

IV - no caso de os dados pessoais terem sido transmitidos ou disponibilizados por país estrangeiro, esse país tiver dado o seu consentimento prévio à transferência, sem prejuízo do disposto no inciso II; V - no caso de uma transferência ulterior para outro país ou para uma organização internacional, a autoridade competente que realizou a transferência inicial ou outra autoridade competente do mesmo país autorizar a transferência ulterior, após análise de todos os fatores pertinentes, nomeadamente a gravidade da infração penal, a finalidade para que os dados pessoais foram inicialmente transferidos e o nível de proteção no país ou na organização internacional para os quais os dados pessoais forem ulteriormente transferidos; e VI - a transferência não comprometer o nível de proteção das pessoas assegurado pela presente lei. § 1º. As transferências sem o consentimento prévio a que alude o inciso IV apenas são permitidas se forem necessárias para prevenir uma ameaça imediata e grave à segurança pública do Brasil ou de um país estrangeiro e o consentimento prévio não puder ser obtido em tempo hábil. § 2º. No caso previsto no §1º, a autoridade responsável por dar o consentimento deve ser informada em até 48 horas.	§ 1º No caso de os dados pessoais terem sido transmitidos ou disponibilizados por país estrangeiro, é necessário ainda, para a transferência, que esse país tenha dado seu consentimento prévio, salvo se a transferência for necessária para prevenir ameaça imediata e grave à segurança pública do Brasil ou de país estrangeiro e o consentimento prévio não puder ser obtido em tempo hábil. § 2º Sendo aplicada a exceção prevista na parte final do §1º, a autoridade responsável por dar o consentimento deve ser informada em até 48 horas. § 3º Quando do envio de dados pessoais a outro país ou organização internacional, deverá ser ressaltado expressamente que a transferência ulterior desses dados para um terceiro país ou organização internacional só será permitida mediante consentimento da autoridade competente nacional responsável pela transferência inicial. § 4º O consentimento previsto no § 3º deverá levar em conta todos os fatores pertinentes, nomeadamente a gravidade da infração penal, a finalidade para que os dados pessoais foram inicialmente transferidos e o nível de proteção no país ou na organização internacional para os quais se pretende que os dados pessoais sejam ulteriormente transferidos.
	Art. 42. As transferências serão sempre documentadas, devendo o responsável pelo tratamento manter registro das informações sobre a data e hora da transferência, a autoridade competente que as recebe e a natureza dos dados pessoais transferidos.
Seção II. Transferências com base numa decisão de adequação Art. 51. A transferência de dados pessoais para um país estrangeiro ou para uma organização internacional pode ser efetuada com base numa decisão de adequação que determine que aquele país, território ou uma de suas unidades subnacionais, ou a organização internacional destinatária, asseguram um nível de proteção adequado. §1º. A transferência de dados pessoais com base numa decisão de adequação deve observar o art. 34 da Lei nº 13.709/2018 e dispensa uma autorização específica, sem prejuízo dos demais requisitos legais. §2º. A autoridade nacional poderá estabelecer procedimento simplificado para a tomada de decisão sobre o nível de adequação de um país, quando este for um Estado Parte da Convenção do Conselho da Europa, de 1981 (CETS 108) e de seus protocolos.	

§3º. Os atos da autoridade nacional que revoguem, alterem ou suspendam a decisão de adequação não prejudicam as transferências de dados pessoais para outro país, território ou uma sua unidade subnacional, ou para uma organização internacional, quando efetuadas nos termos dos artigos 52 e 53.	
Seção III. Transferências sujeitas a garantias adequadas Art. 52. Na falta de decisão de adequação, os dados pessoais podem ser transferidos para um país estrangeiro ou para uma organização internacional se: I - tiverem sido apresentadas garantias adequadas no que diz respeito à proteção de dados pessoais mediante um instrumento juridicamente vinculativo; ou II - o responsável pelo tratamento tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados. §1º. O responsável pelo tratamento informará a autoridade nacional sobre as categorias de transferências abrangidas pelo inciso II. **§ 2º. As transferências baseadas no inciso II serão documentadas, devendo o responsável pelo tratamento disponibilizar à autoridade nacional, a pedido desta, toda a documentação pertinente, incluindo informações sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos.**	SEÇÃO II TRANSFERÊNCIAS SUJEITAS A GARANTIAS ADEQUADAS Art. 43. Os dados pessoais podem ser transferidos para um país estrangeiro ou para uma organização internacional se: I - tiverem sido apresentadas garantias adequadas no que diz respeito à proteção de dados pessoais, mediante documento formal subscrito pela autoridade destinatária competente; ou II - o responsável pelo tratamento tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados. § 1º Sem prejuízo da possibilidade de avaliações adicionais, **presume-se a existência de garantias adequadas quando**: I - o destinatário se tratar de Estado Parte da Convenção do Conselho da Europa, de 1981 (CETS 108) e de seus protocolos; ou II - a transferência se der no âmbito de organização internacional criada com a finalidade de cooperação nas atividades previstas no artigo 1º, integrada pelo Brasil como país-membro ou participante, e que tenha, em seus tratados constitutivos ou normativos internos, previsões de mecanismos adequados de proteção de dados.
Seção IV. Derrogações aplicáveis em situações específicas Art. 53. **Na falta** 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 país estrangeiro ou para uma organização internacional só podem ser efetuadas se forem necessárias I - para proteger os interesses vitais do titular dos dados ou de outra pessoa; II - para salvaguardar os legítimos interesses do titular dos dados; III - para prevenir uma ameaça imediata e grave contra a segurança pública no Brasil ou em país estrangeiro; IV - **em casos específicos**, para exercer direitos de defesa no âmbito de um processo judicial ou administrativo punitivo, **sem prejuízo das demais exigências legais**; ou	SEÇÃO III DERROGAÇÕES APLICÁVEIS EM SITUAÇÕES ESPECÍFICAS Art. 44. A análise da existência de garantias adequadas nos termos do artigo anterior **poderá ser dispensada**, sem prejuízo das demais exigências legais, quando a transferência de dados pessoais para país estrangeiro ou para uma organização internacional for necessária: I - para proteger os interesses vitais do titular dos dados ou de outra pessoa; II - para salvaguardar os legítimos interesses do titular dos dados; III - para prevenir ameaça imediata e grave contra a segurança pública no Brasil ou em país estrangeiro; IV - para exercer direitos de defesa do Estado no âmbito de processo judicial ou administrativo punitivo; ou

V - em casos específicos, para a cooperação jurídica internacional, de acordo com regras e instrumentos de direito internacional. § 1º. Ainda que se verifiquem os fundamentos previstos no inciso IV, os dados pessoais não serão transferidos se a autoridade competente para proceder à transferência considerar que os direitos, liberdades e garantias fundamentais do titular dos dados em causa prevalecem sobre as finalidades que motivariam a transferência por interesse público. § 2º. As transferências de dados efetuadas com base neste artigo serão limitadas aos dados estritamente necessários para a finalidade almejada. § 3º. O responsável pelo tratamento documentará a informação pertinente referente às transferências realizadas com base no caput, devendo disponibilizar a documentação à autoridade nacional, a pedido desta, incluindo informações sobre a data e a hora da transferência, a autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos.	V - para a cooperação jurídica internacional, de acordo com regras e instrumentos de direito internacional aplicáveis. § 1º Ainda que se verifiquem os fundamentos previstos no inciso IV, os dados pessoais não serão transferidos se a autoridade competente para proceder à transferência considerar que os direitos, liberdades e garantias fundamentais do titular dos dados em causa prevalecem sobre as finalidades que motivariam a transferência por interesse público. § 2º As transferências de dados efetuadas com base neste artigo serão limitadas aos dados estritamente necessários para a finalidade almejada.
Seção V Transferências de dados pessoais para destinatários estabelecidos em outros países Art. 54. Em derrogação do disposto do inciso III do art. 50 e sem prejuízo de um acordo internacional tal como definido no §1º deste artigo, uma autoridade pública com poderes de prevenção, investigação, detecção ou repressão de infrações penais ou de execução de sanções penais, incluindo a prevenção de ameaças à segurança pública, pode, em casos específicos, transferir dados pessoais diretamente a destinatários estabelecidos em outros países desde que, respeitadas as disposições da presente lei, estejam preenchidas as seguintes condições cumulativas: I - A transferência ser estritamente necessária a uma função desempenhada pela autoridade competente que efetua a transferência e prevista por lei, tendo em vista as finalidades indicadas no artigo 1º; II - A autoridade competente que efetuar a transferência considerar que os direitos, liberdades e garantias fundamentais do titular dos dados a serem transferidos não prevalecem sobre as finalidades que exigem a transferência no caso em apreço III - A autoridade competente que efetua a transferência considerar que a transferência para uma autoridade competente para os fins do artigo 1º, no outro país, revela-se ineficaz ou inadequada, especificamente por não ser possível efetuá-la em tempo hábil; IV - A autoridade competente para os efeitos referidos no artigo 1º no outro país, seja informada	SEÇÃO IV TRANSFERÊNCIAS DE DADOS PESSOAIS PARA DESTINATÁRIOS ESTABELECIDOS EM OUTROS PAÍSES Art. 45. Sem prejuízo de outras disposições estabelecidas em acordo internacional tal como definido no parágrafo único deste artigo, a autoridade pública com poderes de prevenção, investigação, detecção ou repressão de infrações penais ou de execução de sanções penais, incluindo a prevenção de ameaças à segurança pública, poderá transferir dados pessoais diretamente a destinatários estabelecidos em outros países, desde que respeitadas as disposições da presente lei, estejam preenchidas as seguintes condições cumulativas: I - a transferência ser estritamente necessária a uma função desempenhada pela autoridade competente que efetua a transferência e prevista por lei, tendo em vista as finalidades indicadas no artigo 1º; II - a autoridade competente que efetuar a transferência considerar que os direitos, liberdades e garantias fundamentais do titular dos dados a serem transferidos não prevalecem sobre as finalidades que exigem a transferência no caso em apreço; III - a autoridade competente que efetua a transferência considerar que a transferência para uma autoridade competente para os fins do artigo 1º, no outro país, revela-se ineficaz ou inadequada, especificamente por não ser possível efetuá-la em tempo hábil; IV - a autoridade competente para os efeitos referidos no artigo 1º no outro país, seja informada

sem demora injustificada, a menos que tal comunicação se revele ineficaz ou inadequada; e V - A autoridade competente que efetua a transferência informar o desti natário da finalidade ou das finalidades específicas para as quais deve tratar os dados pessoais, desde que o tratamento seja necessário. §1º. Para os fins previstos no caput, por acordo internacional entende-se um acordo internacional bilateral ou multilateral em vigor entre o Brasil e o outro país no campo da cooperação jurídica internacional ou da cooperação policial. **§2º. A autoridade competente que efetuar a transferência deve informar a autoridade de controle sobre as transferências realizadas na forma deste artigo.** **§3º. As transferências efetuadas nos termos do presente artigo devem ser documentadas pelo responsável pelo tratamento.**	sem demora injustificada, a menos que tal comunicação se revele ineficaz ou inadequada; e V - a autoridade competente que efetua a transferência informar o destinatário da finalidade ou das finalidades específicas para as quais deve tratar os dados pessoais, desde que o tratamento seja necessário. Parágrafo Único. Para os fins previstos no caput, por acordo internacional entende-se um acordo internacional bilateral ou multilateral em vigor entre o Brasil e o outro país no campo da cooperação jurídica ou policial internacional.
Seção VI. Cooperação internacional no domínio da proteção de dados pessoais Art. 55. Em relação a países estrangeiros e a organizações internacionais, os agentes responsáveis pelo tratamento adotarão as medidas necessárias destinadas a: I - estabelecer procedimentos internacionais de cooperação que visem facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais; II - prestar assistência mútua em matéria de aplicação da legislação de proteção de dados pessoais, nomeadamente através da notificação, da transmissão de reclamações, da assistência na investigação e do intercâmbio de informações, sob reserva das garantias adequadas para a proteção dos dados pessoais e dos outros direitos e liberdades fundamentais; III - associar as partes interessadas aos debates e às atividades que visem promover a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais; IV - promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, inclusive sobre conflitos jurisdicionais com outros países.	SEÇÃO V COOPERAÇÃO INTERNACIONAL NO DOMÍNIO DA PROTEÇÃO DE DADOS PESSOAIS Art. 46. Em relação a países estrangeiros e a organizações internacionais, as autoridades competentes nacionais adotarão as medidas necessárias destinadas a: I - estabelecer procedimentos internacionais de cooperação que visem facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais; II - prestar assistência mútua em matéria de aplicação da legislação de proteção de dados pessoais, nomeadamente através da notificação, da transmissão de reclamações, da assistência na investigação e do intercâmbio de informações, sob reserva das garantias adequadas para a proteção dos dados pessoais e dos outros direitos e liberdades fundamentais; III - associar as partes interessadas aos debates e às atividades que visem promover a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais; e IV - promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, inclusive sobre conflitos jurisdicionais com outros países.
CAPÍTULO X AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS Art. 56. A Autoridade Nacional de Proteção de Dados será responsável por implementar a presente lei, nos termos do art. 55- J da Lei 13.709	CAPÍTULO VII DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS E DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE SEÇÃO I DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS Art. 47. A Autoridade Nacional de Proteção de Dados (ANPD), criada pela Lei nº 13.709, de 14 de agosto de 2018, será responsável por zelar,

de 2018, destacando recursos especializados para essa atribuição. Parágrafo único. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.	implementar e fiscalizar a presente lei em todo o território nacional, de forma cumulativa às suas atribuições estabelecidas na Lei nº 13.709, de 14 de agosto de 2018. Art. 48. À ANPD ficam acrescidas às suas competências descritas na Lei nº 13.709, de 14 de agosto de 2018: I - zelar pela proteção dos dados pessoais na segurança do Estado, na defesa nacional, na segurança pública e na persecução penal, nos termos da legislação; II - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; III - apreciar petições de titular contra o controlador no prazo estabelecido em regulamentação; IV - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais na segurança do Estado, na defesa nacional, na segurança pública e persecução penal; V - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais na segurança do Estado, na defesa nacional, na segurança pública e persecução penal; VI - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; VII - solicitar, a qualquer momento, às autoridades competentes submetidas a esta lei informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; VIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade na segurança do Estado, na defesa nacional, na segurança pública e persecução penal; IX - solicitar relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco aos direitos previstos nesta Lei; X - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; XI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização sobre o tratamento de dados pessoais efetuado pelas autoridades competentes; XII - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

	XIII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei pelas autoridades competentes; e XIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.
	Art. 49. O funcionamento e a organização da Autoridade permanecem os mesmo estabelecidos na Lei nº 13.709, de 14 de agosto de 2018.
	SEÇÃO II DO CONSELHO NACIONAL DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE Art. 50. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, em acréscimo às suas competências estabelecidas na Lei nº 13.709, de 14 de agosto de 2018: I - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais na segurança do Estado, na defesa nacional, na segurança pública, investigação e persecução penal; II - propor à Autoridade Nacional de Proteção de Dados a edição de regulamentos e procedimentos sobre proteção de dados pessoais e privacidade na segurança do Estado, na defesa nacional, na segurança pública e persecução penal; e III - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;
	Art. 51. O funcionamento e a organização do Conselho permanecem os mesmo estabelecidos na Lei nº 13.709, de 14 de agosto de 2018.
CAPÍTULO XI SANÇÕES Art. 57. As infrações às normas previstas nesta Lei ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: I - advertência, com indicação de prazo para adoção de medidas corretivas; **II - publicização da infração após devidamente apurada e confirmada a sua ocorrência;** III - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; **IV - eliminação dos dados pessoais a que se refere a infração;** V - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de **6 (seis) meses**, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; **VI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;** § 1º. O agente público que facilitar ou der causa à infração das normas desta Lei responderá	CAPÍTULO VIII SANÇÕES Art. 52. As infrações às normas previstas nesta Lei ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - bloqueio dos dados pessoais a que se refere a infração até a sua regularização, quando cabível; III - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de **2 (dois) meses**, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador, quando cabível; § 1º O agente público que facilitar ou der causa à infração das normas desta Lei responderá

administrativamente, conforme a lei disciplinar aplicável, incluindo, conforme o caso, a Lei de Improbidade Administrativa. § 2º. Se o mesmo fato constituir simultaneamente crime e infração administrativa contra a mesma pessoa natural, o procedimento administrativo será suspenso quando iniciada medida de investigação de infração penal, retomando-se o caso não sobrevenha sentença declarando a inexistência material do fato ou sua prática em legítima defesa, estado de necessidade, exercício regular de um direito ou cumprimento de um dever.	administrativamente, conforme a lei disciplinar aplicável, incluindo, conforme o caso, a Lei de Improbidade Administrativa. § 2º Se o mesmo fato constituir simultaneamente crime e infração administrativa contra a mesma pessoa natural, o procedimento administrativo será suspenso quando iniciada medida de investigação de infração penal, retomando-se caso não sobrevenha sentença declarando a inexistência material do fato ou sua prática em legítima defesa, estado de necessidade, exercício regular de um direito ou cumprimento de um dever. § 3º A responsabilização administrativa não afastará a civil e a penal.
Art. 58. A fixação da sanção aplicável será feita de maneira fundamentada e considerará: I - A gravidade da lesão; II - A culpabilidade do agente; **III - A capacidade econômica do infrator.** § 1º. São circunstâncias que agravam a sanção: I - A reiteração de infrações II - A motivação político-partidária, preconceituosa ou de qualquer forma direcionada a grupos ou instituições determinadas; III - A condição de funcionário público no exercício da função. § 2º. São circunstâncias que atenuam a sanção: I - A comunicação espontânea da infração à autoridade e aos titulares dos dados; II - O emprego espontâneo dos meios disponíveis para mitigação do dano; III - A reparação espontânea dos danos; IV - A adoção de política eficaz de proteção de dados; § 3º. Quando a lesão for de menor magnitude e presentes as atenuantes do § 2º, a autoridade poderá, em decisão motivada e fundamentada, deixar de aplicar a sanção, ausentes as agravantes do § 1º.	Art. 53. A fixação da sanção aplicável será feita de maneira fundamentada e considerará: I - a gravidade da lesão; e II - a culpabilidade do agente; § 1º São circunstâncias que agravam a sanção: I - a reiteração de infrações; II - a motivação político-partidária, preconceituosa ou de qualquer forma direcionada a grupos ou instituições determinadas; e III - A condição de funcionário público no exercício da função. § 2º São circunstâncias que atenuam a sanção: I - a comunicação espontânea da infração à ANPD e aos titulares dos dados; II - o emprego espontâneo dos meios disponíveis para mitigação do dano; III - a reparação espontânea dos danos; IV - a adoção de política eficaz de proteção de dados; § 3º Quando a lesão for de menor magnitude e presentes as atenuantes do § 2º, a Autoridade Nacional de Proteção de Dados poderá, em decisão motivada e fundamentada, deixar de aplicar a sanção, ausentes as agravantes do § 1º.
Art. 59. O descumprimento desmotivado de ordem judicial de quebra de sigilo por pessoas jurídicas de direito privado controladoras de dados poderá ser considerado ato atentatório à dignidade da Justiça, nos termos do artigo 77, § 2o, do Código de Processo Civil, sem prejuízo do crime de desobediência, caso a determinação possua previsão legal. § 1º. O cálculo da multa deve se dar de maneira fundamentada, observando as balizas do art. 58, e considerará: I - Eventual cumprimento parcial da ordem; II - Capacidade do controlador do dados; e III - Onerosidade ao controlador dos dados. § 2º. Nos termos do artigo 11 ,§3º, a incapacidade técnica decorrente do emprego de mecanismo de proteção de dados, a exemplo da criptografia ponta-	

a-ponta, torna impossível o cumprimento da ordem judicial, não dispensando o destinatário da ordem da obrigação quanto aos dados disponíveis. § 3º. Em casos de questionamento razoável sobre a validade da ordem à luz da legislação regente em matéria de proteção de dados pessoais que for levado a juízo ou à autoridade nacional, o controlador de dados não será punido por atraso no cumprimento.	
CAPÍTULO XII DISPOSIÇÕES FINAIS E TRANSITÓRIAS Art. 60. O órgão previsto no artigo 14 da Lei n. 9.613, de 3 de março de 1998 [COAF], é autoridade competente e submete-se ao disposto nesta Lei. §1º. Os dados pessoais tratados pelas pessoas obrigadas referidas no artigo 9o, caput e parágrafo único, da Lei 9.613, de 3 de março de 1998, devem se limitar ao mínimo necessário para o cumprimento do disposto no artigo 11 do mesmo diploma legal, submetendo-se ao disposto na presente Lei §2º. Os dados referidos no caput não podem ser tratados pelas autoridades competentes de forma incompatível com as finalidades previstas na Lei 9.613, de 3 de março de 1998, e as normas da presente Lei. §3º. É vedado o tratamento dos dados referidos no caput deste artigo para quaisquer outros fins, como os fins comerciais.	
Art. 61. As autoridades fiscais e aduaneiras, as unidades de investigação de inteligência financeira, as autoridades administrativas independentes, ou as autoridades dos mercados financeiros, responsáveis pela regulamentação e supervisão dos mercados de valores mobiliários obrigadas legalmente à comunicação de suspeita de prática de infração penal às autoridades definidas no artigo 1o submetem-se ao disposto nesta Lei, restringindo-se à transmissão aos dados estritamente necessários para o atendimento da finalidade legal específica, sem prejuízo de prévia autorização judicial quando exigida em lei.	
Art. 62. O Decreto -Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações: “Invasão de dispositivo informático Art. 154-A. Acessar indevidamente ou invadir dispositivo informático alheio, conectado ou não à rede de computadores, ou nele instalar vulnerabilidade: (NR) Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (NR) Petrechos para invasão § 1º Produzir, oferecer ou difundir dispositivo, programa de computador, técnica ou vulnerabilidade com o intuito de permitir a prática da conduta definida no caput: (NR) Pena – detenção, de 6 (seis) meses a 2 (anos), e multa. (NR) § 2º A pena será de reclusão, de 2 (dois) a 5 (cinco) anos, se o fato não constitui crime mais grave, se resultar: I - na obtenção, modificação ou eliminação de: (NR)	

a) dados de comunicações eletrônicas privadas; (NR) b) segredos profissionais, comerciais ou industriais; (NR) c) informações sigilosas, assim definidas em lei ou decisão judicial; (NR) d) dados pessoais sensíveis. (NR) II - na modificação, alteração ou interrupção do funcionamento de sistema informático ou no impedimento de seu restabelecimento: (NR) § 3º Aumenta-se a pena de um a dois terços se: (NR) I - o crime for praticado por funcionário público em razão do exercício de suas funções; (NR) II – o sistema infor mático pertencer à Administração Pública, nacional ou estrangeira, ou a organização internacional; (NR) II – o crime for praticado com o fim de obtenção de vantagem indevida; (NR) IV - resultar em prejuízo econômico a outrem; (NR) V - o agente obtiver o controle remoto não autorizado do dispositivo; (NR) VI - o agente obtiver informações classificadas como reservadas, secretas ou ultrassecretas, conforme a lei; (NR) VII - houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos; (NR) III - houver divulgaçã o, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (NR) §4º Considera-se dispositivo informático todo equipamento tecnológico com capacidade computacional, fixo ou móvel. (NR) Ação Penal Art. 154-B. Nos crim es definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (NR) Parágrafo único. Se o crime é cometido contra organização internacional ou entidades estatais ou representações diplomáticas de país estrangeiro, somente se procede mediante requisição do Ministro da Justiça. (NR) Capítulo V - Dos crimes contra a proteção de dados pessoais (NR) Transmissão ilegal de dados pessoais (NR) Art. 154-C. Transmitir, distribuir, usar de forma compartilhada, transferir, comunicar, difundir dados pessoais ou interconectar bancos de dados pessoais sem autorização legal: (NR) Pena - reclusão, de 1 (um) a 4 (quatro), anos e multa. (NR) Parágrafo único. Aumenta-se a pena de um a dois terços se: (NR) I - os dados pessoais forem sensíveis ou sigilosos; (NR) II – praticado por funcionário público em razão do exercício de suas funções; (NR) III – praticado com o fim de obtenção de vantagem indevida; (NR) IV – a conduta causar dano ao titular dos dados ou a terceiros a ele relacionados. (NR) ..... Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública 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. Parágrafo único. Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública. (NR) ..... Inserção de dados falsos em sistema informático (NR) Art. 313-A. Inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos no sistema informático ou em bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (NR) Pena – reclusão, de 3 (três) a 8 (oito) anos, e multa. (NR) Modificação ou alteração não autorizada de sistema informático (NR) Art. 313- B. Modificar ou alterar o funcionamento de sistema informático sem autorização ou solicitação de autoridade competente: (NR) Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa. Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta prejuízo para a Administração Pública ou para o administrado. (NR) ..... Desobediência Art. 330..... Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.” (NR) Art. 63. O artigo 1º, parágrafo único, da Lei 8.137, de 27 de dezembro de 1990, passa a vigorar com a seguinte redação: “Art. 1º..... ..... Parágrafo único. A falta de atendimento da exigência da autoridade, no prazo de 10 (dez) dias, que poderá ser convertido em horas em razão da maior ou menor complexidade da matéria ou da dificuldade quanto ao atendimento da exigência, sujeitará o autor à pena de reclusão, de 1 (um) a 3 (anos), e multa.” (NR) Art. 64. O disposto no artigo 69 da Lei n. 9.605, de 12 de fevereiro de 1998, passa a vigorar com a seguinte redação: “Art. 69..... Pena – reclusão, de um a três anos, e multa” (NR)	
	CAPÍTULO IX DISPOSIÇÕES FINAIS E TRANSITÓRIAS Art. 54. A Lei nº 12.850, de 2 de agosto de 2013 passa a vigorar com as seguintes alterações: Artigo 10 -A ..... § 1º..... II - dados cadastrais: são os dados apresentados pelo titular para realização ou manutenção do cadastro perante particular ou poder público, abrangendo aquelas informações referentes à qualificação pessoal, dados biométricos, filiação, endereço, nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão, identificação de usuário ou código de acesso que tenha sido atribuído no momento da conexão, bem como demais dados não sujeitos a sigilo constitucional

	ou legal. Artigo 15. O delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito. Art. 55. A Lei nº 12.965, de 23 de abril de 2014, passa a vigorar com as seguintes alterações: “Art. 5º ..... VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP e porta lógica de acesso utilizados pelo terminal para o envio e recebimento de pacotes de dados; ..... IX - dados cadastrais: são os dados apresentados pelo titular para realização ou manutenção do cadastro perante particular ou poder público, abrangendo aquelas informações referentes à qualificação pessoal, dados biométricos, filiação, endereço, nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão, identificação de usuário ou código de acesso que tenha sido atribuído no momento da conexão, bem como demais dados não sujeitos a sigilo constitucional ou legal.” (NR) “Artigo 10 .....§ 3º O disposto no caput não impede o acesso aos dados cadastrais, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.” (NR) Art. 56. A Lei nº 9.613, de 3 de março de 1998, passa a vigorar com as seguinte alteração: “Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado, na forma da lei, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.” (NR) Art. 57. A Lei nº 12.037, de 1º de outubro de 2009, passa a vigorar com as seguintes alterações: “Art. 7º-C ..... § 2º O Banco Nacional Multibiométrico e de Impressões Digitais tem como objetivo armazenar dados de registros biométricos, de impressões digitais e, quando possível, de íris, face e voz, para subsidiar investigações criminais federais, estaduais ou distritais, bem como apoiar a identificação ou verificação de identidade do cidadão. ..... § 6º No caso de bancos de dados de identificação de natureza civil, administrativa ou eleitoral, a integração ou o compartilhamento dos registros do Banco Nacional Multibiométrico e de Impressões Digitais incluirá impressões digitais, biometria facial, voz, íris, entre outras, e às informações

	necessárias para identificação do seu titular. § 7º A integração ou a interoperação dos dados de registros multibiométricos constantes de outros bancos de dados com o Banco Nacional Multibiométrico e de Impressões Digitais ocorrerá por meio de acordo ou convênio com a unidade gestora e não dependerá de ressarcimento ao detentor dos dados. ..... § 11. A mera verificação biométrica da autenticidade de documento de identificação pessoal, com uso do BNM, é permitida a agentes públicos para fins de segurança pública e de identificação do cidadão (NM).” (NR)
	Art. 58. O compartilhamento de dados, entre unidades da Administração Pública Federal, com a finalidade de subsidiar atividades de segurança pública e investigação criminal, é obrigatório, respeitará o disposto nesta Lei e independerá de ressarcimento ou de qualquer tipo de remuneração ao detentor originário do banco de dados. Parágrafo Único. O disposto no caput respeitará o sigilo legal ou constitucional de dados, regulados pela legislação processual penal vigente, e será, nesses casos de sigilo, operado mediante autorização judicial.
Art. 65. A adequação do tratamento de dados às normas previstas nesta lei deverá ser implementada pelos agentes de tratamento até a sua entrada em vigor. § 1º. O não atendimento ao disposto no caput dentro prazo de dois anos implicará na ilicitude do tratamento e os dados deverão serem eliminados. §2 º. A autoridade nacional deverá supervisionar o cumprimento do disposto neste artigo, emitindo orientações e estabelecendo normas sobre a adequação progressiva de banco de dados constituídos até a entrada em vigor desta lei, considerando a complexidade das operações de tratamento, a natureza dos dados, a amplitude do compartilhamento de bancos de dados.	
[O anteprojeto não tem art. 66] Art. 67. Esta lei entrará em vigor **18 (dezoito) meses** após a data de sua publicação.	Art. 59. Esta lei entrará em vigor **180 dias** a contar da data de sua publicação.
Legenda * As marcações em **negrito** salientam as diferenças, inclusões e exclusões, de conteúdo do anteprojeto para o Projeto de Lei, especialmente quando identificada a importação de artigos de um para o outro com modificações. ** Os destaques em vermelho indicam erros formais na redação da proposta.	

Fonte: elaborado pela autora com base no anteprojeto[282] e no PL 1.515/2022.[283]

[282] CORDEIRO, Nefi *et al.* **Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal**. Brasília, DF, 2020. Disponível em: https://www.conjur.com.br/dl/anteprojeto-lei-disciplina-protecao.pdf. Acesso em: 28 fev. 2022.

[283] ARMANDO, Coronel. **Projeto de lei nº 1.515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, DF: Câmara dos Deputados, 7 jun. 2022.

Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node09wqlrgv9qemi1qa4zbdv699tb12566378.node0?codteor=2182274&filename=Tramitacao-PL+1515/2022. Acesso em: 1 ago. 2022.