PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS
Programa de Pós-Graduação em Direito

Sidney Cassio Alves Rocha

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA ATIVIDADE JURÍDICO-PENAL DO ESTADO: análise garantista a partir da teoria do bem jurídico

Belo Horizonte
2025

Sidney Cassio Alves Rocha

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA ATIVIDADE JURÍDICO-PENAL DO ESTADO: análise garantista a partir da teoria do bem jurídico

Tese apresentada ao Programa de Pós-Graduação *stricto sensu* em Direito da Pontifícia Universidade Católica de Minas Gerais como requisito parcial para a obtenção do título de Doutor em Direito.
Orientador: Prof. Dr. Henrique Viana Pereira

Belo Horizonte
2025

FICHA CATALOGRÁFICA
Elaborada pela Biblioteca da Pontifícia Universidade Católica de Minas Gerais

Rocha, Sidney Cassio Alves
R672p Privacidade e proteção de dados pessoais na atividade jurídico-penal do estado: análise garantista a partir da teoria do bem jurídico / Sidney Cassio Alves Rocha. Belo Horizonte, 2025.
185 f.

Orientador: Henrique Viana Pereira
Tese (Doutorado) - Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito

1. Informação confidencial - Proteção. 2. Segurança de dados. 3. Proteção de dados pessoais. 4. Bem jurídico. 5. Direito penal - Brasil. 6. Direito à privacidade. Direitos fundamentais. I. Pereira, Henrique Viana. II. Pontifícia Universidade Católica de Minas Gerais. Programa de Pós-Graduação em Direito. III. Título.

CDU: 343:681.3
Ficha catalográfica elaborada por Fabiana Marques de Souza e Silva - CRB 6/2086

Sidney Cassio Alves Rocha

PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NA ATIVIDADE JURÍDICO-PENAL DO ESTADO: análise garantista a partir da teoria do bem jurídico

Tese apresentada ao Programa de Pós-Graduação *stricto sensu* em Direito da Pontifícia Universidade Católica de Minas Gerais como requisito parcial para a obtenção do título de Doutor em Direito.

_____
Prof. Dr. Henrique Viana Pereira – PUC Minas (Orientador)

_____
Profª. Drª. Klelia Canabravo Aleixo – PUC Minas (Banca examinadora)

_____
Prof. Dr. José Adércio Leite Sampaio – PUC Minas (Banca examinadora)

_____
Prof. Dr. Julio César Faria Zini – UFMG (Banca examinadora)

_____
Profª. Drª. Carla Silene C. Lisboa Bernardo Gomes - IBMEC (Banca examinadora)

Belo Horizonte, 02 de abril de 2025.

RESUMO

A transição para a Sociedade 5.0 acarreta avanços tecnológicos que se manifestam de diversas formas na vida dos indivíduos. A expansão do Direito Penal utiliza a obtenção de informações sigilosas a partir de novos recursos de vigilância, interceptação e infiltração em dispositivos informáticos, acarretando violações a bens jurídicos de fundamental importância no desenvolvimento livre e autônomo dos indivíduos. Tais bens jurídicos relacionam-se com a privacidade e seus diversos aspectos ou manifestações jurídicas, tais como intimidade, vida privada, segredo, isolamento e formas de controle de informações sobre si, especialmente (mas não unicamente) na forma de dados pessoais e constituem autênticos direitos fundamentais. As medidas interventivas em direitos fundamentais demandam apropriada legislação que regulamente adequadamente as atividades de tratamento de dados pessoais a serem realizadas pelo Estado em sua atuação jurídico-penal. A experiência alemã neste tema é notável por seu pioneirismo e pela abordagem compatível com a dogmática constitucional-penal daquele país, servindo de paradigma para a necessária abordagem brasileira que ainda necessita de regulamentação. A evolução jurídica do tema de proteção de dados pessoais no Brasil deve ser considerada por ocasião da elaboração legislativa de norma regulamentadora da atuação jurídico-penal do Estado. Ao mesmo tempo, refuta-se ceder aos clamores expansionistas do Direito Penal da criminalização por meio da criação de novos tipos penais, uma vez que o Código Penal brasileiro já tipifica suficientemente tais condutas incriminadoras.

Palavras-chave: Privacidade. Proteção de dados. Direitos fundamentais. Medidas de intervenção penal. Bem jurídico.

ABSTRACT

The transition to Society 5.0 has brought about technological advances that are manifested in different ways in individuals' lives. Criminal law expansion uses new surveillance, interception and infiltration resources to obtain confidential information on computer devices, leading to violations of legal assets that are of fundamental importance to the free and autonomous development of individuals. These legal assets relate to privacy and its various aspects or legal manifestations, such as intimacy, private life, secrecy, isolation and ways of controlling information about oneself, especially (but not exclusively) in the form of personal data and constitute authentic fundamental rights. Measures to intervene in fundamental rights require appropriate legislation to adequately regulate the processing of personal data to be carried out by the state in its legal and criminal activities. The German experience in this field is notable for its pioneering spirit and its approach compatible with Brazilian constitutional-penal dogmatic work, serving as a paradigm for the necessary Brazilian legislative approach, which still needs to be regulated. The legal evolution of personal data protection in Brazil must be considered when drafting legislation to regulate the state's legal-penal action. At the same time, there is no question of giving in to the expansionist clamors of criminal law by creating new legal crime descriptions, since Brazilian Penal Code already sufficiently typifies such incriminating conducts.

Keywords: Privacy. Data protection. Fundamental rights. Criminal intervention measures. Legal assets.

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
ADPF	Arguição de Descumprimento de Preceito Fundamental
ANPD	Autoridade Nacional de Proteção de Dados Pessoais
EUA	Estados Unidos da América
GDPR	General Data Protection Regulation
IA	Inteligência Artificial
IBGE	Instituto Brasileiro de Geografia e Estatística
IoT	Internet of Things
LGPD	Lei Geral de Proteção de Dados
NSA	National Security Agency
NIST	National Institute of Standards and Technology
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ONU	Organização das Nações Unidas
PL	Projeto de Lei
PLS	Projeto de Lei do Senado
PUC Minas	Pontifícia Universidade Católica de Minas Gerais
RGPD	Regulamento Geral sobre a Proteção de Dados
SERPRO	Serviço Federal de Processamento de Dados
STF	Supremo Tribunal Federal
TFUE	Tratado sobre o Funcionamento da União Europeia
TI	Tecnologia da Informação
UNESCO	Organização das Nações Unidas para a Educação, a Ciência e a Cultura

SUMÁRIO

1 INTRODUÇÃO

O mundo caminha a passos largos em direção à onipresença tecnológica nas mais diversas áreas da atuação humana. Na medicina, na guerra, na agricultura, no noticiário, em tudo a tecnologia avança rompendo com o antigo, e não seria diferente no Direito.

Há anos a tecnologia tem adquirido status central na vida humana. Seja pela facilidade de uso, integração social, disponibilidade de informação, elevada produtividade, é impensável uma sociedade contemporânea minimamente desenvolvida sem utilização da tecnologia disponível. Ainda, pode-se assumir que a “corrida” que definirá o domínio geopolítico, militar e econômico mundial está intimamente relacionada à capacidade de pesquisa, desenvolvimento, adoção e imposição de padrões tecnológicos como 6G, Inteligência Artificial, robótica, Internet das Coisas e computação quântica, dentre outros.

Este avanço tecnológico de múltiplas camadas estará disponível não somente para a sociedade civil, mas também para o Estado e seu insaciável apetite por controle. Os impactos sociais produzidos pelas transformações tecnológicas se refletirão, mais tarde ou menos tarde, no Direito, especialmente no Direito Penal, que será demandado a lidar com a regulamentação desse admirável mundo novo, mas com as velhas dificuldades que são carregadas de etapa em etapa, em ciclos de evolução social cada vez mais curtos.

A administração pública busca utilizar a tecnologia com diversas finalidades, passando pelo fornecimento de novos, mais rápidos e melhores serviços. No campo da fiscalização, por exemplo, a integração cada vez mais ampla de seus sistemas informáticos permite ao Estado minimizar o inadimplemento tributário e obter dados que lhe forneçam informações valiosas, em prazos reduzidos, sobre a arrecadação estatal. Já no campo penal, que é o que interessa a esse trabalho, a administração pública avança empregando tecnologia a fim de obter dados a partir de fontes que não obtinha com certa facilidade, como na utilização de câmeras de vigilância para identificar suspeitos e criminosos por meio de reconhecimento facial, e a fim de realizar análises que servirão à matéria criminal, seja na investigação, ao longo do processo penal ou mesmo na execução penal.

Assim, o indivíduo, que compulsoriamente é submetido ao exercício do poder penal estatal, percebe sua privacidade integralmente devassada pelo Estado desde o momento que é considerado suspeito até o momento que, caso tenha sido condenado e tenha cumprido sua pena, sai pela porta do sistema prisional, sofrendo consequências permanentes, em razão da persistente violação de sua autodeterminação informacional, que o acompanharão até o fim da sua existência.

A introdução de novos métodos de intervenção oriundos desse estrondoso avanço tecnológico inclui a utilização de diversas tecnologias que permitem, por parte dos agentes estatais, a obtenção de comunicações, imagens e todos os tipos de dados que se possam armazenar em dispositivos informáticos de utilização pessoal.

Entretanto, conforme será abordado no presente trabalho, essas medidas de intervenção afetam diretamente bens jurídicos do mais importante valor, inerentes ao núcleo mais profundo da representação da dignidade humana. São bens jurídicos contidos no direito à privacidade e à proteção de dados pessoais, direitos estes dotados de valor constitucional, alçados a direitos fundamentais.

Simultaneamente, a dogmática penal enfrenta a demanda por tutela penal desses bens jurídicos frente à excessiva possibilidade de intervenção estatal na esfera privada do indivíduo, sem as devidas garantias da preservação dos aspectos mínimos desses direitos, seja por desconhecimento da natureza desses bens jurídicos, seja por ausência de legislação apropriada que regulamente tais intervenções.

Assim, a problematização do tema envolve a compreensão da evolução dogmática da privacidade enquanto bem jurídico constitucional-penal, a análise do direito comparado especialmente na forma da experiência jurídica alemã, em razão da proximidade dos institutos penais alemães e brasileiros, e do pioneirismo alemão no tema.

A dificuldade inerente à conceituação e delimitação da privacidade e suas nuances na forma de expressões como intimidade, vida privada, segredo, confidencialidade, controle de acesso, dentre outros, torna árdua a tarefa do legislador penal em proteger tais bens jurídicos. Em razão disso, críticos da teoria do bem jurídico podem questionar a legitimidade e adequação (ou rendimento) dessa teoria para fundamentar a devida proteção constitucional-penal a esses valores e interesses jurídicos contemporâneos.

Ainda, pretende-se identificar o adequado caminho a ser trilhado pela dogmática constitucional-penal brasileira no estabelecimento de critérios jurídicos que forneçam adequada proteção aos bens jurídicos abordados neste trabalho. A análise abordará o cenário jurídico atual brasileiro em justaposição ao cenário jurídico alemão, tomado aqui neste trabalho como paradigmático.

O legislador da principal legislação de proteção de dados pessoais brasileira, a Lei Geral de Proteção de Dados, excetuou a sua aplicabilidade para atividades de tratamento de dados pessoais realizadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, transferindo tal regulamentação para legislação específica sobre o assunto. Pretende-se trazer à discussão a evidente urgência na devida regulamentação do tema de tratamento e proteção de dados pessoais em matéria jurídico-penal.

Abordaremos, por fim, o insistente apelo do Direito Penal expansionista quanto à tipificação e criminalização de novas condutas atinentes às transformações sociais emergentes da sociedade da informação.

A hipótese formulada a ser confirmada ou rejeitada é de que a proteção dos bens jurídicos representados pela privacidade e proteção de dados pessoais demandam esforço do Estado brasileiro na elaboração de apropriada legislação adequada a regulamentar a intervenção dos agentes estatais na privacidade e proteção de dados pessoais dos indivíduos em todo o procedimento jurídico-penal, desde seus estágios iniciais da investigação até a execução penal e a reabilitação do condenado.

A inexistência de tal legislação tem sido fonte de preocupação da dogmática constitucional-penal brasileira, de modo que no momento de elaboração deste trabalho, existe em andamento Arguição de Descumprimento de Preceito Fundamental (ADPF) de número 1143, que denuncia ausência de atuação normativa do Congresso Nacional na regulamentação do instituto penal da “infiltração online” no ordenamento jurídico brasileiro, demandando fixação de tese sobre o tema.

Ainda, convém assinalar a escassez de bibliografia brasileira sobre o tema, prejudicando o aprofundamento no pensamento dos pesquisadores e da dogmática nacional, tendo que recorrer a (também escassa) literatura estrangeira. Entretanto, aqui reside o caráter inovador da pesquisa, na identificação de elementos que consideramos

fundamentais para tratativa da dogmática constitucional-penal brasileira e dotados de certa “urgência”, dados os profundos impactos nos valores inerentes ao núcleo essencial da pessoa humana.

Assim, cabe ainda apontar o necessário desenvolvimento do interesse por parte do Poder Legislativo sobre o tema, que deverá se debruçar sem perda de tempo na audiência de especialistas, pesquisadores e da sociedade de modo geral, a fim de elaborar adequada legislação a disciplinar a atuação jurídico-penal do Estado, para que responda aos atuais e futuros desafios do alvorecer da Sociedade 5.0 (e das que virão).

Portanto, restam definidos os objetivos deste trabalho de pesquisa. O objetivo geral foi estudar os bens jurídicos inerentes à privacidade e à proteção de dados pessoais em matéria jurídico-penal. Os objetivos específicos são: recuperar a evolução histórica e jurídica da privacidade; compreender em que medida a privacidade e a proteção de dados pessoais constituem bens jurídicos merecedores de tutela constitucional-penal; comparar a abordagem da proteção de tais bens jurídicos por meio do direito comparado alemão; identificar violações aos bens jurídicos pelo exercício jurídico-penal do Estado; discutir o panorama legislativo nacional aplicado à proteção de dados pessoais; identificar lacunas de proteção eventualmente existentes e propor soluções adequadas e compatíveis com o Estado Democrático de Direito e com os princípios garantistas constitucionais-penais.

A metodologia utilizada para o desenvolvimento deste trabalho inclui pesquisas documentais-jurídicas, pesquisas teóricas e dogmáticas e pesquisas bibliográficas.

Quanto à pesquisa documental-jurídica, foram consultadas legislações nacionais e estrangeiras, seja na forma de Constituição (ou seu equivalente, como no caso da Lei Fundamental alemã) ou na forma de legislação infraconstitucional atinente ao tema. Assim, foi realizada análise crítica de pressupostos teóricos contidos nesses documentos na forma de exegese sistemática.

Foi adotada vertente jurídico-teórica tendo a dogmática alemã como paradigmática, seja em razão de sua experiência pioneira com o tema, seja em razão da relativa proximidade com a dogmática constitucional-penal brasileira.

Definida a vertente jurídico-teórica, a pesquisa documental se fundamentou na dogmática constitucional-penal de tutela dos bens jurídicos identificados sob a forma de direitos fundamentais ou de sua relação com estes.

Ainda, a pesquisa documental adotou viés propositivo-jurídico, a fim de apontar possíveis caminhos para suprir eventual deficiência legislativa no tratamento geral e específico de dados pessoais em matéria jurídico-penal pelo Estado brasileiro e seus agentes.

Na pesquisa bibliográfica foram consultados livros, artigos, periódicos, jornais e demais publicações de caráter científico-jurídico pertinentes ao tema de pesquisa, seja em formato manuscrito físico, seja em formato virtual.

2 PRIVACIDADE E PROTEÇÃO DE DADOS

Mal conseguimos absorver o conceito da Indústria 4.0 e a chamada “sociedade da informação”, e o mundo já se encaminha para a intitulada “Sociedade 5.0”. Nessa transição, a sociedade imergirá em uma *Smart Society* (ou sociedade inteligente, em tradução livre), em que se buscará “integrar elementos tecnológicos em cada processo da sociedade”[1] (Calp; Bütüner, 2022, p. 184).

A Sociedade 5.0 será marcada pela busca da cooperação entre homem e máquina, especialmente no âmbito da Inteligência Artificial e tecnologias relacionadas. Segundo Calp e Bütüner (2022, p. 189), “as novas informações obtidas a partir das sociedades da informação estarão disponíveis para os humanos, mas também compartilharão tais informações com robôs de Inteligência Artificial”[2]. O processo de digitalização e transformação desse novo avanço (ou revolução, para alguns) favorecerá a integração da tecnologia baseada em Inteligência Artificial de maneira que tanto os ativos de IA quanto as próprias pessoas poderão “obter informações fora da área econômica ou de trabalho, em cada *frame* da vida social, e engajarão em mútua cooperação e compartilhamento de informações”[3] (Calp; Bütüner, 2022, p. 189).

Este avanço tecnológico de múltiplas camadas estará disponível não somente para a sociedade civil, mas também para o Estado e seu insaciável apetite por controle. Os impactos sociais produzidos pelas transformações tecnológicas se refletirão, mais tarde ou menos tarde, no Direito, especialmente no Direito Penal, que será demandado a lidar com a regulamentação desse admirável mundo novo, mas com as velhas dificuldades que são carregadas de etapa em etapa, em ciclos de evolução social cada vez mais curtos.

A preocupação já se manifesta na dogmática penal, que classifica o Direito Penal “novo” como diferente do Direito Penal “clássico” em diversos aspectos para lidar com a criminalidade moderna (Hassemer, 1994, p. 3). Esse aspecto “novo” consistiria em um

---

[1] Tradução livre: (…) integrate technological elements into every process of society.
[2] Tradução livre: Society 5.0 will not only make the new information obtained from information societies available to humans, but it will also share this information with AI robots
[3] Tradução livre: AI-based technological assets and people will be able to obtain information outside of the economy/work area, in every frame of social life, and will engage in mutual information sharing and cooperation.

"aguçamento de medidas", especialmente na fase preliminar da persecução penal, a investigação.

Estima-se que haja, no início de outubro de 2024, um total de 5,52 bilhões de pessoas conectadas à internet ao redor do mundo, o que seria equivalente a 67,5 porcento da população total mundial[4][5]. A presença massiva de mais da metade da população mundial na internet e outros meios eletrônicos, a superação do volume de crimes realizados por meios tradicionais pelos realizados por meios virtuais[6] e a evolução tecnológica mundial (tecnologia 5G[7], Internet das Coisas (IoT)[8], tecnologias de vigilância, inteligência artificial[9], dentre outras) são algumas das razões para que os governos de diversos países implementem medidas tecnológicas invasivas à privacidade para o monitoramento, predição, repressão, investigação e persecução penal. A título de exemplo do apetite brasileiro por dados pessoais, já em 2010 o Brasil figurava, segundo o Google, como a nação que mais demandava informações privadas sobre usuários de sua plataforma, seguido pelos EUA[10].

Ainda, a máxima "o recurso mais valioso do mundo não é mais petróleo, mas dados"[11] tem sido amplamente reforçada em todo mundo[12], dado o alto nível de dependência, competitividade e inovação gerada a partir da utilização de dados – dentre eles, principalmente, os dados pessoais. Trata-se do ativo mais valioso do mundo,

---

[4] DATAREPORTAL. **Digital Around the World**. Disponível em: https://datareportal.com/global-digital-overview. Acesso em: 05 jan. 2025.
[5] Tradução livre: A total of 5.18 billion people around the world were using the internet at the start of Q2 2023, which is equivalent to 64.6 percent of the world's total population.
[6] EUROPOL. **The relentless growth of cybercrime**. Disponível em: https://www.europol.europa.eu/media-press/newsroom/news/relentless-growth-of-cybercrime. Acesso em: 12 mai. 2023.
[7] Câmara dos Deputados. **Debatedores defendem rapidez na adoção da tecnologia 5G pelo Brasil**. Disponível em: https://www.camara.leg.br/noticias/751436-debatedores-defendem-rapidez-na-adocao-da. Acesso em: 12 mai. 2023.
[8] STATISA. **Number of Internet of Things (IoT) connected devices worldwide**. Disponível em: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide. Acesso em: 12 mai. 2023.
[9] CARNEGIE. **The Global Expansion of AI Surveillance**. Disponível em: https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847. Acesso em: 12 mai. 2023.
[10] The Register. **Google tool ranks gov appetite for your private data**. Disponível em: https://www.theregister.com/2010/04/20/google_government_request_tool. Acesso em: 12 mai. 2023.
[11] Tradução livre: The world's most valuable resource is no longer oil, but data.
[12] The Economist. **The world's most valuable resource is no longer oil, but data**. Disponível em: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data. Acesso em 15 mai. 2023.

entretanto, o mais vulnerável[13]. Tal realidade associada ao "apagão" de mão-de-obra especializada em segurança da informação[14], crimes informáticos (ou cibernéticos) rompendo todos os índices[15], a generalizada falta de cultura de segurança da informação[16] e o baixo investimento em proteção de dados pessoais no país[17], tem suscitado debates sobre a criminalização de violações à proteção de dados pessoais por meio da elaboração de novos tipos penais.

Recentes estudos indicam um aumento generalizado nos índices relacionados às violações (ou suas tentativas) informáticas, incluindo violações a dados pessoais. Um estudo conduzido pela Universidade de Maryland (EUA) quantificou uma frequência quase constante de ataques realizados em seus computadores com acesso à Internet: em média, um ataque a cada 39 segundos[18]. Ainda, o custo médio de um vazamento de dados atingiu seu pico em 2023, sendo estimado, em média, a US$ 4,45 milhões, um aumento de mais de 15% em relação ao custo médio identificado pelo relatório de 2020[19].

Diante de tantas tentativas em curso a uma frequência quase constante e em escala mundial, uma vez que basta estar conectado à Internet para se tornar um potencial alvo, naturalmente a quantidade de violações tem aumentado com a mesma rapidez. O Relatório de Crimes na Internet[20] do FBI aponta o número de 1.181 de vítimas de crimes pela internet no Brasil no ano de 2022[21], enquanto os EUA possuem o número de

---

[13] TechCrunch+. **Data is the world's most valuable (and vulnerable) resource**. Disponível em: https://techcrunch.com/2021/03/04/data-is-the-worlds-most-valuable-and-vulnerable-resource. Acesso em: 15 mai. 2023.
[14] Forbes. **Why overcoming the Cybersecurity labor shortage matters to company success.** Disponível em: https://www.forbes.com/sites/forbestechcouncil/2023/03/01/why-overcoming-the-cybersecurity-labor-shortage-matters-to-company-success. Acesso em: 15 mai. 2023.
[15] Open Access Government. **Cybercrime is on the rise, is your business prepared?**. Disponível em: https://www.openaccessgovernment.org/cybercrime-is-on-the-rise-is-your-business-prepared/143070/. Acesso em: 15 mai. 2023.
[16] Rewterz. **Security Awareness – Lack of fundamental security knowledge can put your company at risk**. Disponível em: https://www.rewterz.com/articles/security-awareness-lack-of-fundamental-security-knowledge-can-put-your-company-at-risk. Acesso em: 15 mai. 2023.
[17] ZDNET. **Investment in data Privacy in Brazil falls below global average**. Disponível em: https://www.zdnet.com/article/investment-in-data-privacy-in-brazil-falls-below-global-average. Acesso em: 15 mai. 2023.
[18] University of Maryland. **Study: Hackers Attack Every 39 Seconds**. Disponível em: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds. Acesso em: 08 mar. 2024.
[19] IBM. **Cost of a Data Breach Report**. Disponível em: https://www.ibm.com/reports/data-breach. Acesso em: 08 mar. 2024.
[20] Tradução livre: Internet Crime Report.
[21] FBI. **2022 Internet Crime Report.** Disponível em: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. Acesso em: 08 mar. 2024.

479.181 vítimas identificadas. Os números registrados pelo FBI no Brasil, obviamente, são apenas uma pequena parcela do que realmente ocorre no país: subnotificação, dificuldade na obtenção de índices completos, atualizados e classificados pela Administração Pública brasileira sobre os crimes informáticos.

Tal panorama tem provocado reações por parte da sociedade e do Estado em diversos países. Parte dessas reações são devidas ao temor de violações à privacidade. Segundo uma pesquisa realizada nos EUA ainda em 2016[22], 92% dos estadunidenses são preocupados sobre sua privacidade quando usam a internet[23].

A utilização dos dados pessoais de indivíduos por parte do Estado, especialmente em matéria penal (abrangidas aqui a prevenção e monitoramento, repressão, persecução penal e segurança pública), é autorizada em diversos diplomas legais, entretanto, pouca regulamentação foi realizada disciplinando tal utilização. O resultado desse incremento sem limites do apetite do Estado pelos dados pessoais (compreendidos, à luz da definição legal contida na Lei 13.709/2018, como sendo toda informação relacionada à pessoa natural identificada ou identificável) tem sido percebido diariamente nos noticiários, quando identificadas: ações sigilosas por parte do Governo mirando professores e policiais antifascistas[24], fornecimento de software avançado de extração de dados de aparelhos celulares às polícias estaduais em troca de todos os dados apreendidos[25], compra e venda de bases de dados pessoais entre órgãos estatais sem finalidade explícita e definida[26], uso político da Polícia Rodoviária Federal contra

---

[22] TrustArc. **Study Finds More Americans Concerned About Data Privacy Than Losing Their Income**. Disponível em: https://trustarc.com/study-finds-more-americans-concerned-about-data-privacy-than-losing-their-income. Acesso em: 08 mar. 2024.

[23] Tradução livre: (…) 92 percent of American Internet users worrying to some extent about their privacy online (…).

[24] UOL. **Ação sigilosa do governo mira professores e policiais antifascistas**. Disponível em: https://noticias.uol.com.br/colunas/rubens-valente/2020/07/24/ministerio-justica-governo-bolsonaro-antifascistas.htm. Acesso em: 12 mai. 2023.

[25] The Intercept. **As planilhas de Bolsonaro: Ministério da Justiça equipa polícias para vasculhar celulares em troca de dados**. Disponível em: https://theintercept.com/2022/03/21/ministerio-da-justica-equipa-policias-para-vasculhar-celulares-em-troca-de-dados. Acesso em: 12 mai. 2023.

[26] The Intercept. **PRF desrespeita lei e compra base de dados biométricos de todos os motoristas com CNH no Brasil**. Disponível em: https://www.intercept.com.br/2023/05/02/prf-desrespeita-lei-e-compra-copia-da-base-de-dados-biometricos-de-todos-os-motoristas-com-cnh-no-brasil. Acesso em 12 mai. 2023.

transporte de eleitores em dia de votação[27], solicitações de dados e fotos de todas as CNHs do país por parte da ABIN ao SERPRO[28], dentre tantos outros casos de exposição da utilização indevida de dados pessoais.

Naturalmente, as violações à privacidade e proteção de dados pessoais que são consequência de ataques cibernéticos (ou informáticos) possuem maior visibilidade e recebem mais atenção por diversos fatores: escala (quantidade de vítimas) e amplitude (quantidade de dados violados) dos ataques, prejuízos imediatos causados, tensões entre países, são alguns deles. Entretanto, as violações à privacidade e proteção de dados pessoais perpetradas pelo próprio Estado recebem bem menos atenção, por mais que representem potencialmente escala e amplitude assombrosos, tanto em volume de indivíduos e dados quanto em potencial intrusivo dessas violações e medidas de intervenção.

Desta maneira, entendemos como urgente encontrar uma resposta à seguinte questão: é necessária a elaboração de legislação penal específica para proteção de dados pessoais na atividade jurídico-penal do Estado?

2.1 Os conceitos de privacidade e proteção de dados pessoais

A despeito das diversas nuances que envolvem a privacidade, é fundamental buscar compreender os diversos conceitos e o que está abrangido neles para que se entenda, de fato, o que se quer proteger enquanto bem jurídico, em nossa pesquisa, especialmente o penalmente relevante.

Edward Shills (1996, p. 281), ao mencionar alguns dos diversos significados e das diversas aplicações práticas que são invocados à mente que se propõe a analisar privacidade, aponta também os numerosos termos que se relacionam e até mesmo

---

[27] G1. **Mapa de cidades para operações da PRF no 2º turno foi feito por servidor do Ministério da Justiça e incluía todos os estados do Nordeste**. Disponível em: https://g1.globo.com/politica/blog/andreia-sadi/post/2023/04/04/mapa-de-cidades-para-operacoes-da-prf-no-2o-turno-foi-feito-por-servidor-do-ministerio-da-justica-e-incluia-todos-os-estados-do-nordeste.ghtml. Acesso em: 12 mai. 2023.

[28] The Intercept. Documentos vazados mostram que ABIN pediu ao SERPRO dados e fotos de todas as CNHs do país. Disponível em: https://www.intercept.com.br/2020/06/06/abin-carteira-motorista-serpro-vigilancia. Acesso em: 19 ago. 2024.

contrastam com ela: “liberdade, autonomia, publicidade, segredo, confidencialidade, intimidade, e assim por diante”[29].

Um dos grandes desafios da epistemologia contemporânea do tema é precisamente conceituar o que são privacidade e proteção de dados pessoais. Conforme Nissenbaum (2010, p. 67), “o terreno do trabalho teorético em privacidade é vasto, abrangendo disciplinas desde a filosofia à ciência política, política e teoria jurídica, mídia e estudos da informação, e, de modo crescente, ciência da computação e engenharia”[30].

Edwards Shills (1996, p. 281) afirma que “a ideia de privacidade é vaga e difícil de tê-la em uma perspectiva correta”[31] e Richard Parker (1974, p. 275) assinala que “atualmente, não há consenso na literatura legal e filosófica sobre uma definição de privacidade”[32]. Ruth Gavison (1980, p. 422) lamenta em sua obra o espírito diverso da literatura acadêmica a respeito da privacidade quanto a um suposto amplo consenso sobre sua “importância e distinção” obtido por meio de legislação e jurisprudência (norte-americana). Afirma, também, que “comentaristas argumentam que a retórica da privacidade é errônea: quando estudamos os casos nos quais a lei (ou nossas intuições morais) sugere que um ‘direito à privacidade’ foi violado, sempre percebemos que algum outro interesse foi envolvido’”[33].

Alldridge e Brants (2001, p. 20) confirmam tal constatação afirmando que “em casos de conflitos de interesses e direitos, é o direito à privacidade que quase sempre cede”[34]. Westin (1967, p. 7) vai além ao afirmar que “poucos valores tão fundamentais para a sociedade como a privacidade foram deixados tão indefinidos na teoria social ou foram o objeto de tal escrita vaga e confusa pelos cientistas sociais”[35]. Iness (1992, p. 3)

---

[29] Tradução livre: Freedom, autonomy, publicity, secrecy, confidentiality, intimacy, and so forth.
[30] Tradução livre: The landscape of theoretical work on privacy is vast, spanning disciplines from philosophy to political science, political and legal theory, media and information studies, and, increasingly, computer science and engineering.
[31] Tradução livre: The idea of privacy is a vague one and difficult to get into a right perspective.
[32] Tradução livre: Currently, there is no consensus in the legal and philosophical literature on a definition of privacy.
[33] Tradução livre: Commentators have argued that privacy rhetoric is misleading: when we study the cases in which the law (or our moral intuitions) suggests that a "right to privacy" has been violated, we always find that some other interest has been involved.
[34] Tradução livre: (…) in cases of conflicting rights and interests, it is the right of privacy that almost always gives way.
[35] Tradução livre: Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confused writing by social scientists.

chega a afirmar que “explorar o conceito de privacidade remete a explorar um pântano desconhecido. (...) Encontramos intensa discordância sobre questões triviais e cruciais (...)”[36]. Thomson (1975, p. 295) afirma que “talvez a coisa mais impactante sobre o direito à privacidade é que ninguém parece ter qualquer ideia muito clara do que isso seja”[37].

Não por acaso, Solove (2008, p. 1) conclui categoricamente que a “privacidade é um conceito em desarranjo. (...) Filósofos, teóricos legais, e juristas têm frequentemente lamentado a grande dificuldade em atingir uma concepção satisfatória de privacidade”[38]. Para o desespero dos pesquisadores, ao “buscarmos a literatura jurídica e filosófica sobre a privacidade na esperança de ganhar firme apoio, encontramos caos”[39] (Iness, 1992, p. 3). Fazemos coro à constatação de Nissenbaum (2010, p. 67), que afirma que “um ponto no qual parece haver concordância quase unânime é que privacidade é um assunto complexo e confuso”[40].

Este “caos” jurídico-filosófico sobre a definição de privacidade, seu “status” atual, as ameaças às quais está submetida, direitos (mediatos e conexos) que devem ser garantidos e protegidos, é potencializado exponencialmente na abordagem penal da privacidade.

Solove (2008, p. 1) explica que:

> Atualmente, privacidade é um conceito amplo, abrangendo (dentre outras coisas) liberdade de pensamento, controle sobre o corpo de alguém, solidão em sua própria casa, controle sobre informações pessoais, liberdade de vigilância, proteção da reputação, e proteção a partir de pesquisas e interrogatórios.

Doneda (2019, p. 23) adverte que “certas formas de tratamento de nossos dados pessoais podem implicar na perda da nossa autonomia, da nossa individualidade e, ainda, da nossa liberdade”.

---

[36] Tradução livre: Exploring the concept of privacy resembles exploring an unknown swamp. (…) We find intense disagreement about both trivial and crucial issues (…).
[37] Tradução livre: Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.
[38] Tradução livre: Privacy, however, is a concept in disarray. (…) Philosophers, legal theorists, and jurists have frequently lamented the great difficulty in reaching a satisfying conception of privacy.
[39] Tradução livre: (…) we turn to the legal and philosophical literature on privacy in the hope of gaining a foothold. Instead, we find chaos (…).
[40] Tradução livre: One point on which there seems to be near-unanimous agreement is that privacy is a messy and complex subject.

De acordo com Christophe Lazaro (2015), o conceito de privacidade “compreende uma miríade de definições as quais todas requerem em certa extensão algum nível de controle a partir do usuário”[41].

Rubenfeld (1989, p. 750) aponta um representativo número de autores/comentadores que consideram ter o direito à privacidade quando adicionam a palavra “autonomia” ao vocabulário de privacidade. Sendo a autonomia o “direito de fazer escolhas e decisões”, segundo Rubenfeld, a questão é quais escolhas e decisões são protegidas[42]. Aqui parece residir um fundamental ponto de inflexão no tema da privacidade em matéria criminal.

O conceito de privacidade (ou do que se quer proteger da privacidade) varia de acordo com a nação, sua tradição, história e seu momento. Westin (1967, p. 26) reforça que “é importante perceber que diferentes tradições históricas e políticas entre nações contemporâneas criaram diferentes tipos de balanços gerais sociais de privacidade”[43].

Ruth Gavison (1980, p. 428) apresenta um conceito de privacidade que “em seu sentido mais sugestivo, privacidade é uma limitação do acesso de outros a um indivíduo”[44]. Richard Parker (1974, p. 281), de modo semelhante, defende que “privacidade é controle sobre quando e por quem as várias partes de nós podem ser sentidas por outros”[45]. É importante observar que no conceito de limitação do acesso de outros pode perfeitamente ser incluída a limitação do acesso do próprio Estado sobre o indivíduo.

Há uma longa relação de autores que entendem privacidade como uma forma de controle sobre informações sobre si. E sempre que há algum tipo de controle envolvido na vida humana, há uma relação de poder em disputa. Ruth Gavison (1980, p. 427) assinala que “controle sugere que o importante aspecto da privacidade é a condição de

---

[41] Tradução livre: Indeed, the concept of privacy encompasses a myriad of definitions which all require to a certain extent some level of control from the user.
[42] Tradução livre: A number of commentators seem to think that they have it when they add the word "autonomy" to the privacy vocabulary. (…) The privacy doctrine involves the "right to make choices and decisions”. (...) The question, however, is which choices and decisions are protected.
[43] Tradução livre: It is important to realize that different historical and political traditions among contemporary democratic nations have created different types of overall social balances of privacy.
[44] Tradução livre: In its most suggestive sense, privacy is a limitation of others’ access to an individual.
[45] Tradução livre: (…) privacy is control over when and by whom the various parts of us can be sensed by others.

escolher e ver que essa escolha é respeitada”[46]. Enquanto do século 14 ao século 18, “pessoas foram ao juízo por bisbilhotagem ou por terem suas cartas pessoais abertas e lidas, desde o século 19 a ênfase se direcionou para informações pessoais com a mesma intenção que é controlar informações sobre si mesmo”[47] (Holvast, 2008, p. 15)

Buscando descrever melhor os aspectos da privacidade, Westin (1980, p. 31) oferece a descrição de quatro estados básicos da privacidade individual: solidão, intimidade, anonimidade e reserva. No estado de solidão, o indivíduo se encontra separado de grupos, em um estado de diálogo com sua própria consciência, o mais completo estado de privacidade atingível por um indivíduo. Já no segundo estado da privacidade, intimidade, o indivíduo se encontra em um estado relaxado, em uma relação franca com um ou mais indivíduos. Exemplos são o casamento, a familia, amigos etc. O terceiro estado da privacidade, a anonimidade, é atingido quando um indivíduo se encontra em locais públicos, ou realizando atos públicos, mas que ainda busca liberdade de se identificar ou de vigilância. Já a reserva, segundo Westin (1980, p. 32), “o quarto e mais sutil estado da privacidade, é a criação de uma barreira psicológica contra intrusão indesejada”[48].

Tais “estados da privacidade” propostos por Westin se aproximam do conceito elaborado por Hubmann (e das variações elaboradas por outros, como Giesker, Henkel, Hans-Heinrich Maass etc.) sobre a *Sphärentheorie* (ou teoria das esferas, em tradução livre) em que círculos concêntricos delimitam áreas de privacidade, cada qual com sua profundidade, conduzindo a um núcleo da personalidade do indivíduo onde ali se encontra o mais profundo segredo, esfera inviolável, sob pena de violação da própria da dignidade humana.

Já Daniel Solove (2002, p. 1094) subdivide as diferentes concepções de privacidade entre seis tópicos: (1) o direito de ser deixado sozinho; (2) acesso limitado a si; (3) segredo; (4) controle sobre informações pessoais; (5) personalidade; (6)

---

[46] Tradução livre: Control suggest that the important aspect of privacy is the ability to choose it and see that the choice is respected.
[47] Tradução livre: Since the 14th through the 18th century, people went to court for eavesdropping or for opening and reading personal letters. Since the end of the 19th century, the emphasis shifted more toward personal information with the same intention that is, to control one’s own information.
[48] Tradução livre: Reserve, the fourth and most subtle state of privacy, is the creation of a psychological barrier against unwanted intrusion (…).

intimidade[49]. Para a abordagem que seguirá, é importante compreender a advertência de Daniel Solove: esses tópicos frequentemente se sobrepõem, mas ainda assim, cada um possui uma perspectiva distinta sobre a privacidade.

Dentro do direito de ser deixado sozinho (a sós ou em paz, todos sentidos semelhantes), Daniel Solove (2002, p. 1099) menciona o famoso artigo que representa um marco na história da privacidade, *The Right to Privacy*, dos estadunidenses Samuel Warren e Louis Brandeis. O direito de ser deixado a sós abordado por Brandeis e Warren representou, à época, uma maneira de "demonstrar que muitos dos elementos de um direito à privacidade existiam dentro do *common law*"[50]. Mais, representou um protesto pessoal de Warren que constantemente tinha sua intimidade e de sua família exposta nos tabloides e jornais. A inovação tecnológica trazida pela miniaturização das, até então, enormes máquinas fotográficas, despertou a preocupação do que viria a seguir e seus impactos na privacidade dos indivíduos que, "por meio de invasões em sua privacidade, sujeitariam um indivíduo ao estresse e sofrimento mental"[51]. Estudiosos do tema alegaram, posteriormente, que Warren e Brandeis nunca definiram o que é privacidade sendo que, na verdade, colocaram mais esforços em "demonstrar as lacunas existentes no direito *common law*".

Dentro da perspectiva do "limitado acesso ao eu", Daniel Solove (2002, p. 1097), este é o conceito adotado por diversos pesquisadores como sendo uma "formulação mais sofisticada" do direito de ser deixado em paz. Sendo um conceito mais amplo que a mera "solidão" (que também pode ser considerada um componente dos conceitos de limitação de acesso), a limitação do acesso ao "eu" aborda a liberdade de interferência, intrusões e observações indesejadas. É uma perspectiva bastante identificada com o "poder de controle", de limitar a acessibilidade de outros a determinados aspectos da existência do indivíduo de acordo com sua própria vontade.

David O'Brien (1979, p. 15) adverte que "privacidade não é idêntica ao controle sobre o acesso ao eu de alguém, pois nem toda privacidade é escolhida. Alguma

[49] Tradução livre: (1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy.
[50] Tradução livre: demonstrate that many of the elements of a right to privacy existed within the common law.
[51] Tradução livre: Modern enterprise and invention have, through invasions upon his privacy, subjected [an individual] to mental pain and distress (…).

privacidade é acidental, compulsória ou até mesmo involuntária”[52]. A privacidade seria, de acordo com o autor, uma condição da vida e, como tal, não teria conexão necessária com o controle sobre as informações pessoais.

Uma das compreensões mais comuns da privacidade é que ela constitui o “segredo”, a confidencialidade em certas questões. Para Daniel Solove (2002, p. 1106), “o conceito de privacidade como segredo pode ser entendida como um subconjunto do limitado acesso ao eu”[53]. De fato, em diversos contextos, a percepção de que uma vez que uma informação ou um dado não seja mais completamente um segredo, ela não pode mais ser privada, representando uma associação direta e dependente entre segredo e privacidade. Entretanto, diversos autores enfatizam que “compreender privacidade como segredo conceitua privacidade de maneira muito estreita”[54]. Não é difícil perceber que a divulgação de segredos representa uma violação à privacidade, entretanto, nem toda violação à privacidade envolve a divulgação de segredos ou quebra de confidencialidade.

O quarto aspecto da privacidade abordado por Daniel Solove é o “controle sobre informações pessoais”, sendo essa uma das teorias mais predominantes da privacidade. De fato, Alan Westin (1967, p. 7) em sua clássica obra *Privacy and Freedom* já apresentava o conceito de que “privacidade é a demanda de indivíduos, grupos, ou instituições em determinar para si mesmos quando, como, e com qual extensão as informações sobre si são comunicadas a outros”[55].

Atualmente, enorme parte da discussão sobre o tema da privacidade e proteção de dados pessoais se concentra precisamente nas informações pessoais (ou dados pessoais) e a autonomia dos indivíduos sobre elas, bem como o adequado tratamento dessas informações e suas possíveis violações. Entretanto, como se pode perceber, o tema da proteção de dados pessoais é uma nuance da privacidade, que envolve outras matizes incompatíveis com a própria natureza do conceito aplicado a “dados” (como, por

---

[52] Tradução livre: Privacy is not identical with control over access to oneself, because not all privacy is chosen. Some privacy Is accidental, compulsory, or even involuntary.
[53] Tradução livre: The privacy-as-secrecy conception can be understood as a subset of limited access to the self.
[54] Tradução livre: A number of theorists have claimed that understanding privacy as secrecy conceptualizes privacy too narrowly.
[55] Tradução livre: Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.

exemplo, o respeito ao desejo da limitação do indivíduo de determinado convívio com outros ou da autonomia personalíssima em decisões sobre si – como se casar ou ter filhos).

Este conceito enfatiza o "controle", o poder sobre o fluxo de informações de si, representando em boa parte a relação com a autodeterminação informacional (que abordaremos em nosso trabalho). As situações envolvendo violações à privacidade do controle de informações acarretam precisamente a "perda" desse controle como, por exemplo, quando há a gravação oculta de conversa entre particulares ou acesso a sistemas com obtenção de dados pessoais (um diário, anotações, e-mails etc.). Uma vez que haja a obtenção dessas informações (seja na forma de áudio, vídeo ou dados), perde-se o "controle" que se tinha sobre eles. Entretanto, considerar somente este aspecto estreitaria bastante o conceito de privacidade. Richard Parker (1974, p. 281), por exemplo, defende o conceito de privacidade como "o controle sobre quando e por quem as várias partes de nós podem ser sentidas por outros"[56]. O autor explica que o "sentir" representa simplesmente o ver, ouvir, tocar, cheirar ou provar (o gosto), o que não seria uma aplicação prática ao conceito de informações e dados.

O quinto aspecto abordado por Daniel Solove (2002, p. 1116) é a personalidade. Solove assinala que o termo personalidade se refere a "aqueles atributos de um indivíduo que são irredutíveis em sua individualidade"[57]. A privacidade de uma pessoa protege os aspectos de dignidade de autonomia, centrais para a liberdade tutelada pela Décima Quarta emenda constitucional dos Estados Unidos.

Na demanda intitulada "*Planned parenthood of Southeastern Pa. v. Casey*"[58], a Suprema Corte estadunidense elaborou o que a privacidade protegida pelo direito constitucional à privacidade abrangia, assinalando que "no coração da liberdade está o direito de o indivíduo definir seu próprio conceito de existência, de sentido, do universo, e do mistério da vida humana"[59]. Assim, a Suprema Corte materializou a proteção da

[56] Tradução livre: The definition of privacy defended in this article is that privacy is control over when and by whom the various parts of us can be sensed by others.
[57] Tradução livre: (…) those attributes of an individual which are irreducible in his selfhood.
[58] U.S. Supreme Court. **Planned Parenthood of Southeastern Pa. v. Casey, 505 U.S. 833 (1992)**. Disponível em: https://supreme.justia.com/cases/federal/us/505/833. Acesso em: 17 ago. 2024.
[59] Tradução livre: At the heart of liberty is the right to define one's own concept of existence, of meaning, of the universe, and of the mystery of human life.

privacidade como “a não interferência do Estado em certas decisões que são essenciais para definir a personalidade”[60]. O direito à personalidade será abordado ao longo do nosso trabalho, entretanto, a partir da experiência europeia, especialmente a alemã.

O sexto e último aspecto da privacidade abordado por Daniel Solove (2002, p. 1121) é a intimidade. Temos um especial interesse neste aspecto pois a intimidade é um bem jurídico constitucional, especial direito elevado a direito fundamental disposto na Constituição brasileira em seu art. 5º, X, dotado de inviolabilidade.

Existem diferentes correntes de pensamento a respeito do conceito desse bem jurídico, representação para o indivíduo e seu escopo de proteção. Daniel Solove (2002, p. 1121) afirma que “essa teoria reconhece apropriadamente que privacidade não é apenas essencial para o autodesenvolvimento do indivíduo, mas também para relações humanas”[61]. Assim, para parte dos pesquisadores, a intimidade tem direta relação com os aspectos de confidencialidade e o controle sobre o fluxo de informações pessoais sobre si, “localizando o valor da privacidade no desenvolvimento de relações pessoais”[62].

Esse bem jurídico é apresentado em vários momentos por uma dualidade que aparentemente é indissociável: intimidade e vida privada. O texto constitucional confere inviolabilidade à intimidade, à vida privada, à honra e à imagem das pessoas, apresentando alguns componentes da privacidade que se relacionavam entre si de acordo com o entendimento do constituinte.

Uma parte dos autores defendem um conceito plural do direito à intimidade e à vida privada, dotado de ampla imprecisão e generalidade, muitas vezes recorrendo a uma formulação taxonômica (como Daniel Solove e Alan Westin, por exemplo). José Adércio Leite Sampaio (1998, p. 218) assinala que nesta categoria se encontram também aqueles que se negam a conferir valor a esses conceitos e até mesmo aqueles que entendem que sequer deve se formular tais conceitos em razão de impingir-lhes “muito mais uma função desagregadora no âmbito social do que protetora de interesses, pessoal ou coletivo, relevantes”.

---

[60] Tradução livre: (…) state’s noninterference in certain decisions that are essential to defining personhood.
[61] Tradução livre: This theory appropriately recognizes that privacy is not just essential to individual self-creation, but also to human relationships.
[62] Tradução livre: (…) it locates the value of privacy in the development of personal relationships.

Para outros autores e pesquisadores, o direito à vida privada e à intimidade é de base conceitual única, “embora possa transparecer como um direito de múltiplas faculdades, com incursões em diversos domínios” (Sampaio, 1998, p. 230). Entretanto ainda aqui permanece difícil encontrar essa base conceitual consensual. Nesse viés, José Adércio Leite Sampaio assinala que “não se pode, *a priori* [grifo do autor], conceituar, em toda a sua extensão e plenitude, intimidade e vida privada. Seus contornos exatos só podem ser aferidos, levando em conta suas peculiaridades e o contexto de cada caso concreto”.

Já Vânia Siciliano Aieta (1999, p. 101), por sua vez, manifesta opinião contrária, considerando que “a questão de maior importância acerca da conceituação do direito à intimidade se constrói em relação à demanda fundamental de estabelecer as fronteiras e as diferenças conceituais de privacidade, intimidade, reserva e segredo”. Entretanto, reconhece a autora, “várias tentativas existiram, com o propósito de discernir as diferentes graduações da privacidade”, assumindo uma equivalência entre os conceitos apresentados.

José Laércio Araújo (2000, p. 50) afirma que a doutrina unitária é de origem alemã e que “considera a existência de um único direito da personalidade e não de ‘direitos da personalidade’”. De outro lado, afirma Araújo, a doutrina pluralista é de origem italiana, também adotada pelo direito anglo-saxônico, e que “se contrapõe à teoria da unificação dos bens personalíssimos tutelados, ante à diversidade de características de que se reveste cada um e, ainda, aos variados mecanismos de defesa para a sua tutela”.

Paulo José da Costa Junior (2004, p. 13), ao declamar a lentidão do legislador que avança com o passo trôpego, mais lentamente que os fatos sociais “que evoluem vertiginosamente, reivindicando normas e providências”, afirma que “surgem assim valores novos, que vão avante das leis, desprotegidos, a reclamar tutela”. Curiosamente, Costa Junior assinala que “dentre esses novos valores, que estavam a merecer tutela pronta e urgente do direito, sobressai a intimidade”. Talvez o célebre penalista estivesse a mencionar o período imediatamente anterior ao reconhecimento da intimidade (e da vida privada) como direito fundamental na Constituição de 1988, entretanto, como abordado neste trabalho, a intimidade (a privacidade, de modo geral) tem raízes bem mais profundas na história.

Distingue, Costa Junior (2004, p. 14) a intimidade entre intimidade interior e exterior, sendo interior a revestida de “natureza física e material”, o recolhimento do indivíduo “em seu castelo”; e exterior a de natureza psíquica, estando alheio à multidão “em pleno tumulto coletivo”.

Um aspecto interessante trazido por Paulo José da Costa Junior (2004, p. 21) é sua adoção do termo “privatividade” ao invés do amplamente adotado termo “privacidade”. Justifica-se Costa Junior ao anotar que “a expressão exata, em bom vernáculo, é privatividade, que vem de privativo. E não privacidade, que é péssimo português e bom anglicismo (vem de *privacy* [grifo do autor])”.

Renné Ariel Dotti (1980, p. 67) aborda a distinção entre intimidade e vida privada: “a construção de um direito à intimidade como círculo mais restrito do direito à vida privada é tipicamente francesa e provém da necessidade em se precisar um núcleo mais profundo ao qual foi dada proteção pela Lei de 17.7.1970, em França”. Para o autor, “é preciso desde logo acentuar que os conceitos de ‘vida privada’ e ‘intimidade’ não são coincidentes” (Dotti, 1980, p. 68).

Miguel Urabayen (1977, p. 149), ao analisar a jurisprudência francesa da época, encontra certa dificuldade em diferenciar um conceito do outro, concluindo que:

> O que nos confirma em nossa ideia que se os conceitos não são exatamente iguais – um é um círculo concêntrico e de menor raio que o outro – sua prévia diferenciação legal pode oferecer dificuldades tão amplas como de pouca transcendência posto que a linha protetora está já situada no círculo exterior.[63]

A dificuldade em analisar tais diferenças e semelhanças também é notada por José Serpa de Santa Maria (1994, p. 162), que destaca a acentuação “de uma maneira geral, os juristas, a espinhosa tarefa de definir um direito ainda não suficientemente delimitado. Tal terreno ainda movediço, inçado de obstáculos e de dissidências, sobretudo em seu conteúdo e fronteiras, tem gerado certa perplexidade”.

Concorda Edson Ferreira da Silva (1998, p. 31), ao afirmar que “todos temos noção, mais ou menos coincidente, do que respeita a nossa intimidade. No entanto,

---

[63] Tradução livre: Lo que nos confirma en nuestra idea que si los conceptos no son exactamente iguales – uno es un círculo concéntrico y de menor radio que el otro – su previa diferenciación legal puede ofrecer dificultades tan amplias como de poca transcendencia, puesto que la línea protectora está ya situada en el círculo exterior.

dificuldades quase insuperáveis se apresentam para a definição do direito e precisão do seu conteúdo".

Conclui, brilhantemente, José Adércio Leite Sampaio (1998, p. 236):

> Estamos a falar assim de um conceito relativo, mutável, contextual e conseguintemente impossível de assunção em um único lance de todas as suas fronteiras normativas como instituto formal irretocável. Esse relativismo se patenteia no próprio sentido do que cada pessoa pode, diferentemente das demais e até de si mesma no curso de sua vida, conceber como íntimo ou privado, a partir das influências que decisivamente sofra de fatores culturais, religiosos, políticos, filosóficos e até mesmo climáticos, sem se esquecer de que as próprias circunstâncias, ou um dado momento existencial, podem permitir acepções até então não cogitadas.

Analisando o tema das biografias no Brasil e sua relação com diversos outros institutos e direitos, Eduardo Lasmar Prado Lopes (2015, p. 150) faz coro ao afirmar que:

> O conceito de privacidade e de intimidade varia no tempo e no espaço. Assim como o conceito se volatilizou em 1800 para 1950, os limites e significados desses direitos fundamentais, certamente não encerram a mesma definição, nos dias atuais, do que em 1950. Provavelmente, no futuro, esse significado também será alterado de acordo com as novas cosmovisões da sociedade.

Daí se compreende a extrema dificuldade dos pesquisadores em "encaixar" a privacidade em um conceito de fronteiras estanques, imutavelmente delimitadas. Essa dificuldade também se apresenta como um desafio à teoria do bem jurídico, uma vez que seus críticos questionam, dentre outros, sua adaptabilidade às questões contemporâneas e futuras, como presente na crítica de Christoph Burchard (2012, p. 36):

> O denominador comum da doutrina do bem jurídico – melhor dizendo das teorias do bem jurídico – é seu absolutismo ou sua estreita relação com um resultado binário absoluto (bem jurídico ou nenhum bem jurídico). A doutrina do bem jurídico permite e possibilita estabelecer limites absolutos entre punibilidade e não punibilidade, ainda que estes limites absolutos sejam muito difíceis de atingir em uma sociedade democrática e pluralista. Na estrutura argumentativa da doutrina do bem jurídico propriamente não existem zonas cinzas, já que quando surgem, se usam outros princípios auxiliares, por exemplo, o princípio *in dubio pro libertate*.

Não é o propósito deste trabalho a defesa ou a crítica da teoria do bem jurídico, entretanto, como uma breve justificação da adoção dessa teoria como marco teórico,

precisamente por sua segurança após mais de um século de seu desenvolvimento e sujeições às críticas mais diversas e severas, e pela sua ampla comunicabilidade com o ordenamento jurídico (ao se relacionar com outros institutos e princípios jurídicos, por exemplo), encontramos razões suficientes para adotá-la em nossa fundamentação.

2.2 As origens do conceito de privacidade e proteção de dados pessoais

Apesar do conceito de privacidade nos tempos atuais ter uma ligação mediata com o tema da proteção de dados pessoais em uma economia de (ou baseada na exploração de) dados e uma percepção da privacidade como um desejo distintivamente humano, "há estudos sobre o comportamento animal e organização social que sugerem que a necessidade humana por privacidade pode encontrar raízes em sua origem animal"[64] (Westin, 1967, p. 8). Jan Holvast (2008, p. 15), por sua vez, reflete que "humanos sempre tiveram uma necessidade por privacidade"[65], sendo que que "a discussão sobre privacidade é primariamente uma discussão política sobre a maneira que um indivíduo distinto e os interesses da sociedade podem ser equilibrados"[66].

Moore (2019), ao apontar a origem do "Público" em uma abordagem de estudos antropológicos, descreve da vida do Esquimó como a "reação ambivalente a obrigações sociais, especialmente a obrigação de compartilhar comida e utensílios". Segundo o autor, "na superfície tudo é harmonia e cooperação. Abaixo da superfície há uma considerável carga de irritação". Complementa, ainda, que a "privacidade, portanto, aparece como um escape de demandas e fardos da interação social"[67].

Na história antiga, a questão da privacidade já ocupava os manuscritos dos filósofos gregos, incluindo Sócrates, na distinção realizada entre o "exterior" e o "interior", entre o público e o privado, entre a sociedade e a solidão. Flaherty (1972, p. 45), em seus

---

[64] Tradução livre: Yet studies of animal behavior and social organization suggest that man's need for privacy may well be rooted in his animal origins (…).
[65] Tradução livre: Humans have always had a need for privacy.
[66] Tradução livre: (…) the discussion on privacy primarily is a political discussion about the way the distinct individual and societal interests can be balanced.
[67] Tradução livre: The most prominent theme to emerge from the description of Eskimo life is the ambivalent reaction to social obligations, especially the obligation to share food and utensils. On the surface all is harmony and cooperation. Beneath the surface there is a considerable charge of resentment. Privacy thus appears as an escape from the demands and burdens of social interaction.

estudos sobre a privacidade na Nova Inglaterra colonial (em um período que vai aproximadamente de 1650 a 1750), afirma que “o primeiro local onde os colonialistas procuraram privacidade foi nos confins do lar (...)”[68]. Jan Holvast (2009, p. 15) reafirma que, “ainda hoje, o lar é visto daquele modo, já que o lar é um castelo pessoal (...)”[69].

Tal afirmação, de que o lar de um homem é seu castelo (e, consequentemente, deve ter sua “privacidade” respeitada e protegida), se faz presente em diversos autores que discorrem sobre a história da privacidade (*privacy*) e é oriunda da *common-law*, mais precisamente a partir do julgamento “*Semayne Case*”, em 1604, que impedia a entrada de um xerife local na propriedade de um cidadão que deveria ter sua dívida “executada”[70]. Joseph Story (1833, p. 843), em seus “Comentários sobre Constituição dos Estados Unidos”[71], a respeito da provisão 1893 da Constituição daquele país, afirma que “seu objeto simplesmente é assegurar o perfeito gozo daquele grandioso direito da *common law* de que a casa de um homem deve ser seu próprio castelo, protegida contra toda intrusão civil e militar”[72]. De fato, a Emenda nº 4 de 15 de dezembro de 1791 da Constituição Estadunidense estabelece que “o direito das pessoas de estarem seguras em suas pessoas, casas, documentos e bens, contra buscas e apreensões injustificadas, não deve ser violado (...)[73].

Segundo Rodotá (2008, p. 26), entretanto, “o nascimento da privacidade pode ser historicamente associado à desagregação da sociedade feudal”. Nessa organização social, o isolamento era um privilégio destinado a muito poucos (ou lhe era imposto a algumas classes como os monges ou bandidos). Assim, ainda segundo Rodotá, “a privacidade configura-se assim como uma possibilidade da classe burguesa, que consegue realizá-la sobretudo graças às transformações sócio-econômicas [sic] relacionadas à Revolução Industrial”, posição corroborada por Danilo Doneda (2020, p. 118) ao afirmar que a privacidade passa a ser uma prerrogativa de uma emergente classe

---

[68] Tradução livre: Within the confines of the home, the primary place where colonists sought privacy (…).
[69] Tradução livre: The home is still seen in that way since the home is a personal castle (…).
[70] The house of everyone is to him his castle and fortress, as well as his defense against injury and violence, as for his repose. Semayne’s Case, 5 Co. Rep. 91b 77 Eng. Rep. 195.
[71] Tradução livre: Commentaries on the Constitution of the United States.
[72] Tradução livre: Its plain object is to secure the perfect enjoyment of that great right of the common law, that a man’s house shall be his own castle, privileged against all civil and military intrusion.
[73] Tradução livre: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.

burguesa, tendência acelerada pelo fim da sociedade feudal e, posteriormente, pela Revolução Industrial. Doneda (2020, p. 119), ainda, aponta uma “concepção de privacidade associada diretamente à proteção da propriedade, preponderante na época”. Assim, continua o autor, o direito de propriedade seria condição inafastável para chegar à privacidade.

O sentido da própria expressão “propriedade privada” traz a tônica da relação de poder e domínio sobre “a coisa” ou “o ente”. José Adércio Leite Sampaio (1998, p. 30) ensina que “a doutrina romana da propriedade absoluta assegurava ao *dominus* inúmeras e amplas faculdades, dentre as quais o direito de, em seus limites, desenvolver uma vida secreta, distante da curiosidade alheia”. Possuindo características de direito real, sua proteção contra a violação do isolamento que queria preservar era *erga omnes*.

O debate da propriedade enquanto direito de autor e direito à imagem na forma de espécies do direito à propriedade foi vívido até que a elaboração jurisprudencial e doutrinária da segunda metade do Século XIX direcionasse o direito à imagem para uma proteção da individualidade, que tomaria em pouco tempo a feição dos direitos de personalidade. Ainda, Ricardo Campos (2021, p. 16), prefaciando a obra de Carissa Véliz (Privacidade é Poder), lembra que “a decisão do censo alemão de 1983 distanciou-se da privacidade ou proteção de dados como expressão eminentemente advinda do direito de propriedade, apoiando-se fortemente em aspectos de indisponibilidade advindos do direito da personalidade”.

A abordagem da privacidade e proteção de dados pessoais em matéria penal proposta neste trabalho a partir da teoria do bem jurídico tem por objetivo aproveitar uma base sólida no Direito Penal atual para estruturar os princípios que guiarão a atividade estatal na persecução e execução penal, competências que possui o monopólio em decorrência de reserva de jurisdição.

2.3 O direito da privacidade como manifestação do direito à personalidade e direito humano

Vários são os autores que remetem o direito à privacidade como um desdobramento do direito geral da personalidade. A origem dos direitos da personalidade

não encontra consenso entre os estudiosos e pesquisadores. Alguns situam sua origem na antiguidade, especialmente na Grécia com as *dike kakegiorias* ou em Roma, com a *actio injuriarum.* Outros autores situam sua origem na Idade Média, a partir da busca do homem pelo sobrenatural e o culto da espiritualidade. Ainda, há os que situem a origem nos séculos XIX e XX (Sampaio, 1998, p. 40).

Stolze (2022, p. 119) conceitua os direitos de personalidade como “aqueles que têm por objeto os atributos físicos, psíquicos e morais da pessoa em si e suas projeções sociais”. Bittar (2015) ensina que os direitos da personalidade são “reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos no homem, como a vida, a higidez física, a intimidade, o segredo, o respeito, a honra, a intelectualidade e outros tantos”.

Tais direitos de personalidade são, assim como os direitos reais, absolutos e oponíveis *erga omnes* (Dotti, 1980, p. 25). Os direitos da personalidade tinham pouco tratamento normativo, sendo que “o reconhecimento solene do direito à vida privada, com projeção autônoma dos demais direitos da personalidade, é relativamente recente” (Dotti, 1980, p. 27). A atenção devida a esse novo leque de direitos somente se deu a partir da Segunda Guerra Mundial, conforme diversos autores apontam.

René Dotti (1980, p. 27) ressalta a “preocupação internacional após a revolução tecnológica do ocidente, especialmente após a 2ª Guerra Mundial”. De modo concordante, apesar de Rodotá situar as bases da privacidade moderna na transição feudal-industrial como um privilégio da classe burguesa, vários autores localizam as raízes da discussão geral sobre a privacidade (*privacy*), especialmente nos Estados Unidos, se iniciando logo após a Segunda Guerra Mundial[74] (Holvast, 2008, p. 15).

Bittar (2015) afirma que “foi sob a égide da doutrina alemã e, depois, da suíça que se cogitou do enunciado de regras gerais sobre direitos da personalidade (...). Na Alemanha, ao passo que “entendia-se que a proteção da personalidade era suficientemente resguardada pelos direitos da personalidade expressos pela lei (Zanini, 2017, p. 12) que tratava Direitos de Autor em Obras de Artes Plásticas e Fotografia, a

[74] Tradução livre: The general discussion on privacy started shortly after the Second World War in the United States.

KUG (*Kunsturhebergesetz*), não havia um reconhecimento jurisprudencial alemão ao direito geral de personalidade. De fato, segundo Bittar (2015), "no BGB[75] (de 1896), reconheceu-se o direito ao nome (§12) e impôs-se a obrigação de reparação do atentado contra a pessoa (§823), textos que têm sido vistos como aceitação dos direitos da personalidade, mas ainda não suficientemente definidos".

Ao fim da Segunda Guerra Mundial, com a vigência da Lei Fundamental de Bonn, em 23 de maio de 1949, como reação aos abusos cometidos pelo Nazismo, a dignidade da pessoa humana e o livre desenvolvimento da personalidade (art. 1, 1 e art. 2, 2) passaram a constituir valores centrais na nova ordem jurídica alemã (Zanini, 2017, p. 20). Pouco tempo depois, o BGH (*Bundesgerichtshof*) alemão proferiu sua primeira decisão reconhecendo o direito geral de personalidade no célebre caso *Leserbrief* de 1954 e no caso *Herrenreiter* de 1958 (Zanini, 2021, p. 93).

De fato, Schwabe (2005, p. 674) confirma que:

> O direito fundamental à inviolabilidade do domicílio, enquanto direito clássico de liberdade (negativa), outorga ao seu titular (qualquer pessoa natural, nacional ou estrangeira submetida ao poder estatal alemão) o direito de resistir à intervenção do Estado em sua esfera "espacial" de privacidade (domicílio), tão necessária ao livre desenvolvimento da personalidade (daí sai relação de especialidade em face do direito geral de personalidade tutelado pelo Art. 2 I GG, que tem com um de seus principais desdobramentos o direito à privacidade como elemento de auto-preservação *(sic)* do seu titular).

Ainda, Schwabe (2005, p. 866) menciona que:

> No ano de 1958, o Tribunal Federal (BGH) concedeu pela primeira vez, na decisão (*Urteil*) assim denominada "*Herrenreiter*", indenização de pequeno valor em dinheiro ao atingido em seu direito da personalidade em razão de dano não patrimonial (BGHZ 26, 349). Na fundamentação, que se liga à decisão de 1954 (BGHZ 13, 334), discorre-se que dos Art. 1 e 2 GG decorreria, não apenas a obrigação de se respeitar a personalidade: deles resultaria a necessidade de garantir a proteção, em intervenções na esfera pessoal, contra danos próprios da essência [da personalidade].

É possível depreender que, portanto, a jurisprudência alemã dos tribunais cíveis admite indenizações por danos imateriais (morais) nos casos de violações graves ao

[75] BGB: *Bûrgerliches Gesetzbuch*. O Código Civil alemão.

direito geral da personalidade, sendo compatível, conforme Schwabe (2005, p. 866) com a Constituição daquele país (*Grundgesetz*).

Na história dos direitos da personalidade da Itália, Bittar (2005) opina que "a melhor definição da matéria ecoou no Código Civil italiano de 1942". Adriano de Cupis (2008, p. 28) afirma que "o Código Civil italiano vigente deu-lhes uma parcial disciplina". Entretanto, os direitos da personalidade estão dispostos na Constituição do Estado Italiano considerados como direitos invioláveis do homem (Cupis, 2008, p. 28). Zanini (2021, p. 96) afirma que "há autores defendendo que a Constituição italiana teria mudado substancialmente esse quadro, reconhecendo, em seu art. 2º, uma cláusula geral de tutela da pessoa humana".

Também de difícil sistematização é a distinção entre os direitos da personalidade e os direitos humanos. Segundo Ramos (2014, p. 19), "os direitos humanos consistem em um conjunto de direitos considerado indispensável para uma vida humana pautada na liberdade, igualdade e dignidade". Sua "fundamentalidade" pode ser formal, na medida que esses direitos sejam inscritos no rol de direitos protegidos pelas Constituições ou tratados internacionais, ou material, sendo considerados em si mesmos, ou seja, integrantes dos direitos humanos que, ainda que não estejam expressos, são indispensáveis para a promoção da dignidade humana (Ramos, 2014).

De fato, a Declaração Universal dos Direitos Humanos foi adotada em 10 de dezembro de 1948 pela Assembleia Geral das Nações Unidas[76] e seu artigo 12 contempla a proteção à privacidade como direito humano: Ninguém será sujeitado a interferência arbitrária em sua privacidade, família, lar ou correspondência, nem a ataques sobre sua honra e reputação. Todos têm o direito à proteção da lei contra tais interferências ou ataques[77].

Percebe-se que os horrores da guerra demandaram um pós-guerra focado na proteção da humanidade, seus direitos essenciais, e esta mesma época impulsionou tanto o desenvolvimento dos direitos da personalidade quanto dos direitos humanos.

---

[76] United Nations. **Universal Declaration of Human Rights**. Disponível em: https://www.un.org/en/about-us/universal-declaration-of-human-rights. Acesso em: 01 mai. 2024.

[77] Tradução livre: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Eduardo Ustaran (2018, p. 4) afirma que “a Declaração dos Direitos Humanos nasceu após as atrocidades da Segunda Guerra Mundial e confirmou o que agora se tornou valores universais e tradições (...)”[78].

Pouco depois, em 1950, na cidade de Roma[79], o Conselho da Europa convidou seus estados para assinar a Convenção Europeia de Direitos Humanos (*European Convention on Human Rights* – ECHR), sendo um tratado internacional para proteção de direitos e liberdades fundamentais (Ustaran, 2018, p. 5). Esta convenção, assim como a Declaração Universal dos Direitos Humanos, reconhece o direito ao “respeito pela vida privada e familiar” em seu Artigo 8[80]. Outros instrumentos foram elaborados na Europa posteriormente, entretanto, detalharemos o assunto quando abordarmos o tema da proteção de dados pessoais.

São diversos os termos envolvendo direitos humanos utilizados na Constituição brasileira. São utilizados “direitos humanos”, “direitos e garantias fundamentais”, “direitos e liberdades fundamentais”, “direitos e liberdades constitucionais”, “direitos e garantias fundamentais”, dentre outros. No Direito Internacional, como recorda Ramos (2014), há diversas locuções, inclusive da expressão “direitos fundamentais”, ao tratar dos direitos humanos.

Os autores, em sua maioria, tendem a compreender os direitos humanos como os direitos “estabelecidos pelo “*Direito Internacional em tratados e demais normas internacionais* [grifo do autor]”. Já a expressão “direitos fundamentais” se referiria os direitos “*reconhecidos e positivados pelo Direito Constitucional* [grifo do autor] de um Estado específico” (Ramos, 2014). Entretanto, em razão da evolução conceitual do tema, há, atualmente, uma união de termos em razão de uma “*aproximação e mútua relação entre o Direito Internacional e o Direito interno na temática dos direitos humanos* [grifo do autor]” e a consequente gradual perda da importância dessa distinção.

Bittar (2015), por sua vez, distingue os “direitos do homem” (expressão atualmente bastante criticada em razão de seu caráter sexista) ou “direitos fundamentais” (ou seja, o

---

[78] Tradução livre: The Human Rights Declaration was born following the atrocities of World War II and acknowledged what have now become universal values and tradition (…).
[79] European Court of Human Rights. **European Convention on Human Rights**. Disponível em: https://www.echr.coe.int/european-convention-on-human-rights. Acesso em: 01 mai. 2024.
[80] European Court of Human Rights. **European Convention on Human Rights**. Disponível em: https://www.echr.coe.int/documents/d/echr/Convention_ENG. Acesso em: 01 mai. 2024.

autor aborda os dois termos de maneira equivalente, intercambiável) dos “direitos da personalidade”. Os direitos do homem ou fundamentais da pessoa natural seria objeto da relação do indivíduo com o Estado, enquanto os direitos da personalidade seriam destinados a proteção da pessoa natural na relação com os particulares (Bittar, 2015).

Nos parece inadequada essa distinção em razão, especialmente na abordagem deste trabalho, da proteção da privacidade (e suas diversas faces como a intimidade, o segredo etc.) do indivíduo com relação ao Estado, em uma relação assimétrica de poder que é tão ou mais merecedora de proteção quando comparada à proteção do indivíduo em relação ao particular, especialmente aquele que se encontra sob completa entrega à tutela estatal, o indivíduo condenado à pena privativa de liberdade.

O Brasil, por meio do Decreto nº 592, de 6 de julho de 1992, aderiu ao Pacto Internacional dos Direitos Civis e Políticos, que teve seu Protocolo Facultativo promulgado por meio do Decreto nº 11.777, de 9 de novembro de 2023. O Pacto Internacional dos Direitos Civis estabelece, em seu artigo 17, item 1, que “ninguém poderá ser objeto de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação” e, no item 2, que “toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas”[81]. Tal Pacto foi adotado pelas Assembleia Geral das Nações Unidas em 16 de dezembro de 1966 e adquiriu vigência em 23 de março de 1976. Em maio de 2012, o Pacto havia sido ratificado por 176 países[82].

[81] BRASIL. **DECRETO Nº 592, DE 6 DE JULHO DE 1992.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em 05 mai. 2024.
[82] Council of Europe. **The International Covenant on Civil and Political Rights**. Disponível em: https://www.coe.int/en/web/compass/the-international-covenant-on-civil-and-political-rights. Acesso em: 05 mai. 2024.

3 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS ENQUANTO BENS JURÍDICOS CONSTITUCIONAIS-PENAIS

Inicialmente, é importante abordar, ainda que brevemente, aspectos distintivos entre os conceitos de privacidade e de proteção de dados pessoais. Conforme o órgão supervisor europeu de proteção de dados (EDPS – *European Data Protection Supervisor*)[83], "privacidade e proteção de dados, embora conectados, são comumente reconhecidos em todo o mundo como dois direitos separados"[84]. Assim, na União Europeia, "a dignidade humana é reconhecida como um direito fundamental absoluto. (...) Privacidade não é apenas um direito individual, mas também um valor social"[85].

Já a proteção de dados[86], ainda segundo o EDPS, "é sobre proteger qualquer informação relacionada a uma pessoa natural (viva) identificada ou identificável, incluindo nomes, datas de nascimento, fotografias, imagens de vídeo, endereços de e-mail e números de telefone"[87]. Enquanto o direito à privacidade ou à vida privada é consagrado na Declaração Universal dos Direitos Humanos e reconhecido como um direito humano universal, a proteção de dados pessoais ainda não o é, por mais que seja reconhecido como direito fundamental (assim como a privacidade) nos tratados da União Europeia e na Carta de Direitos Fundamentais da União Europeia.

De acordo com Kokott e Sobotta (2013, p. 223), "enquanto a Constituição dos EUA não menciona explicitamente privacidade ou proteção de dados, proteção de ambos os direitos é explicitamente estabelecida no nível constitucional na Europa (...)"[88]. Os autores ainda concluem que as provisões legais europeias permitem observar que "estes dois direitos não são completamente sinônimos" e que "apesar dessa distinção

---

[83] European Data Protection Supervisor. **Data Protection**. Disponível em: https://www.edps.europa.eu/data-protection/data-protection_en. Acesso em: 21 dez. 2024.
[84] Tradução livre: Privacy and Data Protection, though connected, are commonly recognized all over the world as two separate rights.
[85] Tradução livre: In the EU, human dignity is recognized as an absolute fundamental right. (…) Privacy is not only an individual right but also a social value.
[86] European Data Protection Supervisor. **Data Protection**. Disponível em: https://www.edps.europa.eu/data-protection/data-protection_en. Acesso em: 21 dez. 2024.
[87] Tradução livre: Data protection is about protecting any information relating to an identified or identifiable natural (living) person, including names, dates of birth, photographs, video footage, email addresses and telephone numbers.
[88] Tradução livre: While the US Constitution does not explicitly mention privacy or data protection, protection of both rights is explicitly established at the constitutional level in Europe (…).

estabelecida na Carta [Europeia de Direitos Fundamentais], a jurisprudência tem justificadamente considerado a privacidade estar no núcleo da proteção de dados”[89].

3.1 A TEORIA DO BEM JURÍDICO

O bem jurídico ocupa uma posição central na dogmática penal. Segundo Ana Elisa Bechara (2014, p. 70):

> Tratando especificamente da função do Direito Penal, a partir do primeiro terço do século XIX, e com base na herança utilitária do Iluminismo, passou-se a considerá-la tradicionalmente como a proteção de direitos subjetivos, depois traduzidos em bens jurídicos, ou bens jurídico-penais, entendidos em sentido amplo como aqueles bens e valores fundamentais da pessoa e da sociedade.

O conceito material de crime é a violação ou exposição a perigo do bem jurídico. Segundo Cláudio Brandão (2019, p. 38), a “definição legal de crime desvinculada do bem jurídico seria representaria um corpo sem alma”, tal o grau de importância da teoria do bem jurídico para o Direito Penal.

Conforme Claus Roxin (2013, p. 18), pode-se definir os bens jurídicos como “circunstâncias reais dadas ou finalidades necessárias para uma vida segura e livre, que garanta todos os direitos humanos e civis de cada um na sociedade ou para o funcionamento estatal que se baseia nestes objetivos”. Tal conceito é fundamental e de completo alinhamento com este trabalho, uma vez que o conceito de bem jurídico, em nosso entendimento, não se relaciona unicamente com a proteção a ser conferida pelo Direito Penal por meio da criminalização de condutas, mas, sim, conforme o conceito apresentado por Roxin, para todo o “funcionamento estatal que se baseia nestes objetivos”. Isso inclui o funcionamento jurídico-penal do Estado (investigação, persecução, repressão) e suas medidas de intervenção em direitos fundamentais (infiltração encoberta ou *online*, interceptação ou vigilância telefônica ou telemática, violação do sigilo de correspondência etc.), especialmente na privacidade e a proteção de dados em matéria penal em razão de serem o objeto deste trabalho.

---

[89] Tradução livre: In spite of the distinction between privacy and data protection laid down in the Charter, the jurisprudence has justifiably considered privacy to be at the core of data protection.

3.2 A evolução da teoria do bem jurídico

Luigi Ferrajoli (2000, p. 374) afirma que o bem jurídico, enquanto interesse protegido, possui uma história que "coincide, em boa parte, com a história moderna do conceito de delito". Ao final do século XVII, Paul Johahn Anselm Ritter von Feuerbach foi o primeiro a produzir uma "tentativa consequente de um conceito material de crime, transcendente e crítico face ao direito penal vigente" (Costa Andrade, 2004, p. 43) e "ensaiou o que se considera o primeiro conceito material de crime da modernidade" (Badaró, 2017, p. 26). Naquela época, quando os ideais iluministas e liberais foram trazidos para o Direito Penal, a preocupação se dirigia ao objeto de tutela penal e sua finalidade (Brandão, 2019, p. 40).

Assim, Feuerbach, de acordo com Cláudio Brandão (2019, p. 40), "em seu tratado datado de 1801, buscou apresentar o objeto de proteção do direito penal", que seria a tutela de direitos subjetivos. Estes seriam "o conjunto de direitos privados ou individuais atribuídos às pessoas que são titulares desses direitos". Nesta concepção, segundo Tatiana Badaró (2017, p. 26), a "compreensão de direito subjetivo é transportada do âmbito civil para o penal" e possuía "inegável viés privatista, pois considerava como núcleo do delito a violação a alguma faculdade jurídica inerente à liberdade garantida pelo contrato social". De fato, Feuerbach (1989, p. 64) em seu Tratado de Direito Penal (em tradução livre), afirma que "o que lesiona a liberdade garantida pelo contrato social e assegurada mediante leis penais, comete um *crime* [grifo do autor]"[90].

Por outro lado, uma tendência de espiritualização à época não pode ser deixada de lado, "especialmente a partir da teoria do Direito e do delito de Georg Wilheim Friedrich Hegel" (Bechara, 2014, p. 94). O surgimento do conceito de bem, portanto, também tem raízes no sistema de delito hegeliano, que influenciou autores como Günther Jakobs.

A ideia de bem em Direito Penal surgiu a partir de Johann Michael Franz Birnbaum, que "foi o primeiro autor a empregar referida expressão, em 1834, visando com ela a abranger um conjunto de valores apto a basear a punibilidade dos comportamentos que

[90] Tradução livre: El que lesiona la libertad garantizada por el contrato social y asegurada mediante leyes penales, comete un crimen.

os ofendessem" (Bechara, 2014, p. 95). O conceito de bem jurídico, apesar de não ter sido utilizada diretamente essa expressão, portanto, é atribuída a Birnbaum nascendo a partir da polêmica sobre o conteúdo da tutela penal (Brandão, 2019, p. 41). Isso porque Birnbaum, segundo Cláudio Brandão (2019, p. 42), constrói sua teoria a partir da crítica nominal a Feuerbach e sua teoria de proteção a direitos subjetivos. Assim, de acordo com Ana Elisa Bechara (2014, p. 98), "embora se reconheça a falta de precisão de Birnbaum sobre o conteúdo do bem merecedor de tutela penal, a importância da teoria reside na concretização, a partir da natureza das coisas, de um conceito fundamental à teoria do delito".

Em 1834, Karl Binding publica o artigo *Über das Erfordernis einer Rechtsverletzung zum Begriff des Verbrechens*, que representa "o início da história doutrinal e político-criminal do conceito de bem jurídico" (Costa Andrade, 2004, p. 51). Apesar desse marco histórico, de acordo com Costa Andrade (2004, p. 52), o conceito de bem jurídico ainda viria a ser mais bem desenvolvido por juristas como Franz von Liszt em um breve futuro, porquanto ainda não se encontraria no conceito de elaborado por Birnbaum "uma formulação acabada e claramente recortada". De todo modo, sua contribuição foi fundamental pois, como assinala Cláudio Brandão (2019, p. 45)," caso não houvesse essa contribuição, não haveria o desenvolvimento, ainda no século XIX, do instituto penal do bem jurídico".

Abraçando inteiramente o positivismo e rompendo definitivamente com o legado do Iluminismo, de acordo com Cláudio Brandão (2019, p. 46):

> Binding afasta-se da ideia de *bem garantido pelo direito através do Estado*, que estava no substrato da construção de Birnbaum, pressupondo a anterioridade do bem, que é reconhecido e protegido pelo direito penal, e constrói a nomenclatura *bem jurídico (Rechsgut)* [grifos do autor]).

Este novo caminho trilhado por Binding procurou, segundo Costa Andrade (2004, p. 52), "formular o conceito de bem jurídico indutivamente a partir da lei – como produto de um processo de desenvolvimento social". Brandão (2019, p. 47), por sua vez, assinala que "para Binding, a norma é a única fonte do bem jurídico". Ao determiná-lo, o bem jurídico, a norma consequentemente revelaria o conteúdo de sua lesão, também chamada de violação do bem jurídico. Curiosamente, segundo Costa Andrade (2004, p.

64), “a expressão Rechtsgut viria, contudo, a sofrer, ao longo da experiência doutrinal germânica, uma evolução semântica e político criminal que a emanciparia dos limites que lhe foram consignados pelos primeiros textos de Binding”, retornando, assim, ao conceito original em Birnbaum.

Posteriormente, Franz von Liszt estabelece seu conceito de bem jurídico e, junto dele, “um conteúdo material do delito a servir de fronteira limitadora da intervenção penal, assinalando que é a realidade social, e não o legislador, que impõe os objetos merecedores de proteção” (Bechara, 2014, p. 102). Franz von Liszt afirmava que “a proteção de interesses é a essência do direito, a ideia finalística a força que o produz”, sendo que chamaria de “bens jurídicos os interesses que o direito protege. Bem jurídico é, pois, o interesse juridicamente protegido” (2006, p. 93).

Liszt foi, portanto, opositor das ideias de Binding e, mesmo que tenham partido de um mesmo ponto de vista sobre o Direito, Binding o faria a partir da centralidade da norma (não do bem jurídico), enquanto Liszt conferia à política criminal a busca de interesses merecedores de proteção penal, “uma vez que os interesses a proteger penalmente e susceptíveis de ser [sic] atingidos pelo crime existem antes e independentemente da lei (...) (Costa Andrade, 2004, p. 67). O próprio Liszt (2006, p. 96) afirmaria que “o nosso ponto de partida em relação à theoria [sic] geral do direito é consequentemente o mesmo de Binding. Mas logo se separam os nossos caminhos”.

3.3 A teoria neokantista do bem jurídico

No início do século XX, uma corrente de pensamento ganharia força e traria mudanças significativas para o Direito Penal, o neokantismo. O neokantismo surgiu a partir de uma crítica “contra a cientificidade que pretendia, no âmbito positivista, transpor o método experimental das ciências naturais à análise dos fenômenos sociais, inclusive da esfera jurídica” (Bechara, 2014, p. 105). De acordo com Brandão (2019, p. 48), o direito penal seria visto como “uma ciência natural” pelo neokantismo, sendo este conceito de cultura “fundamental para o desenvolvimento da teoria do direito”.

Assim, uma mudança importante ocorre na compreensão do bem jurídico à época. O conceito metodológico, de base normativista, se torna o expoente por meio de

pressupostos próprios da chamada escola de Badem (ou subocidental alemã), a partir de 1920. De acordo com Tatiana Badaró (2017, p. 50), “a metodologia adotada pelo idealismo neokantista da Escola de Baden impulsionou a elaboração dogmática do Direito Penal, passando os conceitos jurídico-penais a serem entendidos como conceitos essencialmente valorativos”.

Essa distinção entre “natureza e cultura” encontra suas origens na dicotomia kantiana da crítica da razão pura e da crítica da razão prática, adotando métodos diferentes para a investigação dos objetos (Brandão, 2019, p. 48). Importante notar que as teorias penais da atualidade são essencialmente de base neokantiana pois, de acordo com Cláudio Brandão (2019, p. 48), “tratam metodologicamente o direito penal pela compreensão valorativa, o que é próprio das ciências culturais. Assim, tanto o finalismo quanto o funcionalismo têm suas matrizes no neokantismo”.

Um importante representante dessa teoria, Edmung Mezger, defendia que “a identificação do bem jurídico também deve ser feito com o apoio do Direito supralegal, composto pelas normas de cultura das quais todo Direito emana” (Badaró, 2017, p. 52). Hans Welzel (1971, p. 199), por sua vez, afirma que “a razão mais profunda do fracasso da filosofia do Direito neokantiano não se encontra em seu formalismo, no relativismo ou no historicismo de sua ‘medida’ ideal, senão na manutenção e consolidação do conceito positivista do Direito”[91]. Assim, o positivismo havia reduzido o Direito ao poder, sendo que “poderia se designar a filosofia do Direito neokantiana como uma teoria complementar ao positivismo jurídico”[92] (Welzel, 1971, p. 199).

Por fim, assinala Tatiana Badaró (2017, p. 108):

> Conclui-se, então, que o conceito metodológico de bem jurídico, ao reduzi-lo à finalidade da norma, não representou limitação alguma ao Direito Penal, podendo-se afirmar que a ideia de restringir o legislador em sua competência penal a partir do conceito de bem jurídico só se tornou objeto relevante da discussão político-criminal após a Segunda Guerra Mundial.

[91] Tradução livre: La razón más profunda del fracaso de la filosofía del Derecho neokantiano no se encuentra en el formalismo, en el relativismo o en el historicismo de su “medida” ideal, sino en el mantenimiento y consolidación del concepto positivista del Derecho.
[92] Tradução livre: (...) puede designarse la filosofía del Derecho neokantiana como una teoría complementaria del positivismo jurídico.

Durante o período de 1933 a 1945, grandes transformações foram impostas ao direito alemão, em razão da tomada de poder absoluto pelo regime nacional-socialista. A sujeição dos indivíduos ao cumprimento de ordens e, especialmente aos juristas uma abordagem de que “antes de tudo, deve-se cumprir as leis”, silenciou qualquer tipo de discordância intelectual. A substituição do princípio *nullum crimen nula poena sine lege* pela nova máxima *nullum crimen sine poena* revelaria uma configuração autoritária de um Direito Penal moralista, usado como arma ao invés de escudo de proteção. Assim, “o ideal nazista acaba, portanto, com a diferença entre moral e Direito, até então considerada em sua importância como pilar do positivismo” (Bechara, 2014, p. 111).

De acordo com Tatiana Badaró (2017, p. 55), “a ciência penal, no contexto da ditadura nazista, assistiu à controvérsia entre a Escola de Marburgo e a Escola de Kiel a respeito da manutenção da noção de bem jurídico”. Assim, enquanto a Escola de Marburgo ainda tentava adequar o conceito a um Direito Penal de Estado totalitário, mesmo que esvaziando-o de seu conteúdo material, a Escola de Kiel via na teoria do bem jurídico “um inimigo a ser eliminado, em razão do seu legado liberal e individualista” (Badaró, 2017, p. 55). Entretanto, segundo Santiago Mir Puig (2003, p. 115), “em 1937 e 1938 estes mesmos autores aceitaram-no em duas obras distintas, depois de o neokantiano Schwinge e o nacional-socialista Klee terem defendido a compatibilidade do bem jurídico com o nacional-socialismo”[93].

Luigi Ferrajoli (2002, p. 376) atribui às consequências desse momento histórico um marco adotado pelos juristas nazistas de modelo “acentuadamente ético e subjetivista do direito penal da vontade”, em que não lhes restava abandonar o conceito construído de bem jurídico, substituindo-o por conceitos de “violação do dever, desvalor da atitude interna, ou infidelidade ao Estado ou ao seu chefe”. Teria alcançado o conceito de bem jurídico, assim, o “fim da sua parábola”.

[93] Tradução livre: Pero en 1937 y 1938 estos mismos autores lo aceptaron en sendos trabajos, después de que el neokantiano Schwinge y el nacional-socialista Klee defendiesen la compatibilidad de bien jurídico y nacional-socialismo.

3.4 Teorias funcionalistas sistêmicas

Terminado o pesadelo da Segunda Guerra e de suas atrocidades, o Direito Penal voltaria a se preocupar com a filosofia do Direito, o Direito natural e o mundo dos valores (Bechara, 2014, p. 115). O Direito Penal passaria, então, a passar da proteção de bens jurídicos para uma garantia ético-social positiva. Hans Welzel (1956, p. 4) afirma que "somente sobre o asseguramento dos valores elementais ético-sociais da ação, pode obter-se um amparo amplo e duradouro dos bens jurídicos"[94].

Ana Elisa Bechara (2014, p. 117) afirma que "(...) há de se ressaltar que a Hans Welzel corresponde o mérito de ter retomado a ideia de um conteúdo material do bem jurídico, retirando-lhe o rótulo de *ratio legis* ou elemento meramente formal de legitimação da intervenção penal". Desse modo, novas correntes político-criminais seguindo o período pós-Segunda Guerra, "buscaram no conteúdo do delito e, assim, no bem jurídico, o referente material para fundar as propostas de revisão crítica do Direito Penal (Bechara, 2014, p. 117).

Posteriormente, ainda no pós-guerra, "a sociologia passou a tomar lugar como provedora da ideologia para legitimar o poder estatal de punir" (Ishida, 2017, p. 40), substituindo a filosofia e a teoria política da Europa neste sentido. Surgem, então, as teorias sociológicas (funcionalistas-sistêmicas e interacionistas simbólicas), que atribuíam ao direito penal "não mais a função de proteção de bens jurídicos, mas sim o papel de manutenção do funcionamento hígido do sistema social, negando, com isso, qualquer importância da teoria do bem jurídico (...)" (Raposo, 2011, p. 90).

De acordo com Tatiana Badaró (2017, p. 76), "a doutrina funcionalista sistêmica tem origem na obra de Durkheim, desenvolvendo-se, posteriormente, com os trabalhos de Merton, Parsons e Luhmann. Knut Amelung, um dos expoentes dessa fase, "entendia ser a noção de bem jurídico válida como teoria sistêmica e critério de nocividade social" (Prado, 2019, p. 53). Já Günther Jakobs, de acordo com Luiz Regis Prado (2019, p. 54), afirmava que "a missão do Direito Penal é assegurar a validade fática ou a vigência das

[94] Tradução livre: Solamente sobre el aseguramiento de los valores elementales ético-sociales de la acción, puede lograrse un amparo amplio y duradero de los bienes jurídicos.

normas jurídicas, no sentido de garantir expectativas indispensáveis ao funcionamento do sistema social".

Entretanto, a principal crítica às teorias funcionalistas sistêmicas é a de que apesar da construção teórica destinada a legitimar a reprodução de qualquer sistema social, tal representação serviria, indistintamente, para fins de regimes tanto democráticos, quanto totalitários (Badaró, 2017, p. 84). Ocorre que, conforme Jorge de Figueiredo Dias (1999, p. 66), essas teorias desprezam o fato de que o apelo direto a tal sistema "é incapaz de emprestar ao conceito de bem jurídico a indispensável concretização".

De fato, Amelung, não obtendo êxito em estabelecer uma noção pré-positiva de danosidade social, acaba por retornar ao conceito positivista de bem jurídico de Binding, mantendo-o em uma posição de proeminência em relação à danosidade social, reduzida a pano de fundo (Badaró, 2017, p.84). Também Costa Andrade (2004, p. 103) assinala que "as 'inesperadas' conclusões de Amelung 'realizam precisamente aquilo que ele se propunha esconjurar: um *retorno a Binding* e à definição do bem jurídico como tudo o que, do *ponto de vista do legislador* [grifos do autor], constitui condição de uma vida sã da comunidade jurídica'".

3.5 A teoria constitucional do bem jurídico

Conforme já abordamos, após o difícil período vivenciado na segunda guerra mundial, suas atrocidades e arbitrariedades, a nova realidade proporcionou a reconstrução do conceito de Estado de Direito, mas desta vez amparada pela Declaração Universal dos Direitos Humanos de 1948. O enunciado da dignidade humana como fundamento do Estado democrático e sua incorporação nos ordenamentos jurídicos de diversos países impediria, em tese, intervenções indevidas nos direitos fundamentais dos indivíduos, especialmente na esfera penal.

Desse modo, de acordo com Tatiana Badaró (2017, p. 86):

> As teorias constitucionalmente orientadas buscaram na Constituição a fonte jurídica superior da qual os bens jurídico-penais devem emergir. Para essas teorizações, o conceito de bem jurídico político-criminalmente vinculante se encontra refletido num valor constitucional, preexistindo, por conseguinte, ao ordenamento jurídico-penal.

Ainda, de acordo com Luiz Regis Prado (2019, p. 61), as teorias constitucionais do bem jurídico procuram “formular critérios capazes de se impor de modo necessário ao legislador ordinário, limitando-o no momento de criar o ilícito penal”. Entretanto, entendemos que a limitação imposta pela vinculação constitucional vincula não somente o legislador na criação de tipos penais, mas também todo o funcionamento do sistema jurídico-penal, nas suas diferentes etapas e funções, assim como as medidas de intervenção nos direitos fundamentais, conforme será abordado ao longo desse trabalho.

Luigi Ferrajoli (2002, p. 376) assinala que estes bens jurídico-penais protegidos seriam os de tipo individual ou social, tanto do dano causado quanto do perigo. Estes bens externos ao direito penal seriam todos os direitos fundamentais, tanto os direitos individuais e liberais, quanto os coletivos e/ou sociais.

Há três correntes dos defensores da teoria constitucional do bem jurídico, conforme destaca Tatiana Badaró (2023, p. 48). Na corrente estrita ou rígida, a proteção penal recai somente sobre “os bens de expressa relevância constitucional”. Já a corrente moderada ou intermediária defende que adicionalmente estão compreendidos os “valores constitucionais implícitos”. Por fim, a corrente branda ou ampla, estende ainda mais “a noção constitucionalmente orientada de bem jurídico-penal para abarcar também os bens não compatíveis com a Constituição”. De acordo com Claus Roxin (2013, p. 18), o conceito de bem jurídico aqui defendido seria um conceito “crítico com a legislação, na medida em que pretende mostrar ao legislador as fronteiras de uma punição legítima”. Roxin, assim, contraria o conceito metódico de bem jurídico em que o bem jurídico seja a própria finalidade das normas, a *ratio legis*.

Críticos da teoria constitucional estrita sinalizam preocupação com a vinculação com a expressa relevância constitucional abre espaço para interpretações diversas, uma vez que o texto constitucional possui “expressões abertas e abstratas” (Badaró, 2017, p. 89), como “dignidade da pessoa humana”, “justiça social”, dentre outras. Atualmente, a teoria ampla que expande a noção constitucional de bem jurídico é a mais adotada, alcançando “os bens de relevância constitucional implícita e os bens não incompatíveis com a Constituição”.

Luiz Regis Prado (2019, p. 66) acolhe a concepção de que “o bem jurídico protegido deve estar sempre em compasso (de conformidade) com o *quadro axiológico* vazado na Constituição (princípios e valores – chamado núcleo material constitucional), e a noção de Estado democrático de e social de Direito (Estado Constitucional)”,

Assim, ainda de acordo com Prado (2019, p. 67), “a ideia de bem jurídico fundamenta a ilicitude material, ao mesmo tempo em que legitima a intervenção penal”. Tal concepção é de importante assimilação pelo aparato jurídico-penal estatal, entretanto, nos parece incompleta, uma vez que o bem jurídico-penal constitucional deve abranger a imposição de limites à intervenção penal em seu sentido amplo, especialmente em suas medidas interventivas em direitos fundamentais (tidos como os bens jurídicos de mais alto valor para o indivíduo e para a sociedade).

Claus Roxin (1997, p. 57) defende que “o conceito do bem jurídico é certamente de tipo normativo; mas não é estático, uma vez que dentro do marco das finalidades constitucionais está aberta ao campo social e aos progressos do conhecimento científico”[95]. Assim, Roxin (1997, p. 56) apresenta um conceito próximo ao que defendemos neste trabalho:

> Os bens jurídicos são circunstâncias dadas ou finalidades que são úteis para o indivíduo e seu livre desenvolvimento em um marco de um sistema social global estruturado sobre a base desta concepção dos fins ou para o funcionamento do próprio sistema[96].

Após tantas transformações, segundo Ana Elisa Bechara (2014, p. 271), “o pensamento jurídico-penal enfrenta, na atualidade, uma fase de marcado desencanto sobre a capacidade efetiva da teoria do bem jurídico de orientar as escolhas legislativas e, assim, de limitar a intervenção penal”. Os questionamentos são tão profundos que até mesmo o próprio fundamento do Direito Penal tem sido abordado em discussões.

Assim, diversas correntes buscam alternativas que funcionem como critérios para fundamentar a legitimidade do Direito Penal, especialmente frente ao que Winfried

---

[95] Tradução livre: La concepción del bien jurídico descrita es ciertamente de tipo normativo; pero no es estática, sino que dentro del marco de las finalidades constitucionales está abierta al cambio social y a los progresos del conocimiento científico.

[96] Tradução livre: Los bienes jurídicos son circunstancias dadas o finalidades que son útiles para el individuo y su libre desarrollo en el marco de un sistema social global estructurado sobre la base de esa concepción de los fines o para el funcionamiento del propio sistema.

Hassemer chama de “criminalidade moderna”. Hassemer (1994, p. 1) resume seu pensamento da seguinte maneira:

> A atual política criminal é totalmente diferente do que era há vinte anos atrás. O Direito Penal é incapaz de solucionar os modernos problemas da criminalidade, e nós temos que refletir a respeito de algo que seja melhor, mais eficaz, que seja capaz de solucionar esses problemas. Eu chamo a isso de “Direito de Intervenção”.

Segundo o autor, o Direito Penal “novo” é inteiramente diferente do Direito Penal clássico em diversos aspectos. Expondo sua experiência na Alemanha, Hassemer (1994, p.3) assinala que “não há necessidade de reforma na Parte Geral do Direito Penal. Aí nada mudou. Não temos necessidade de reforma na execução penal, no direito processual penal. Tudo isso acabou, está morto”.

A nova criminalidade demandaria um novo tipo de criminalização e, segundo Hassemer (1994, p. 4), um “aguçamento das medidas” especialmente na fase de investigação, a fase preliminar. Nisso consistiria, segundo Hassemer, a “reforma penal alemã dos últimos vinte anos”.

Ao abordar os novos métodos utilizados na Alemanha para lidar com a criminalidade moderna, Hassemer (1994, p. 4) descreve os métodos introduzidos: utilização de métodos técnicos audiovisuais, permitindo a observação policial por meio de aparelhos de escuta e câmeras filmadoras o longo de “muitas semanas, de muitos meses, contra uma determinada pessoa, o que antes não era possível nem permitido”; a utilização de dados armazenados em sistemas informatizados, fazendo com que “milhões de cidadãos entrem no processo investigatório para encontrar três ou quatro pessoas”; a utilização de investigadores disfarçados ou infiltrados.

A denúncia de Hassemer (1994, p. 4) é contundente e preocupante. Um dos exemplos citados menciona a “utilização de dados informatizados de milhões de alemães que pagavam suas contas de luz com dinheiro – método utilizado pelos terroristas para não serem localizados filtrando informações para localizar três ou quatro terroristas”. Outro exemplo menciona que em um único processo em Frankfurt “foi feita a escuta de trinta e seis mil telefonemas”. Hassemer conclui que “é preciso refletir quando falamos em métodos modernos de investigação policial.

O outro método descrito por Hassemer é chamado por ele de “invasão da privacidade de terceiros”, em que os processos de investigação atingem terceiros não suspeitos e com a coleta de milhares de dados que “acabam ficando no computador da polícia. Não são esquecidos, não são apagados, são arquivados e isso constitui uma invasão de privacidade dos cidadãos não suspeitos. Essa privacidade tem que ser respeitada e está fora do direito de intervenção estatal”.

Fabio Romeu Canton Filho (2015, p. 35) faz importante advertência ao anotar que os progressos alcançados pelo Estado de Direito podem ser invalidados com “a restrição de direitos sob a justificativa de se ampliar a segurança”. Isso porque, segundo Canton Filho, “a flexibilização de garantias não constitui qualquer elevação qualitativa na tutela penal, podendo na realidade uma insegurança de tipo mais amplo relacionada a uma ação coercitiva do Estado que perde seu norte ético e seus limites restritos”.

O relato de Hassemer data de 1994, entretanto, após décadas, a situação “moderna” aprofunda ainda mais a voracidade pelas intervenções, pela digitalização, pela tecnocracia em detrimento dos direitos fundamentais e da proteção da dignidade humana. A sociedade dos dados somente iniciou sua história e a teoria do bem jurídico tem sido colocada à prova com a busca por outras teorias úteis e – pretensamente – mais adequadas para justificar a intervenção penal.

3.6 Evolução da privacidade e proteção de dados enquanto bens jurídicos constitucionais penais

Ao abordar o desenvolvimento da privacidade no contexto norte-americano, Edwards Shils (1966, p. 292) identificou o final do século XIX como “a era de ouro da privacidade” e assim classificou este período devido à tendência de industrialização e urbanização (que se seguiu ao declínio da sociedade feudal). Ainda segundo o autor, “a prosperidade crescente e um maior padrão de vida proporcionaram melhores condições de moradia e, portanto, mais privacidade individual e familiar”. Holvast (2008, p.15) ensina

que “historicamente, pobreza e o lar significam menos privacidade, particularmente onde famílias compartilham habitações comuns, com quase nenhuma separação física”[97].

O marco histórico do reconhecimento jurídico estadunidense do direito à privacidade, ou *right to privacy*, é tido como sendo o artigo “*The Right to Privacy*”, de autoria do advogado Samuel D. Warren e do então juiz da Suprema Corte norte-americana Louis D. Brandeis, publicado na *Harvard Law Review* em 15 de dezembro de 1890 (Glancy, 1979, p. 1).

Neste artigo, Brandeis e Warren sinalizam a necessidade de, de tempos em tempos, se definir a exata natureza e extensão da completa proteção à pessoa e à propriedade, um princípio “tão velho quanto a *common law*”[98] (1890, p. 193). Ainda, de acordo com os autores, “mudanças políticas, sociais e econômicas demandam o reconhecimento de novos direitos, e a *common law*, em sua eterna juventude, cresce para suprir tais demandas da sociedade”[99]. Uma afirmativa brilhante e atualíssima mesmo para os tempos atuais, talvez com o acréscimo das “mudanças tecnológicas” no rol de mudanças destacado pelos autores, que chegam a mencionar “as invenções e empresas modernas”.

Curiosamente, há autores que mencionam que Warren e Brandeis escreveram tal artigo influenciados pela introdução tecnológica na imprensa de sua época, como o gravador e a máquina fotográfica portáteis (Glancy, 1979, p. 8), dispositivos que favoreceram um fenômeno intitulado *newspaperization* (algo como uma tendência de tudo noticiar, em uma tradução livre), e pelas violações à sua própria privacidade e de suas famílias. Warren era advogado e filho de um “próspero fabricante de papel e membro da bem estabelecida elite comercial em Boston”[100] (Glancy, 1979, p. 8) e, segundo Wienczyslaw Wagner (1965, p. 366), sua esposa era a “filha de um senador que levava uma vida bastante ativa”. Ainda, segundo Wagner, “os jornais de Boston se esforçavam para obter todos os detalhes possíveis sobre o que se passava na casa dos

[97] Tradução livre: Historically, poverty and the home meant less privacy, particularly where families share common dwellings with almost no physical separation.
[98] Tradução livre: (…) as old as the common law.
[99] Tradução livre: Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.
[100] Tradução livre: Samuel D. Warren was the son of a wealthy paper manufacturer, and a member of the well-established commercial elite in Boston.

Warren a fim de os publicar"[101] e Brandeis "viria a se tornar mais tarde um dos juízes mais célebres da Corte Suprema dos Estados Unidos"[102].

Durante muitos anos o *right to privacy* enfrentou sérias dificuldades na jurisprudência estadunidense. Mesmo tendo sido acolhida jurisprudencialmente, no início do século XX "ainda havia insegurança entre os juristas norte-americanos quanto a sua aceitação generalizada, e até em relação ao sentido e conteúdo que lhe atribuíam os juízes", segundo José Adércio Leite Sampaio (1998, p. 59).

Em 1928, o caso *Olmstead v. United States*[103], acabou por estabelecer que:

> O uso como prova em um julgamento criminal em um tribunal federal de uma conversa telefônica incriminadora conduzida voluntariamente pelo acusado e secretamente ouvida por um agente do governo por meio de uma escuta telefônica não obriga o acusado a ser testemunha contra si mesmo, violando a Quinta Emenda.[104]

Acrescentando que:

> A política de proteger o sigilo das mensagens telefônicas tornando-as, quando interceptadas, inadmissíveis como prova em julgamentos criminais federais pode ser adotada pelo Congresso por meio de legislação, mas não cabe aos tribunais adotarem-na atribuindo um significado ampliado e incomum à Quarta Emenda.[105]

Concluem o caso afirmando:

> De acordo com a *common law*, a admissibilidade da prova não é afetada pelo fato de ela ter sido obtida ilegalmente. (...) Sem a sanção de uma Lei do Congresso, os tribunais federais não têm poder discricionário para excluir provas,

---

[101] Tradução livre: Les journaux de Boston s'efforçaient d'obtenir tous les détails possibles sur ce qui se passait chez les Warren afin de les publier.
[102] Tradução livre: (…) qui devait être plus tard l'un des juges les plus célèbres de la Cour Suprême des Etats-Unis.
[103] Justia – U.S. Supreme Court. **Olmstead v. United States, 277 U.S. 438 (1928)**. Disponível em: https://supreme.justia.com/cases/federal/us/277/438/. Acesso em: 14 jun. 2024.
[104] Tradução livre: Use in evidence in a criminal trial in a federal court of an incriminating telephone conversation voluntarily conducted by the accused and secretly overheard from a tapped wire by a government officer does not compel the accused to be a witness against himself in violation of the Fifth Amendment.
[105] Tradução livre: The policy of protecting the secrecy of telephone messages by making them, when intercepted, inadmissible as evidence in federal criminal trials may be adopted by Congress through legislation, but it is not for the courts to adopt it by attributing an enlarged and unusual meaning to the Fourth Amendment.

> cuja admissão não é inconstitucional, porque foram obtidas de forma antiética.[106]

Tendo essa decisão representado uma derrota para o *right to privacy* na ocasião, Warren Brandeis, que era um dos juízes do caso, claramente manifestou sua opinião de que:

> A proteção garantida pelas Emendas é muito mais ampla em seu escopo. Os criadores de nossa Constituição se comprometeram a garantir condições favoráveis à busca da felicidade. Eles reconheceram a importância da natureza espiritual do homem, de seus sentimentos e de seu intelecto. Eles sabiam que apenas uma parte da dor, do prazer e da satisfação da vida pode ser encontrada em coisas materiais. Eles procuraram proteger os americanos em suas crenças, seus pensamentos, suas emoções e suas sensações. Eles conferiram, em relação ao governo, o direito de ser deixado em paz - o mais abrangente dos direitos e o direito mais valorizado pelos homens civilizados. Para proteger esse direito, toda intrusão injustificável do governo na privacidade do indivíduo, independentemente dos meios empregados, deve ser considerada uma violação da Quarta Emenda. E o uso, como evidência em um processo criminal, de fatos apurados por essa intrusão deve ser considerado uma violação da Quinta Emenda.[107]

Chamou a atenção, ainda, "para a as possibilidades quase ilimitadas de invasão de privacidade, através do uso de recursos técnicos cada vez mais sofisticados", conforme lembra José Adércio Leite Sampaio (1998, p. 60). Um voto proferido em 1928, mas que não poderia ser mais atual.

O artigo de Warren e Brandeis (*The Right of Privacy*) e o voto discordante (*dissent*) de Brandeis no caso *Olmstead* acabaram por "moldar significativamente o direito constitucional" nas décadas por vir, a ponto de a Suprema Corte estadunidense, em 1967,

---

[106] Tradução livre: Under the common law, the admissibility of evidence is not affected by the fact of its having been obtained illegally. (…) Without the sanction of an Act of Congress, federal courts have no discretion to exclude evidence, the admission of which is not unconstitutional, because it was unethically procured.

[107] Tradução livre: The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone -- the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.

adotar a visão de Brandeis a respeito da Quarta Emenda, abandonando o entendimento adotado em *Olmstead* no caso *Katz v. United States*[108] (Solove, 2008, p. 17).

Entretanto, o contexto histórico que mais nos interessa é o desenvolvimento alemão da privacidade e proteção de dados pessoais. Isto porque, segundo Milton Fernandes (1977, p. 244), "datam aproximadamente da mesma época dos norte-americanos e franceses os estudos alemães sobre a vida privada, estando mais uma vez diante de um campo em que a sutileza e a profundidade da doutrina germânica realizaram prodígios" e, no tema de proteção de dados pessoais, a experiência alemã é tida como pioneira (Gleizer; Montenegro; Viana, 2021, p. 21), tendo início já na década de 1970, com a Lei de Proteção de Dados do Estado de Hessen (*Hessisches Datenschutzgesetz*) e, poucas semanas à frente, a publicação da Lei sobre a Organização do Tratamento Eletrônico dos Dados (*Gesetz über die Organisation der elektronischen Datenverarbeitung im Freistaat Bayern – bayrisches EDVG*) pelo Estado da Baviera. Dois modelos diferentes para tratamento de dados, tendo prevalecido o modelo de Hessen, de acordo com a Lei Federal de Proteção de Dados (*Bundesdatenschuzgesetz – BDSG*) de 1977[109].

A outra razão pela qual o contexto alemão nos interessa em particular, é que a Alemanha é o berço dogmático da teoria do bem jurídico amplamente adotado pela dogmática brasileira. Tendo Alselm von Feuerbach sido responsável pela sistematização jurídica do princípio da legalidade em 1801 com sua "teoria da coação psicológica", já no séc. XIX foram desenvolvidos (também pela dogmática alemã) os elementos que formam o conceito de crime que também é adotado pela dogmática brasileira: tipicidade, antijuridicidade e culpabilidade (Brandão, 2019, p. 33).

Essa aproximação entre a autoria alemã da teoria do bem jurídico e o pioneirismo alemão (e seu maduro desenvolvimento) em proteção de dados pessoais representou uma feliz "coincidência" para nosso trabalho, justificando, assim, nosso especial interesse. É importante observar, também, que "a partir da experiência de Hesse,

---

[108] Justia U.S. Supreme Court. **Katz v. United States, 3389 U.S. 347 (1967)**. Disponível em: https://supreme.justia.com/cases/federal/us/389/347/. Acesso em: 14 jun. 2024.
[109] JOTA. **Criação e desenvolvimento da proteção de dados na Alemanha.** Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 15 jul. 2024.

algumas legislações nacionais surgiram na Europa na década de 1970 (...)", conforme nos lembra Danilo Doneda (2021, p. 9), especialmente a lei de proteção de dados da Suécia nº 1973:289 (*Datalag*), datada de maio de 1973[110] e a lei francesa nº 78-17 (*Informatique et Libertés*), datada de janeiro de 1978[111].

Considerando o ponto de partida a teoria geral dos direitos de personalidade, alguns autores de língua germânica elaboraram importante conteúdo acerca deste direito que estava intimamente conectado ao tema da privacidade: Joseph Köhler, em 1893 com a publicação de *Das Recht an Briefen* (direito ao segredo epistolar com proteção da "vida interna individual"); Georg Cohn, em 1902, com a publicação de *Neue Rechtsgüter: Das Recht am eigenem Namem. Das Recht am eigenem Bilde* (Novos bens jurídicos: o direito ao nome próprio. O direito à própria imagem, em tradução livre); Hans Giesker, em 1905, com a publicação de *Das Recht des Privaten an der eigenen Geheimsphäre* (O direito dos indivíduos privados na própria esfera de segredo, em tradução livre). De acordo com José Adércio Leite Sampaio (1998, p. 68), estes "estudos são fundamentais na Europa continental, comparáveis, em importância, ao artigo de *Warren e Brandeis* [grifo do autor]".

Cohn (1902, p. 44), ao tratar do direito de imagem enquanto direito de personalidade, afirma, dentre outras determinações, que "(...) pode-se desejar que a vida privada seja preservada; a vida privada é cercada por um véu que ninguém está autorizado a perfurar, ninguém tem o direito de rompê-lo; ninguém precisa ser expulso de situações íntimas contra sua vontade e ser exposto ao público"[112].

Hubmann (1967, p. 268) teve importante contribuição para a jurisprudência constitucional alemã ao elaborar a teoria das esferas, onde afirmava:

> O direito à individualidade permite que cada indivíduo viva sua própria vida; ele a envolve com o triplo anel protetor da esfera do segredo, da esfera privada e da esfera individual. Dentro desse círculo, todos podem se esforçar para obter a imagem ideal da humanidade original criada apenas para eles, cuja realização

[110] Sveriges Riksdag. **Datalag**. Disponível em: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289. Acesso em: 20 jul. 2024.
[111] CNIL. **La loi Informatique et Libertés**. Disponível em: https://www.cnil.fr/fr/la-loi-informatique-et-libertes. Acesso em: 20 jul. 2024.
[112] Tradução livre: (…) könne man begehren, dass das Internum des Privatlebens gewahrt werde; das Privatleben umgebe ein Schleier, den niemand zu durchbrechen berechtigt sei; keiner brauche sich gegen seinen Willen aus den intimen Situationen herausreissen und der Oeffentlichkeit preisgeben zu lassen (…).

> constitui seu valor geral, seu valor característico como personalidade[113] (1967, p. 376).

Henkel (1958, p. 80) sobre a *Individualsphäre* de Hubmann, afirma que "seguindo Hubmann, toda essa área pode ser descrita como a esfera individual e o direito de preservar a esfera individual pode ser entendido como parte do direito geral da personalidade"[114].

De acordo com Luís Greco (*in* Wolter, 2018, p. 34), o círculo mais externo seria "o da esfera social ou pública, onde admite-se intervenções sem necessidade de justificativas elaboradas". Os círculos interiores seriam divididos em *Privatsphäre* (esfera da privacidade, em tradução livre) e *Geheimsphäre* (esfera do segredo, em tradução livre).

Henkel (1958, p. 80), em sua abordagem da teoria das esferas elaborada por Hubmann, menciona que:

> Hubmann faz distinção apenas entre a esfera do segredo e a esfera da privacidade, deixando de fora a esfera da confiança como uma área de proteção a ser particularmente enfatizada. No entanto, nossas investigações posteriores mostrarão que precisamos dela como uma tipicidade específica para registrar alguns elementos especiais de crimes de indiscrição (1958, p. 83).

Portanto, o conceito de teoria das esferas adotado por Henkel consistia em uma adaptação da teoria de Hubmann, com a representação de três círculos concêntricos na *Individualsphäre*: o mais externo (*Privatsphäre*) seria caracterizada pela privacidade em sua totalidade e a área contida neste círculo, segundo Henkel (1958, p. 81), "no que diz respeito ao indivíduo, abrange os processos e relações da vida que a pessoa em causa deseja proteger da intrusão e da percepção do público em geral, com base nas suas

---

[113] Tradução livre: Das Recht auf Individualität ermöglicht jedem einzelnen sein Eigenleben; es umgibt dieses mit dem dreifachen Schutzring der Geheimsphäre, der Privatsphäre und der Individualsphäre. Innerhalb dieses Kreises kann jeder jenem nur für ihn geschaffenen Idealbild originellen Menschentums nachstreben, dessen Realisierung seinen Gesamtwert, seinen Eigenwert als Persönlichkeit ausmacht.
[114] Tradução livre: Im Anschuluss an Hubmann kann man diesen Bereich als Individualsphäre bezeichnen und als Teilinhalt des allgemeinen Persönlichkeitsrechts das Recht auf die Wahrung der Individualsphäre auffassen.

necessidades pessoais legalmente reconhecidas”[115]; o segundo círculo (*Vertrauensphäre* - interior ao primeiro círculo mais externo) seria o da esfera de confiança, onde as exigências para intervenção seriam mais restritivas; o terceiro círculo e mais interior aos outros, a esfera do segredo (*Geheimsphäre*), onde “a defesa contra as percepções neste domínio é, portanto, a mais rigorosa e a necessidade de proteção jurídica é mais intensa do que nos outros grupos de casos”[116].

Segundo Greco (*in* Wolter, 2018, p. 34), esta seria a “área central, nuclear, da vida privada”, em tradução livre (*Kernbereich Privater Lebensgestaltung*). Neste círculo não haveria possibilidade de intervenção em razão de representar a expressão da dignidade humana, conforme o próprio *Bundesverfassungsgericht* (Tribunal Constitucional Federal alemão) aborda, por exemplo, em sua decisão sobre o caso BVerfGE 109, 279[117] afirmando que “com a garantia da inviolabilidade da dignidade humana, o Artigo 1(1) da Lei Fundamental reconhece um núcleo da vida privada, que goza de proteção absoluta”[118].

Outros autores, como Hans-Heinrich Maass em sua obra *Information und Geheimnis im Zivilrecht* (Informação e Sigilo no Direito Civil, em tradução livre), forneceram conceitos semelhantes à teoria das esferas com diferentes escalas como tentativas de delimitar e graduar a proteção da personalidade contra indiscrição e outras violações. Entretanto, a grande dificuldade permanece até os dias atuais quanto a caracterização e delimitação desses círculos, bem como seu exato conteúdo de proteção.

Manuel da Costa Andrade (2006, p. 97), observando a teoria dos três graus de criação jurisprudencial alemã, observa que a teoria possui “défices do ponto de vista de sua operatividade normativa e prático-jurídica”. Afirma, ainda, “isto dadas sobretudo as dificuldades de demarcação segura das fronteiras que separam as três áreas e os

---

[115] Tradução livre: Er umfasst im Hinblick auf der den Einzelperson diejenigen Lebensvorgänge und Lebensbeziehungen, die der Betreffende aus seinem rechtlich anerkannten Persönlichkeitsbedürfnis heraus vor dem Zudrang und der Wahrnehmung der Allgemeinheit zu schützen wünscht.
[116] Traduçao livre: Die Abwehr von Einblicken in diese Sphäre ist daher die strengste, das Bedürfnis nach rechtlichem Schutz intensiver als bei den anderen Fallgrupen.
[117] BVerfG, Urteil des Ersten Senats vom 03. März 2004 - 1 BvR 2378/98 -, Rn. 1-373. Disponível em: https://www.bverfg.de/e/rs20040303_1bvr237898.html. Acesso em 23 jul. 2024.
[118] Tradução livre: Zur Unantastbarkeit der Menschenwürde gemäß Art. 1 Abs. 1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung.

respectivos regimes, entre as quais medeiam, mais do que linhas de clivagem e de contraste, zonas de penumbra".

Apesar disso, conforme ressalta Milton Fernandes (1977, p. 67), "a utilidade da doutrina das esferas para o estudo do direito à intimidade é manifesta. Embora ainda imperfeitamente delineada, equaciona problemas sociológicos que o Direito precisa absorver, visando à correta solução legal". Afirma, ainda, que nesta teoria "se apoia a moderna construção do direito à intimidade" (Fernandes, 1977, p. 245). Confirmando, Sampaio (1998, p. 155) afirma que "a jurisprudência alemã adotou a teoria das esferas desenvolvidas pela doutrina, sobretudo na vertente original de *Hubmann* [grifo do autor], aplicando-a na elucidação de diversos casos".

Até 1949, não havia proteção conferida à personalidade pelo Tribunal Constitucional Federal Alemão (*Bundesverfassungsgericht,* ou BVerfGE em forma abreviada). O código civil alemão (*Bürgerliches Gesetzbuch*, ou BGB em forma abreviada) não possuía cláusula geral de responsabilidade por atos ilícitos. Segundo José Adércio Leite Sampaio (1998, p. 100), o § 823, I, usa o princípio da tipicidade ao prever responsabilidade civil e o § 826 obriga somente a indenização da causação de danos por atos dolosos e contrários aos bons costumes. Entretanto, continua Sampaio (1998, p. 102), "o direito geral de personalidade foi reconhecido pelo BVerfGE pela primeira vez[119], como 'lei geral' no sentido do art. 5.2. GG[120], conseguintemente como limite do direito à livre expressão do pensamento em 15/1/58 (...)".

Em 1973, o BVerfGE[121] decidiu "ser compatível com a Constituição a jurisprudência dos tribunais civis, de acordo com a qual, na hipótese de graves violações do direito de personalidade, poderá ser exigida indenização em dinheiro também por danos não patrimoniais". Curiosamente, este é um caso exemplo de utilização da teoria das esferas desenvolvida por Hubmann para a solução do tema pela corte constitucional alemã. Porém, uma situação alterou a compreensão do tema pela corte constitucional

[119] BVerfG, Urteil des Ersten Senats vom 15. Januar 1958 - 1 BvR 400/51 -, Rn. 1-75. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1958/01/rs19580115_1bvr040051.html. Acesso em: 18 jul. 2024.
[120] GG sendo a forma abreviada de Grundgesetz, a Lei Fundamental alemã.
[121] BVerfG, Order of the First Senate of 14 February 1973 - 1 BvR 112/65 -, paras. 1-46. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1973/02/rs19730214_1bvr011265en.html. Acesso em: 18 jul. 2024.

alemã de modo a influenciar o entendimento de outros países da Europa e a ampliação de legislação específica para o tema.

A Lei do Censo alemã (*Volkszählungsgesetz*) de 1983 disciplinava a atividade de recenseamento geral alemão coletando diversos tipos de dados (profissão, moradia etc.) para finalidades "estatísticas". Estabelecia os dados a serem levantados e a quem o fornecimento de tais dados se constituía uma obrigação. Tais dados levantados, de acordo com a lei, poderiam ser comparados com outros dados existentes em registros públicos e, ainda, compartilhados (após "anonimizados") com outras repartições públicas federais, estaduais e municipais para finalidades administrativas (Martins, 2005, p. 234).

Em razão do entendimento de diversas pessoas de que tal lei violaria direitos fundamentais, diversas Reclamações Constitucionais foram ajuizadas. Dentre os direitos fundamentais violados, sobressairia a violação ao direito ao livre desenvolvimento da personalidade, disposto no Art. 2 I da *Grungesetz*. Apesar do Tribunal Constitucional Federal Alemão ter julgado tais reclamações só parcialmente procedentes (mantendo, portanto, a constitucionalidade da referida lei), declarou "nulos principalmente os dispositivos sobre a comparação e trocas de dados e sobre a competência de transmissão de dados para fins de execução administrativa" (Martins, 2005, p. 234).

Esta decisão datada de 15 de dezembro de 1983 trouxe diversos elementos importantes para o tema da privacidade e proteção de dados pessoais. O desvio da finalidade declarada da atividade constituiria violação de uma proibição, conforme descrito no tópico de *Datengeheimnis* (confidencialidade dos dados, em tradução livre):

> (1) As pessoas empregadas no processamento de dados no âmbito da Seção 1, Parágrafo 2 ou em nome das pessoas ou entidades nele mencionadas estão proibidas de processar, divulgar ou acessar dados pessoais protegidos sem autorização para uma finalidade diferente daquela que faz parte do respectivo cumprimento legítimo da tarefa de fazer ou de outra forma usar.[122] [123]

[122] Tradução livre: (1) Den im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Personen oder Stellen bei der Datenverarbeitung beschäftigten Personen ist untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen.
[123] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215. Disponível em: https://www.bverfg.de/e/rs19831215_1bvr020983.html. Acesso em: 20 jul. 2024.

Adicionalmente, e talvez uma das mais importantes conclusões dessa decisão, o Tribunal Constitucional Federal alemão estabelece que:

> [Princípios Orientadores] 2. As restrições a este direito à "autodeterminação informacional" só são permitidas se elas servem a um interesse público derrogatório. Requerem uma base legal que deve ser constitucional e que deve satisfazer à exigência de clareza das normas do Estado de Direito. Ao elaborar a sua regulamentação, o legislador deve também observar o princípio da proporcionalidade. Ele também deve tomar precauções organizacionais e processuais para conter o risco de violação dos direitos de personalidade.[124] [125]

A autodeterminação informacional (*Informationelle Selbstbestimmung*) e o conceito da restrição do tratamento à finalidade declarada e de forma proporcional serão abordados em mais detalhes ao longo deste trabalho. Para o momento, basta sinalizar o quão importante a construção legal e jurisprudencial alemã se apresentou já no início da década de 80.

Em 28 de janeiro de 1981 foi aberta para assinatura de países-membros e adesão de países não membros a Convenção nº 108, que foi ratificada pela República Federativa da Alemanha em 19 de junho de 1985 (França, Espanha, Noruega e Suécia já haviam a ratificado inicialmente) e entrou em vigência em 1º de outubro de 1985. O status entre assinaturas e adesões no momento de elaboração deste trabalho é de 55 países[126].

A Convenção nº 108 foi "o primeiro instrumento internacional legalmente vinculante no tema de proteção de dados"[127]. Este instrumento exigia que as partes elaborassem legislação nacional para aplicar os princípios estabelecidos na Convenção e buscar a garantia de respeito pelos direitos humanos e fundamentais de todos os indivíduos com relação ao processamento de dados pessoais[128].

---

[124] Tradução livre: Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

[125] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215. Disponível em: https://www.bverfg.de/e/rs19831215_1bvr020983.html. Acesso em: 20 jul. 2024.

[126] Council of Europe Treaty Office. **Chart of signatures and ratifications of Treaty 108**. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108. Acesso em: 20 jul. 2024.

[127] Tradução livre: (…) was the first legally binding international instrument in the data protection field.

[128] Council of Europe. **Data Protection – Convention 108 and Protocols**. Disponível em: https://www.coe.int/en/web/data-protection/convention108-and-protocol. Acesso em: 20 jul. 2024.

Ustaran (2018, p. 11) afirma que:

> Na Convenção 108, o Conselho da Europa adotou a visão de que aqueles que mantinham e usavam informações pessoais na forma computadorizada tinham uma responsabilidade social de proteger tais informações pessoais, especialmente porque nessa altura, decisões que afetavam indivíduos eram cada vez mais baseadas em informações armazenadas em arquivos de dados computadorizados[129].

Apesar do objetivo pretendido pela Convenção 108 ser uma abordagem harmonizada à proteção de dados com base em um acordo internacional de princípios, sua implementação foi deixada para a discricionariedade dos países membros. Segundo Ustaran (2018, p. 13), "já nos dias mais iniciais, se tornou aparente que a implementação desses princípios em leis nacionais resultava no desenvolvimento de um conjunto diverso de regimes de proteção de dados"[130]. A consequência de tal deficiência coesiva seria de possíveis violações a direitos fundamentais de indivíduos, bem como dificuldades jurídicas frente o livre fluxo de dados pessoais na Europa.

Em 1986 o *Single European Act* revogou tratados anteriores criando um "mercado interno" (efetivo a partir de 1992) e conduziu a adoção de uma moeda única com o fim da regulamentação de fronteiras. Em 1992, o *Treaty on European Union (Maastricht Treaty)* estabeleceu, finalmente, a União Europeia.

A Comissão Europeia, desde 1976, sinalizava ao Parlamento Europeu a necessidade de preparar uma proposta para uma diretiva harmonizando as leis de proteção de dados. Uma diretiva, segundo Ustaran (2018, p. 13), seria "uma forma de legislação vinculante de estados membros, mas que deixaria para as autoridades nacionais a escolha da forma e métodos para implementação"[131].

---

[129] Tradução livre: In Convention 108, the Council of Europe took the view that those holding and using personal information in computerised form have a social responsibility to safeguard such personal information, particularly as that time, decisions were increasingly based on information stored in computerised data files.

[130] Tradução livre: From the earliest days, however, it became apparent that implementation of these principles into national law was resulting in the development of a diverse set of data protection regimes.

[131] Tradução livre: Directives are a form of legislation binding upon member states, but they leave to the national authorities the choice of form and methods for implementation.

Utilizando os princípios delineados na Convenção 108, este esforço da Comissão Europeia culminou com a publicação da Diretiva 95/46/EC[132] sobre a proteção de indivíduos com relação ao processamento de dados pessoais e o livre movimento de tais dados, também chamada de *Data Protection Directive* (Diretiva de Proteção de Dados, em tradução livre).

Mais uma vez houve acentuadas diferenças nos modos de implementação e aplicação da Diretiva conduzidos pelos países membros, resultando em insegurança jurídica e dificuldade no aproveitamento completo de benefícios do mercado interno da União Europeia (Ustaran, 2018, p. 14).

Alguns instrumentos jurídicos tocando o tema de proteção de dados pessoais foram elaborados e publicados na União Europeia ao longo dos anos seguintes, tais como a Diretiva 2000/31/EC, a Carta de Direitos Fundamentais da União Europeia (2000), a adição de um protocolo à Convenção 108 (2001), a Diretiva 2002/58/EC, a Diretiva 2006/24/EC, o Tratado de Lisboa de 2007 e a Diretiva 2009/136/EC. Entretanto, ainda em razão da falta de harmonização da abordagem à proteção de dados pessoais pelos estados membros, a União Europeia iniciou uma revisão da sua estrutura jurídica de proteção de dados em 2009, resultando em uma proposta em janeiro de 2012 para uma reforma da Diretiva 95/46/EC, desta vez na forma de um *General Data Protection Regulation* (Regulamento Geral de Proteção de Dados, em tradução livre), que "imporia um único conjunto de regras por toda a União Europeia" (Ustaran, 2018, p. 16).

Em 27 de abril de 2016, portanto, foi publicado o *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*[133] (Regulamento 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 sobre a proteção de pessoas naturais com

---

[132] EUR-Lex. **Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046. Acesso em: 20 jul. 2024.

[133] EUR-Lex. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)**. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 21 jul. 2024.

relação ao processamento de dados pessoais e do livre movimento de tais dados, e revogando a Diretiva 95/46/EC, em tradução livre).

Especialmente relevante para o nosso trabalho, é fundamental mencionar o *Council Framework Decision 2008/977/JHA* de 27 de novembro de 2008, que tratava da proteção de dados pessoais processados no contexto da cooperação policial e judicial em assuntos criminais. Tal decisão foi revogada pela Diretiva 2016/680 que trata da proteção de pessoais naturais com relação ao processamento de dados pessoais por autoridades competentes para os propósitos de prevenção, investigação, detecção ou persecução de ofensas criminais ou para a execução de penas criminais, no livre movimento de tais dados. Também foi publicada a Diretiva 2016/681 que trata do uso de dados do registro de nome de passageiro (*passenger name record* – PNR) para a prevenção, detecção, investigação e persecução de ofensas terroristas e crimes sérios. Em uma abordagem consistente pelo Conselho da Europa, todos estes instrumentos foram publicados simultaneamente na União Europeia, tanto o GDPR (Regulamento 2016/679), quanto as Diretivas 2016/680 e 2016/681, em 27 de abril de 2016.

Se faz importante notar que a União Europeia utilizou dois instrumentos de naturezas jurídicas distintas: um Regulamento Geral de Proteção de Dados (2016/679) e uma Diretiva de Proteção de Dados em matéria criminal (2016/280). Apesar de permitir que estados membros publiquem regras mais específicas que as determinadas no GDPR em algumas situações (Ustaran, 2018, p. 17), um Regulamento possui efeito amplamente vinculante nos estados membros a partir de sua entrada em vigor, diferentemente de uma Diretiva, que necessariamente demandava dos estados membros um prazo para que esta fosse transposta para leis nacionais. De acordo com o Tratado sobre o Funcionamento da União Europeia (2016/C 202/01), em seu artigo 288[134]:

> Para exercerem as competências da União, as instituições adotam regulamentos, diretivas, decisões, recomendações e pareceres.
> O regulamento tem caráter geral. É obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.
> A diretiva vincula o Estado-Membro destinatário quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios.

[134] Jornal Oficial da União Europeia. **Do Tratado da União Europeia e do Tratado sobre o Funcionamento da União Europeia.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:12016ME/TXT. Acesso em 23 jul. 2024.

> A decisão é obrigatória em todos os seus elementos. Quando designa destinatários, só é obrigatória para estes.
> As recomendações e os pareceres não são vinculativos.

A história da proteção dos dados pessoais no Brasil na forma de uma abordagem jurídica dedicada ao tema é bastante recente. Data de abril de 1980 a primeira tentativa de regulamentação (ainda que mínima) de tema referente à proteção de dados pessoais, o projeto de lei nº 2796/1980, da então deputada Cristina Tavares (PMDB/PE), que assegurava aos cidadãos "acesso as informações sobre sua pessoa constates de bancos de dados", dentre outras providências[135]. Apesar do arquivamento do projeto ocorrido ao final da legislatura, segundo Doneda (2021, p. 12):

> (...) a demanda de que fosse dada maior concretude a alguns direitos relacionados à proteção de dados, em especial os direitos de acesso e retificação, foi se intensificando e ressoava com o movimento de redemocratização da década de 1980, vindo a resultar, entre outros, na presença da ação de *habeas data* na Constituição de 1988.

Em 1988, o instituto do *habeas data* foi introduzido no ordenamento jurídico brasileiro por meio da ação constitucional disposta no art. 5º. LXXII, da Constituição brasileira, ao invés de instituto de direito material. Conforme Doneda (2021, p. 13), alguns intérpretes ressaltaram a "existência e de um direito material de acesso e retificação com relação aos dados pessoais, ainda que não expresso na literalidade na lei". Certamente é uma abordagem insuficiente do tema, especialmente quando comparada à abordagem dos estados membros da União Europeia na mesma época, conforme já abordamos anteriormente.

Ainda na Constituição brasileira de 1988, a inviolabilidade da vida privada foi alçada a direito fundamental, constando no art. 5º, X. Entretanto, em sede de lei ordinária, ao longo dos anos subsequentes, o direito à vida privada foi inserido no Código Civil (Lei 10.406/2012) em seu art. 21. O Código de Defesa do Consumidor (Lei 8.078/1990), em seu art. 43, estabelece, ainda, que de forma bastante restrita, direitos de acesso e retificação de dados pessoais, além de instituir alguns princípios de proteção de dados

[135] Câmara dos Deputados. **PL 2796/1980**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=206829. Acesso em: 21 jul. 2024.

(como a objetividade, clareza, veracidade e linguagem de fácil compreensão) quanto a cadastros e dados de consumidores.

Em 2011, duas leis nacionais se destacaram em sua conexão com o tema de proteção de dados: a Lei do Cadastro Positivo (Lei 12.414/2011) e a Lei de Acesso à Informação (Lei 12.527/2011). Em 2014, um importante marco foi estabelecido, o Marco Civil da Internet (Lei 12.965/2014, posteriormente regulamentada pelo Decreto 8771/2016), que “implementou uma série de direitos e procedimentos relacionados ao uso de seus dados pessoais, ainda que a sua sistemática e sua gramática não sejam facilmente reconduzíveis aos institutos de proteção de dados nos moldes da LGPD e de outras normativas congêneres” (Doneda, 2021, p. 14).

Uma vez que o texto do Marco Civil da Internet informa em seu Art. 3º, III, que a disciplina do uso da internet no Brasil tem como princípio, dentre outros, “a proteção dos dados pessoais, na forma da lei”, conforme Doneda (2014, p. 14), “o Marco Civil da internet já acenava para legislação própria sobre proteção de dados, que lhe seria posterior”.

Os primeiros passos brasileiros que deram origem a LGPD datam de 2005, no âmbito do Mercosul, com as atividades do Subgrupo de Trabalho de número 13 (SGT13). Um primeiro Anteprojeto de Lei Geral de Proteção de Dados Pessoais foi elaborado em 2011, tendo revisões e aperfeiçoamentos até 2015, quando sua segunda versão foi apresentada sendo protocolada na Câmara dos Deputados como PL 5.276/2016 (Doneda, 2021, p. 16). Paralelamente, tanto a Câmara dos Deputados, principalmente por meio do PL 4.060/2012, quanto o Senado, principalmente por meio do PLS 330/2013, já tinham outros projetos de lei abordando o tema de proteção de dados pessoais e seguiam sua regular (e lenta) tramitação de aprovação.

Por meio de uma comissão especial da Câmara dos Deputados com relatoria do deputado Orlando Silva, após diversas audiências públicas, em 29 de maio de 2018 foi aprovado o parecer da comissão, com a matéria seguindo para o Senado identificado como PLC 53/2018 (Doneda, 2021, p. 16).

Não se sabe ao certo se a previsão desde 2016 para entrada em vigor do Regulamento Geral de Proteção de Dados europeu (RGPD, ou GDPR no acrônimo anglófono) em 25 de maio de 2018 teve papel decisivo em todo este processo, uma vez

que havia intensa insegurança jurídica quanto ao aspecto de “ilegalidade” que poderia revestir os tratamentos de dados pessoais entre Brasil e União Europeia, especialmente a transferência internacional de dados e a oferta de bens e serviços entre os países, mas requerimento de urgência foi realizado em julho para a apreciação do Plenário do Senado Federal e, após sua aprovação, seguiu para sanção presidencial. A Lei Geral de Proteção de Dados Pessoais brasileira foi promulgada (com vetos), portanto, em 14 de agosto de 2018, adquirindo vigência em 19 de setembro de 2020 após algumas modificações legislativas ocorridas neste interstício.

Sarlet (*in* Doneda, 2021, p. 26) reforça que “é imperioso citar a relevância do RGPDE par a elaboração da LGPD, que incorporou uma série de institutos, princípios e regras da normativa europeia”.

Uma controvérsia (e certa insegurança jurídica), entretanto, ganhou forma e se expandiu gradativamente na discussão jurídica envolvendo a proteção de dados pessoais no Brasil. Ao passo que enquanto a vida privada e a intimidade eram consideradas invioláveis enquanto direitos fundamentais (CRFB, art. 5º, X), a proteção de dados pessoais conferida pela LGPD, naturalmente, tinha *status* infraconstitucional. Em parte, devido à certa confusão com relação aos bens jurídicos em questão, uma discussão foi travada sobre o direito à proteção de dados pessoais ser reconhecido como direito fundamental no Brasil.

Em 2018 uma Medida Provisória foi editada obrigando as operadoras de telefonia a repassarem dados identificados de seus consumidores de telefonia móvel para o IBGE. Estes dados incluíam o número do celular e endereço. Vícios de inconstitucionalidade foram suscitados e Ações Diretas de Inconstitucionalidade (nº 6387, 6388, 6389, 6393, 6390) foram ajuizadas para suspensão de aplicação de tal Medida.

A decisão proferida pelo Plenário do Supremo Tribunal Federal, chancelando provimento monocrático, em sede de liminar, da ministra Rosa Weber no bojo da ADI 6.387 MC-Ref/DF, julgamento em 6 e 7 de maio de 2020, abordou a centralidade do tema da proteção de dados na manutenção da democracia (mencionando, inclusive, a decisão do *Bundesverfassungsgericht* no caso emblemático do Censo alemão de 1983), foi acolhido como um reconhecimento do direito fundamental autônomo à proteção de dados pessoais.

Questionamentos quanto a validade constitucional desse “reconhecimento de um direito fundamental implicitamente positivado” da suprema corte brasileira foram suscitados por alguns juristas (em contraposição aos aplausos da imensa maioria), entretanto, por fim, tal direito foi expressamente positivado na Constituição por meio da aprovação da Emenda Constitucional nº 115, de 10 de fevereiro de 2022, que o incluiu no inciso LXXIX do Art. 5º.

Adotamos o entendimento que o aludido direito fundamental à proteção de dados é, na verdade, a proteção conferida a um feixe de direitos fundamentais. Conforme Gleizer, Montenegro e Viana (2021, p. 37), “há *vários* [grifo do autor] direitos fundamentais conformando a proteção de dados pessoais em um regime geral de proteção da personalidade (sigilo das telecomunicações, autodeterminação informacional etc.)”.

3.7 A proteção da privacidade e proteção de dados pessoais enquanto direito fundamental

De acordo com Luis Greco (*in* Wolter, 2018, p. 35), “segundo a concepção alemã, os direitos fundamentais são, em primeiro lugar, Abwehrrechte, *direitos de defesa ou de proteção* [grifo do autor], dirigidos contra o Estado”. De fato, na dogmática jurídica alemã dos direitos fundamentais, o *Bundesverfassungsgericht* manifesta tal entendimento claramente no julgamento[136] envolvendo a restrição ao direito fundamental de liberdade de expressão no caso de Veit Harlan, um produtor de filmes durante o regime Nazista, tendo como um de seus maiores trabalhos o filme antissemita Jud Süß, afirmando que “d*ie Grundrechte sind in erster Linie Abwehrrechte des Bürgers gegen den Staat*” (Os direitos fundamentais são, em primeiro lugar, direitos de resistência dos indivíduos contra o Estado, em tradução livre). Ainda, segundo Greco (*in* Wolter, 2018, p. 36), “a chamada *eficácia horizontal ou diante de terceiros* [grifo do autor] (*Drittwirkung*) permanece excepcional”.

[136] BVerfG, Urteil des Ersten Senats vom 15. Januar 1958 - 1 BvR 400/51 -, Rn. 1-75. Disponível em: https://www.bverfg.de/e/rs19580115_1bvr040051.html. Acesso em 24 jul. 2024.

De modo geral, há previsão constitucional para as espécies de limitações que podem ser impostas aos direitos fundamentais. Segundo Dimitri Dimoulis e Leonardo Martins (2020, p. 189), “a área de proteção do direito é invadida *em princípio* [grifo do autor] de forma permitida (intervenção permitida)”. Porém, há um processo de justificação constitucional da “imposição concreta do limite previsto na Constituição” (Dimitri; Martins, 2020, p. 189). Há, adicionalmente, uma reserva legal que “permite ao legislador comum introduzir limitações, restringindo a área de proteção do direito fundamental” (Dimitri; Martins, 2020, p. 192).

O dever do Estado perante esse feixe de direitos fundamentais concentrados no direito fundamental à proteção de dados pessoais é de abstenção, uma vez que, primeiramente, são direitos de resistência do indivíduo perante o próprio Estado. De acordo com Gleizer, Montenegro e Viana (2021, p. 39), “não se trata de, em primeira linha, obrigar o Estado a conferir proteção aos dados, senão de dotar os dados com proteção intrínseca contra a ingerência do Estado”. Portanto, continuam os autores, “exceções a essa regra geral têm de ser especialmente justificadas a título de *intervenções* [grifo do autor] nessa esfera protegida” (Gleizer; Montenegro; Viana, 2021, p. 39).

De acordo com Dimitri e Martins (2020, p. 180), “a dogmática dos direitos fundamentais tem como início e como ponto de chegada o choque de interesses causado pela concretização de direitos fundamentais”. Esse “choque de interesses” pode ocorrer entre os titulares desses direitos, entretanto, pode ocorrer entre o titular de direitos e quem possua “interesses gerais que constitucionalmente têm o condão de limitá-los”, ou seja, o próprio Estado.

Tais intervenções são admitidas porque, conforme José Adércio Leite Sampaio (1998, p. 363) ensina, “os direitos fundamentais não são nem ilimitados, nem absolutos. E não o são por uma razão intrínseca: a multiplicidade de aspectos e projeções valorativas dos direitos humanos que pode levar a situação de aparente conflito, imprimindo a necessidade de opção”.

Limitações ou restrições podem ocorrer diretamente mediante prescrições constitucionais expressas, indiretamente por meio de leis infraconstitucionais por

autorização expressa da Constituição ou por exigência de interpretação em casos concretos não solucionáveis pelos dois meios anteriores (Sampaio, 1998, p. 365).

A possibilidade de intervenção em matéria constitucional que confere direitos fundamentais e a legislação infraconstitucional é uma “relação complexa”, conforme Dimitri e Martins (2020, p. 186), entretanto, em razão do “caráter genérico e abstrato das normas de direitos fundamentais (baixa densidade normativa), torna-as dependentes do legislador ordinário, que as concretiza e (...) necessariamente as limita mediante a concretização”.

As normas que garantem direitos fundamentais são reflexivas, significa dizer que são direcionadas para observância e cumprimento pelo próprio Estado. Dimitri e Martins (2020, p. 180) afirmam que são reflexivas “porque há, em primeira linha, identidade entre o criador e o destinatário da norma: o Estado”. Há, também, a dupla reflexividade, sendo essa a “satisfação da pretensão de uma parte que impede, de forma reflexiva, a satisfação da pretensão da outra”, caracterizando a eficácia horizontal indireta.

Eventualmente, em razão do “imperativo jurídico de proteger os indivíduos e a sociedade e de promover os fins que lhe incumbem, o Estado pode ver-se forçado a adentrar, ou seja, a intervir nesses espaços individuais protegidos” (Gleizer; Montenegro; Viana, 2021, p. 41). Ainda, de acordo com Gleizer, Montenegro e Viana (2021, p. 41), dessa necessidade se extrai o conceito de normas autorizativas a fim de que o parlamento, por meio da adequada atividade legislativa, autorize tais intervenções em direitos fundamentais.

Segundo Dimitri e Martins (2020, p. 188), uma intervenção será permitida (constitucionalmente justificada) em quatro casos, a saber:

> a. Se o comportamento não se situar na área de proteção do respectivo direito (...).
> b. Quando uma norma infraconstitucional restringe o direito fundamental de forma permitida pela Constituição mediante concretização de uma “reserva legal” positivada pelo constituinte junto ou lofo após a outorga de um direito fundamental (...).
> c. Se representar a *concretização* [grifo do autor] de um limite constitucional derivado do chamado direito constitucional de colisão (...).
> d. Se dois direitos fundamentais ou um direito fundamental do indivíduo e um princípio de interesse geral colidirem quando da aplicação de normas do direito infraconstitucional (DIMITRI; MARTINS, 2020, p. 188).

Ressaltam, ainda, Dimitri e Martins (2020, p. 188) que no quarto caso, “sua atualização dá-se, em regra, no momento da interpretação e da aplicação judicial de normas infraconstitucionais que, explícita ou tacitamente, regulamentem a colisão entre direitos fundamentais ou entre estes e outros bens jurídico-constitucionais objetivos”.

Ocorre que diversas limitações aos direitos fundamentais são permitidas mediante uma condição, uma ressalva, tecnicamente chamada de reserva legal. A reserva legal, conforme Dimitri e Martins (2020, p. 192) pode ser classificada como reserva legal simples ou reserva legal qualificada. A reserva legal simples é caracterizada como a regulamentação, o exercício do direito, que será realizada “na forma da lei” ou “nos termos da lei”. Já a reserva legal qualificada ocorre quando “a própria Constituição indica ao menos um dos seguintes elementos: o tipo, a finalidade ou o meio de intervenção autorizados, dos quais o legislador poderá se valer quando da sua concretização (...)”.

Dimitri e Martins (2020, p. 193) ainda mencionam que existem “algumas poucas reservas legais cuja classificação depende da interpretação de seus elementos conceituais constitutivos”, além da possibilidade de autorização de uma limitação ser tácita (ou indireta), “quando a Constituição não utiliza a fórmula ‘nos termos da lei’ ou outra semelhante (...)”. Entretanto, nos interessam as modalidades de reserva legal simples e qualificada para o presente trabalho.

A experiência da dogmática alemã em termos de direitos fundamentais e a Lei Fundamental é abordada por Luis Greco (*in* Wolter, 2018, p. 31), que menciona três etapas necessárias para a análise desse tema. A primeira etapa seria o estabelecimento do âmbito de proteção (*Schutzbereich*) do direito fundamental. Esta etapa de delimitação, conforme Dimitri e Martins (2020, p. 190) é a “concretização, conformação ou configuração” do direito fundamental e, segundo os autores, “qualquer concretização de um direito pode significar sua limitação”.

Fixado seu âmbito de proteção, na segunda etapa será determinado o conceito de intervenção (*Eingriff*) e, na terceira etapa, o de justificação (*Rechtfertigung*) (Wolter, 2018, p. 32). Fica claro, portanto, que a justificação é necessária para a intervenção, sendo que, conforme Greco (*in* Wolter, 2018, p. 32), “uma intervenção não justificada é que se chama de *lesão* ou *violação* [grifo do autor] (*Verletzung*) a direito fundamental”.

Não existindo nenhuma dessas hipóteses autorizativas de intervenções em direitos fundamentais, qualquer intervenção adquire caráter de intervenção proibida, que viola a própria Constituição. Gleizer, Montenegro e Viana (2021, p. 32) sintetizam precisamente este fundamento da dogmática constitucional afirmando que “se, por um lado, direitos fundamentais não são absolutos, por outro, tampouco podem ser violados. O fato de um direito ser *juridicamente inviolável* [grifo do autor] significa que ele só pode ceder se houver uma *justificação* [gripo do autor] jurídica”.

3.8 Intervenção do Direito Penal na privacidade e proteção de dados pessoais

A fim de esclarecer interpretações simplistas, reducionistas do tema, Greco (*in* Wolter, 2018, p. 33) ensina que “inviolável e intocável, na terminologia alemã, não são sinônimos”. De fato, ensinam Gleizer, Montenegro e Viana (2021, p. 33), “inviolabilidade significa vedação a intervenções injustificadas”, conforme abordamos anteriormente. Isso não significa, porém, que o direito fundamental seja intocável. Ele pode sofrer intervenções, desde que estas estejam dentro das hipóteses autorizativas. Neste sentido, podemos afirmar, sim, que todo direito fundamental é inviolável, considerando todo o contexto do que uma violação, de fato, representa.

Há, entretanto, o entendimento que o cerne, o núcleo dos direitos fundamentais, este, sim, é intocável, não comportando limitações, intervenções. A Lei Fundamental alemã aborda explicitamente tal distinção, estabelecendo o que é inviolável (*Unverletzlich*) e o conteúdo essencial (*Wesensgehalt*) de um direito fundamental que é intocável (Wolter, 2018, p. 32). É de Greco (*in* Wolter, 2018, p. 32) o exemplo que trazemos: uma intervenção na dignidade humana por meio de tortura não pode ser considerada lícita, “se há intervenção na dignidade humana, há lesão à dignidade”. Na Constituição brasileira, encontra-se disposta no art. 60, § 4º a manifestação em prol de uma proteção absoluta ao conteúdo essencial dos direitos fundamentais.

Ainda sobre a reserva legal, neste tema reside importante análise a ser realizada a respeito do que pode ser considerado “lei” para autorizar a limitação de direitos fundamentais. A questão principal se refere em compreender se o termo “lei” se refere ao seu sentido material como qualquer norma editada pelos poderes Legislativo e

Executivo, ou se o termo seria adequado às leis formais que tenham sido aprovadas pelo poder legislativo.

Na sua forma positiva, a Constituição se refere à “lei” autorizada a limitação de direito fundamental mediante o ato legislativo. Nesse sentido, conforme Dimitri e Martins (2020, p. 202), “há verdadeira reserva legal”, uma reserva legal de competência parlamentar (*Parlamentsvorbehalt*). Concordam Gleizer, Montenegro e Viana (2021, p. 43) ao afirmar que “outra consequência dos fundamentos de reserva de lei e parlamentar é que a CF (art. 5º, II), assim como grande parte de suas equivalentes estrangeiras, não faz concessões por meio de portarias, regulamentos, decretos ou outro ato normativo diferente de lei”.

Conforme Dimitri e Martins (2020, p. 203):

> A doutrina alemã desenvolveu, para controlar essa delegação, a “teoria da essencialidade” (*Wesentlichkeitslehre*), segundo a qual a delegação, para intervir na área de proteção de um direito fundamental, deve atender a três condições: (a) existência de lei ordinária delegadora em si constitucional; (b) as decisões “essenciais” (daí a teoria da “essencialidade”) sobre pressupostos, contextos e consequências das intervenções devem ser disciplinadas pelo *próprio* [grifo do autor] Poder Legislativo (*Parlamentsvorbehalt* – “reserva parlamentar”), sendo vedada sua delegação; (c) a essencialidade das intervenções mede-se a partir da intensidade com a qual tais intervenções atingirão os direitos fundamentais.

Apesar de no Brasil haver previsão para delegação do poder Legislativo ao Poder Executivo em âmbito federal por meio da lei delegada (CF, art. 68), em âmbito constitucional não deve ser admitida tal delegação.

Assim, delegar a limitação a direitos fundamentais de reserva legal e parlamentar a qualquer outro agente que não seja do Poder Legislativo e dentro do procedimento democrático legislativo não é uma hipótese a ser considerada viável, adequada ou legítima. Gleizer, Montenegro e Viana (2021, p. 45) fazem coro a esse entendimento concluindo que:

> Assim, um dos pontos cruciais do exercício interventivo informacional da segurança pública e do processo penal é o respeito à reserva de lei e à reserva parlamentar, enquanto salvaguardas essenciais dos direitos fundamentais, aqui, sobretudo, os de personalidade. Não há como juízes, policiais, ou órgãos da administração pública superarem a ausência de uma autorização expressa e clara do parlamento, ainda que creiam fortemente fazê-lo por razões justas e de forma ponderada.

Aqui se faz uma importante distinção que, por vezes, parece confundir os agentes estatais. Ainda que seja atribuída a determinado agente estatal determinada "competência", isso não acarreta automática "autorização" para realização de medida de intervenção em direitos fundamentais. Greco (*in* Wolter, 2018, p. 37) adverte que "desde a metade do séc. XX a doutrina publicista alemã assentou *a impossibilidade de derivar de uma competência uma autorização* [grifo do autor] (*kein Schluss von der Aufgabe auf die Befugnis*)". Portanto, quanto ao fundamento legal como pressuposto de medidas de intervenção em direitos fundamentais, norma de competência não se confunde com norma de autorização, ou seja, é indispensável que haja a devida autorização legal para o exercício da competência atribuída ao agente estatal.

As normas de competência se prestam a definir incumbências aos entes estatais, de modo que não haja interferências no desempenho das atividades que deverão respeitar limites a prestar as devidas contas legais em um autêntico exercício do princípio de responsabilização. Já as normas autorizativas, estas devem ser específicas e determinadas para a finalidade legal a qual se propõem intervir. Concluímos, assim, que é fundamental que a autorização para intervenção em matéria de privacidade e proteção de dados pessoais seja regulamentada por meio de legislação específica aplicada às atividades de qualquer órgão do Estado que tenha competência para atuação jurídico-penal.

Entretanto, uma das mais importantes questões a serem analisadas no tema é "como" estabelecer as definições estruturantes de tal legislação de modo a promover a adequada proteção aos bens jurídicos inerentes à privacidade e proteção de dados dos indivíduos. Para realização dessa análise, abordaremos a teoria do bem jurídico, os princípios constitucionais penais e utilizaremos como base alguns fundamentos contidos na Lei Geral de Proteção de Dados pessoais brasileira, a Lei 13.709/2018. A União Europeia realizou algo semelhante, mantendo uma estrutura muito semelhante entre a *Lex Regulation* 2016/679 (GDPR) e a Diretiva 2016/680, ambas já abordadas neste trabalho anteriormente. Continuaremos, adicionalmente, a comparar, quando pertinente, ao que é adotado pela dogmática alemã na proteção de dados pessoais em matéria penal, pelas razões já anteriormente descritas.

Gleizer, Montenegro e Viana (2021, p. 72) afirmam que, apesar de aparentar um caminho natural dada a “proximidade” do GDPR com a LGPD, “sobram razões” para não utilizarmos como base a Diretiva europeia 2016/680 na elaboração de legislação brasileira sobre o tema. Conforme já abordamos anteriormente neste trabalho, embora a União Europeia (2019, p. 7) seja uma “união única econômica e política entre 28 países Europeus”[137], seus Estados Membros todos permanecem estados soberanos e independentes (2018, p. 8) e temas de particular sensibilidade e especificidade, como o tema penal, não são inteiramente integrados e uniformes.

A promulgação de uma Diretiva sobre o tema (2016/680) revela o grande esforço (e, claramente, enorme hesitação) da União Europeia na tentativa de uniformização da abordagem, de integração entre tantos e diversos Estados Membros, suas diferentes culturas, instituições e institutos penais. Em nosso caso, obviamente não temos realidade ou desafios semelhantes, uma vez que tratamos de ordenamento jurídico unicamente nacional (e de competência legislativa da União).

A atuação Estatal na prevenção (segurança pública), inteligência e na persecução penal (investigação, inquérito, processo penal e execução penal) deve ser pautada principalmente pelo princípio da legalidade, com atuação na forma da lei. Entretanto, outros princípios se destacam na atuação penal do Estado, especialmente nas situações em que haja necessidade de atuação invasiva, quando precise “invadir” as esferas de proteção do indivíduo e de preciosos bens jurídicos que estas esferas visam preservar. Quanto mais invasiva a medida de redução do âmbito de proteção, mais barreiras devem ser impostas para que a atuação do ente estatal seja absolutamente estrita. Neste sentido, se destaca a necessidade de erigir um conjunto de princípios que sejam orientadores da atuação do Estado na prevenção e persecução penal.

A compreensão do “problema” contemporâneo passa por conhecer com a máxima profundidade o próprio bem jurídico que estamos prestes a abordar. Tendo abordado o conceito de privacidade e proteção de dados pessoais, fizemos uma síntese de sua história enquanto bem jurídico, sua elevação a direito humano e, finalmente, a direito

[137] Tradução livre: The European Union is a unique economic and political union between 28 European countries.

fundamental no ordenamento jurídico brasileiro constituindo verdadeiro bem jurídico constitucional-penal.

4 PRINCÍPIOS ADEQUADOS À PROTEÇÃO DO BEM JURÍDICO CONSTITUCIONAL-PENAL

A Lei Geral de Proteção de Dados Pessoais (LGPD – Lei 13.709/2018), quanto ao conteúdo principiológico, apresenta em seu art. 6º os princípios que deverão ser observados na realização de atividades de tratamento de dados pessoais. São 10 princípios, além da boa-fé, que abordaremos em maior detalhamento quanto à sua adequação a uma legislação de proteção de dados pessoais em matéria jurídico-penal.

Antes de abordarmos os princípios detalhadamente, cabe uma breve ressalva sobre esta pesquisa. Engana-se (ou se deixa ser enganado) quem cogita a possibilidade de que os efeitos do Direito Penal (e todo o seu arsenal de poder: investigação, persecução, processo, execução etc.) se esgota no tema da prisão. Ilustrando a questão, ao mencionar as medidas interventivas nos direitos fundamentais que podem ser adotadas pelo Estado, Greco (*in* Wolter, 2018, p. 60) afirma que na Alemanha:

> (..) tem-se preferido o termo intervenções processual-penal em direitos fundamentais (*strafprozessuale Grundrechteingriffe*), o que tem a dupla vantagem de fazer mais justiça às medidas investigativas, cujo cerne, diferentemente das medidas clássicas da prisão, da busca e da apreensão, não está em um exercício de força física.

Passemos aos princípios pois, conforme lembra Mariano da Silva (2005, p. 40), “não há como ser estudada a tutela penal de qualquer bem jurídico sem fazer alusão aos princípios constitucionais penais explícitos e implícitos”.

4.1 Princípio da Finalidade

A LGPD institui como seu primeiro princípio, não por acaso, o princípio da finalidade, onde determina que as atividades de tratamento de dados pessoais devem ser realizadas para “para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades”.

A violação deste princípio é uma das principais violações em matéria de proteção de dados pessoais. Daniel Solove (2006, p. 518), que aborda esta violação sob o nome de “uso secundário”, referenciando o relatório produzido pelo *U.S. Department of Health, Education and Welfare* em 1973, extrai a afirmativa que “deve existir uma maneira para um indivíduo prevenir informações sobre si que foram obtidas para um propósito de serem utilizadas ou tornadas disponíveis para outros propósitos sem seu consentimento”[138]. Ainda, segundo Solove, “este princípio, que se tornou conhecido como princípio de especificação de finalidade, foi incorporado em várias leis e princípios de privacidade”[139].

A dogmática alemã aborda tal questão por meio do princípio da vinculação finalística (*Zweckbindung*). O julgamento do Censo Alemão de 1983 já abordava naquela ocasião esta vinculação:

> A obrigação de fornecer dados pessoais pressupõe que o legislador determine precisamente, para cada assunto, a finalidade da utilização; adicionalmente, que a informação obtida seja adequada e necessária para atingir estas finalidades. A coleta de dados não anonimizados para finalidades indefinidos ou ainda indeterminávels não seria compatível com este objetivo. Adicionalmente, é imperativo que todos os órgãos públicos que coletam dados pessoais no exercício de suas funções terão também de se limitar ao mínimo necessário para atingir a finalidade declarada[140] (BVerfGE 65, 153)[141].

Portanto, é nítido que o tratamento de dados pessoais por órgãos da administração pública deve ter finalidade previamente definida e autorizada por lei. Qualquer outra atividade de tratamento, ou até a mesma atividade de tratamento, entretanto para finalidade diversa da que motivou especificamente aquela intervenção, deve ser

---

[138] Tradução livre: There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
[139] Tradução livre: This principle, which has become known as the purpose specification principle, has been embodied in various privacy principles and laws.
[140] Tradução livre: Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. Auch werden sich alle Stellen, die zur Erfüllung ihrer Aufgaben personenbezogene Daten sammeln, auf das zum Erreichen des angegebenen Zieles erforderliche Minimum beschränken müssen.
[141] BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215. Disponível em: https://www.bverfg.de/e/rs19831215_1bvr020983.html. Acesso em: 31 jul. 2024.

considerada ilegal. Uma nova finalidade implica uma nova intervenção, uma nova intervenção requer nova autorização legal.

Luís Greco (*in* Wolter, 2018, p. 44), ao mencionar este princípio abordado pela decisão do Censo Alemão de 1983, confirma que:

> Se o indivíduo tem de ser protegido de condutas estatais como a *obtenção,* o *armazenamento,* a *utilização* e a *transferência de dados* [grifo do autor], as quais têm de encontrar limites, isso significa que essas quatro fases do processamento de informações são intervenções e, principalmente, que elas são intervenções de natureza autônoma: uma norma que autoriza a obtenção de um dado não autoriza já automaticamente a utilização o armazenamento, muito menos a transferência. Necessita-se de uma norma para cada uma das quatro fases.

Entretanto, tal posição não é defendida por todos os pesquisadores do tema. Wimmer (2021, 138) afirma que

> Com base na experiência internacional e à luz do próprio texto da LGPD, é possível compreender que não haveria impedimentos a priori ao compartilhamento de dados com vistas ao tratamento de dados pessoais para finalidades compatíveis com aquelas que justificaram a coleta original, desde que observadas as regras procedimentais e, principalmente, os princípios aplicáveis ao tratamento de dados pessoais, tais como a necessidade, a adequação e a transparência. É certo, por outro lado, que a indeterminação e a abertura do conceito de “compatibilidade” indicam a premência do desenvolvimento de parâmetros mais objetivos para sua aferição nos casos concretos.

Ainda, (Wimmer, 2021, p. 139) mencionando o julgamento do STF no caso da MP 954 (que que determinava o compartilhamento de dados entre empresas de telecomunicações e o IBGE) e a decisão monocrática proferida na ADPF 695, acrescenta que:

> De ambas as decisões, é possível extrair a ideia de que ainda que se possa, em determinadas circunstâncias, admitir o compartilhamento de dados pessoais no âmbito do poder público com mudança das finalidades que justificaram sua coleta, não basta simplesmente conferir um verniz de legalidade para formalmente justificar tal uso secundário. É necessário, ao invés, o estabelecimento de salvaguardas materiais e procedimentais e a observância de todo o conjunto de direitos e princípios associados à proteção de dados pessoais, justificando-se, claramente, o interesse público específico a ser atingido, tendo em vista os parâmetros protetivos conferidos pelos princípios constitucionais que asseguram a liberdade individual, a privacidade e o livre desenvolvimento da personalidade.

Apesar da autora não tratar especificamente do tema de proteção de dados pessoais em matéria penal, ainda assim, discordamos de tal posição, especialmente em matéria penal, uma vez que a observância da dogmática dos direitos fundamentais, dos princípios constitucionais penais e da elevada necessidade de proteção dos bens jurídicos envolvidos intrínseca à toda a dogmática penal, não comporta tais exceções.

4.2 Princípio da separação informacional

A emblemática e paradigmática decisão alemã do Censo de 1983 apresenta fundamentos sólidos que guiaram (e continuam guiando) a dogmática constitucional e, consequentemente, penal, quanto aos princípios e regras atinentes à proteção da privacidade e proteção de dados pessoais.

O Tribunal Constitucional Federal alemão (*Bundesverfassungsgericht*) reforçou importante princípio ao determinar que:

> (1) As pessoas empregadas no processamento de dados dentro do escopo do Parágrafo 1 (2) ou em nome das pessoas ou órgãos mencionados nessa seção estão proibidas de processar, divulgar, tornar acessível ou de outra forma usar dados pessoais protegidos sem autorização para qualquer finalidade que não seja o cumprimento legal das suas respectivas funções[142] (BVerfGE 65, 69).

O "cumprimento legal de suas respectivas funções" se refere à separação de poderes instituído na Alemanha pelo modelo determinado pela Lei Fundamental da Alemanha de 1949. O Brasil adotou sistema semelhante de separação (ou divisão) de poderes, inspirado pela tradição norte-americana (que se inspirou nas ideias de Montesquieu) e pelo modelo alemão (Sarlet, 2023, p. 35).

A importância dessa divisão é explicada por Dallari (1998, p.78), quando afirma que "quando se pretende desconcentrar o poder, atribuindo o seu exercício a vários órgãos, a preocupação maior é a defesa da liberdade dos indivíduos, pois, quanto maior for a concentração do poder, maior será o risco de um governo ditatorial".

---

[142] Tradução livre: (1) Den im Rahmen des § 1 Abs. 2 oder im Auftrag der dort genannten Personen oder Stellen bei der Datenverarbeitung beschäftigten Personen ist untersagt, geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen.

Foi proposta a Ação Direta de Inconstitucionalidade de nº 6529, julgada em outubro de 2021[143], em face do parágrafo único do art. 4º, do §1º do art. 2º e do art. 9º-A da Lei n. 9.883/1999, e, por "arrastamento", do §3º do artigo 1º do Decreto nº 10.445/2020. Em suma, pedia-se a "a declaração parcial de inconstitucionalidade da norma, sem redução de texto", para afastar as hipóteses de compartilhamento [com a ABIN] de "informações sujeitas à reserva de jurisdição, incluindo dados fiscais, bancários, telefônicos, bem como as informações de inquéritos policiais ou da base de dados da Receita Federal e do COAF" a partir de "órgãos integrantes de outros entes federados, de outros Poderes e do Ministério Público" e o afastamento da "proibição de acesso pelas Polícias Judiciárias e pelo Ministério Público às informações produzidas pelas atividades de inteligência, em caso de procedimento investigatório aberto pela autoridade policial/acusatorial para apurar esta atividade", inclusive "pelas pessoas que sejam alvos das atividades de inteligência, garantindo-lhes o acesso às informações".

A Ministra Carmen Lúcia, ao julgar a ADI 6529, afirma:

> O fornecimento de informações entre órgãos públicos para a defesa das instituições e dos interesses nacionais é ato legítimo. É proibido que se torne subterfúgio para atendimento ou benefício de interesses particulares ou pessoais, especialmente daqueles que têm acesso aos dados, desvirtuando-se competências constitucionalmente definidas e que não podem ser objeto de escolha pessoal, menos ainda de atendimento a finalidade particular de quem quer que seja. Também porque essas finalidades são, em geral, criminosas e têm o sentido de agressão a outrem, atentando contra os direitos fundamentais.

Afirma, ainda, que "As atividades de inteligência, ainda que pelo sigilo, se submetem ao escrutínio externo dos demais Poderes (Legislativo e Judiciário), devendo ser afastada qualquer interpretação que dê margem a arbitrariedades".

Sarlet (2023, p. 36) conclui que, neste sentido:

> A separação informacional de poderes consiste em uma ressignificação, tanto lógica quanto necessária, da semântica do princípio da divisão de poderes (art. 2º, CF) à luz do constitucionalismo digital, tendo em vista o atual estado de compartilhamento dos dados em poder do Estado brasileiro que (...) implica uma separação nítida entre as diversas áreas de atuação estatal sob pena de descumprimento de um preceito fundamental e, consequentemente, uma

[143] Supremo Tribunal Federal. **ADI 6529**. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15348384228&ext=.pdf. Acesso em: 01 ago. 2024.

> violação das exigências essenciais do Estado Democrático de Direito (SARLET, 2023, p. 36).

A separação informacional, enquanto princípio de concretização do Estado Democrático de Direito, adquiriu especial relevância desde o advento das tecnologias de processamento automatizado de dados. A decisão do Censo de 1983 (BVerfGE 65, 150) proferida pelo Tribunal Constitucional Federal alemão (*Bundesverfassungsgericht*) explicitou nitidamente (já naquela época) que no contexto da demanda de dados pessoais pelo Estado:

> Não é suficiente simplesmente avaliar o tipo de informação que está sendo demandada. O fator decisivo é como os dados podem ser usados, e para quais hipóteses de utilização. Isso depende, por um lado, da finalidade para a qual os dados são coletados e, por outro lado, das possibilidades de processamento e vinculação inerentes à tecnologia da informação[144].

O poder computacional que iniciava seu desenvolvimento na década de 1980 já sinalizava ao Tribunal Constitucional Federal alemão a especial atenção que o tema da proteção da privacidade e de dados pessoais demandaria nos anos por vir. Se naquela ocasião as possibilidades já assustavam, poucos seriam capazes de vislumbrar (a não ser para roteirização de filmes de ficção científica) o poder computacional que atingiríamos no séc. XXI e os caminhos inesgotáveis que se apresentam com a exploração da Inteligência Artificial.

Novos paradigmas computacionais têm sido estabelecidos por meio do desenvolvimento de diversas novas tecnologias de computação, conforme listado por Gill *et al* (2024, p.24): *Cloud computing, autonomic computing, mobile cloud computing, green cloud computing, fog computing, edge computing, mobile edge computing, serverless computing, osmotic computing, dev computing, quantum computing* são algumas tecnologias utilizadas na era do advento da Inteligência Artificial acessível por todos.

Novos modelos computacionais são utilizados para acelerar e favorecer o aprendizado de máquina (*machine learning*) e, diferentemente de um modelo de

[144] Tradução livre: Dabei kann nicht allein auf die Art der Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten ab.

aprendizado em que os dados se encontram em uma base centralizada, modelos federados de aprendizado (*federated learning*) são desenvolvidos para utilização de dados dispostos descentralizadamente. A grande questão, conforme apresentada por Gill *et al* (2024, p. 24) é: Como poderiam as organizações garantir privacidade em serviços de aprendizado federado?[145]

Dados são necessários para treinamento, teste e validação de modelos de ML [*Machine Learning*][146]" (Gill *et al*, 2024, p. 18) e a avidez por dados permeia tanto as entidades de direito privado quanto, especialmente, as entidades de direito público (conforme os casos já apresentados ao longo deste trabalho que demonstram esse "apetite" estatal). E conforme brilhantemente o Tribunal Constitucional Federal alemão (já nos idos de 1980) conclui, "portanto, dados que aparentem por si mesmos serem insignificantes podem ganhar nova relevância; no contexto do processamento automatizado de dados, não se pode mais assumir que exista dado insignificante"[147] (BVerfGE, 65, 150).

Os dados gerados por humanos para treinamento dos algoritmos, especialmente os dados pessoais em razão da sua própria natureza, são valiosos e se tornarão mais valiosos a cada época. Um recente estudo realizado por pesquisadores indicou que treinamento de algoritmos de IA (inteligência artificial) utilizando dados gerados por outros mecanismos de IA (por exemplo, dados gerados por IA que sejam disponibilizados em *sites* de internet) tendem a conduzir o modelo ao total colapso. Nesse contexto, "dados sobre interações humanas com Grandes Modelos de Linguagem (LLMs) serão cada vez mais valiosos[148] (Shumailov *et al*, 2024, p. 1).

A experiência alemã na separação informacional compreende, adicionalmente aos limites constitucionalmente impostos no desempenho legal das funções estatais, a especificação das atividades de tratamento de dados pessoais como intervenções autônomas individuais. Esta é uma abordagem que nos parece bem mais adequada ao contexto jurídico-penal, uma vez que a LGPD generaliza a abordagem por meio do

---

[145] Tradução livre: How could companies ensure privacy in federated learning service?
[146] Tradução livre: Data is needed for ML model training, testing and validation.
[147] Tradução livre: Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein "belangloses" Datum mehr.
[148] Tradução livre: (…) data about human interactions with LLMs will be increasingly valuable.

conceito de “atividades de tratamento”. Tratamento (ou atividade de tratamento de dados pessoais), de acordo com o art. 5º, X, da LGPD, pode ser considerado como sendo qualquer ação envolvendo dados pessoais, uma vez que o rol trazido pelo inciso é exemplificativo:

> Art. 5º Para os fins desta Lei, considera-se:
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A dogmática alemã optou por destacar atividades específicas como intervenções autônomas nos direitos fundamentais. Assim, as atividades de tratamento em sua forma genérica são chamadas *Datenverarbeitung*; a modificação de dados, *Datenveränderung*; o armazenamento de dados, *Datenspeicherung*; o compartilhamento dos dados, *Datenübermittlung*; a transmissão de dados, *Weitergabe*; o uso dos dados, *Datennutzung*; e aqui, uma abordagem terminológica diferente da adotada pela lei brasileira: o legislador optou por mencionar a atividade de coleta de dados (e essa terminologia foi incorporada de maneira geral para essa atividade), entretanto, a dogmática alemã optou pelo termo “levantamento de dados”, *Datenerhebung*.

De acordo com Gleizer, Montenegro e Viana (2021, p. 28), essa escolha acabou por resolver uma “ambiguidade de que não se trata de uma obtenção de dados seguida de armazenamento”. Entretanto, nos parece que o termo levantamento tem mais adequação ao contexto jurídico-penal em razão de que o termo coleta dispõe de sentido vinculado a uma recolha de algo que está disponível, que se apresenta. O termo levantamento se aproxima do sentido da busca pela informação, dos esforços para obtenção do que não está disponível. O Tribunal Federal Alemão (*Bundesverfassungsgericht*) utiliza toda esta rica nomenclatura em sua decisão do Censo de 1983.

Se a dogmática alemã é profícua neste sentido, já a situação brasileira é preocupante. A legislação existente quanto ao (adequado) tratamento de dados pessoais em matéria jurídico-penal é gravemente deficiente. Gleizer, Montenegro e Viana (2021,

p. 74) são contundentes ao abordar tal situação, no caso, especificamente quanto ao processo penal:

> O processo penal brasileiro é deficiente em normas que autorizem e regulem intervenções no âmbito protegido dos dados pessoais. Embora haja, por exemplo, (insatisfatória) regulação em lei para interceptações telefônicas (LIT) ou infiltrações de agentes (arts. 10 ss. Lei 12.850/13), medidas como infiltrações *online* [grifo do autor] ou observações prolongadas, dentre outras, não estão autorizadas/reguladas. (...) há grave ausência de regulação legal para as demais formas de tratamento: arquivamento, alteração, utilização e, em especial, o compartilhamento".

De fato, em razão de ausência legislativa sobre o tema, a infiltração *online* de agentes (ou infiltração encoberta) chegou a ser objeto de uma arguição de descumprimento de preceito fundamental (ADPF 1143) proposta pela Procuradoria-Geral da República, que aponta a ausência de atuação normativa do Congresso Nacional "na regulação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal", a fim de dar efetividade aos mandamentos constitucionais de proteção estatal da intimidade e da vida privada, e de inviolabilidade do sigilo das comunicações pessoais e de dados, estatuídos no art. 5º, X e XII, da Constituição Federal (de acordo com a manifestação na petição inicial)[149].

Esta separação conceitual de atividades de tratamento é inteiramente pertinente às intervenções jurídico-penais. Por exemplo, uma lei que autorize a intervenção no direito fundamental de sigilo das comunicações por meio de escuta telefônica deve especificar com a máxima precisão possível as atividades autorizadas. Neste caso, o levantamento de dados pessoais seria autorizado para a finalidade específica, entretanto, não seria autorizado o seu compartilhamento com os demais órgãos da administração pública ou mesmo seu armazenamento por prazo indefinido.

Portanto, a separação informacional conjugada com a separação funcional das atividades e o detalhamento das condições aplicadas às atividades especificadamente são medidas garantidoras dos demais princípios constitucionais penais e dos próprios

[149] Supremo Tribunal Federal. **ADPF 1143**. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=6900814. Acesso em: 05 ago. 2024.

direitos fundamentais afetados pelas intervenções a serem regulamentadas por meio de lei com reserva e parlamentar.

4.3 Princípio da proporcionalidade em sentido estrito

O princípio da proporcionalidade é de especial importância para nosso trabalho. Sua importância é tão notável que Gleizer, Montenegro e Viana (2021, p. 88) afirmam que "todos os princípios de tratamento de dados estão vinculados à ideia de proporcionalidade, ou são por ela pressupostos, ou são dela derivados", sendo o principal critério para justificar intervenções na zona externa ao conteúdo essencial (*Wesensgehalt*) e/ou de dignidade, de acordo com Greco (*in* Wolter, 2019, p. 48), o princípio da proporcionalidade.

Importante mencionar que a dogmática constitucional subdivide o princípio da proporcionalidade em três subprincípios: princípio da adequação (ou idoneidade), princípio da necessidade e princípio da proporcionalidade em sentido estrito. Portanto, quando aprofundamos a análise deste tópico, abordamos proporcionalidade como proporcionalidade em sentido estrito.

Podemos encontrar uma das primeiras manifestações da exigência de proporcionalidade das penas em Beccaria, cujos preciosos ensinamentos foram reconhecidos pela Declaração Francesa dos Direitos do Homem e do Cidadão de 1789[150] que determinou, em seu art. 8, que "a lei apenas deve estabelecer penas estrita e evidentemente necessárias (...)[151]". Entretanto, ao longo do séc. XIX que "este princípio começou a ser aplicado nas mais variadas áreas do Direito administrativo alemão"[152] (Bernal Pulido, 2014).

O Tribunal Constitucional Alemão (*Bundesverfassungsgericht*) estabelece o princípio da proporcionalidade como uma de suas bases na decisão do Censo de 1983 (BVerfGE 65, 173), informando que "sob o princípio da proporcionalidade, uma medida

[150] Elysée. **La Déclaration des Droits de l´Homme et du Citoyen**. Disponível em: https://www.elysee.fr/la-presidence/la-declaration-des-droits-de-l-homme-et-du-citoyen. Acesso em: 03 ago. 2024.
[151] Tradução livre: La loi ne doit établir que des peines strictement et évidemment nécessaires (…)
[152] Tradução livre: (…) este principio comenzó a aplicar-se em las más variadas áreas del Derecho administrativo alemán.

deve ser adequada e necessária para a finalidade pretendida; a intensidade da intervenção que lhe está associada não deve ser desproporcional à importância da questão e aos prejuízos impostos ao indivíduo”[153].

Este princípio opera, portanto, como um “critério metodológico, mediante o qual se pretende estabelecer que deveres jurídicos impõem ao Legislador as disposições dos direitos fundamentais tipificadas na Constituição”[154], continua o autor, “há de ser definido como um limite dos limites aos direitos fundamentais”[155] (Bernal Pulido, 2014).

Robert Alexy (1986, p. 267), assinala que a restrição e a possibilidade de restrições dos direitos fundamentais têm limites:

> Uma restrição dos direitos fundamentais só é permitida se, em um caso específico, os princípios contrários tiverem mais peso do que o princípio dos direitos fundamentais. Portanto, pode-se dizer que os direitos fundamentais em si são restrições à sua limitação e possibilidade de restrição. Uma barreira adicional à restrição e restringibilidade parece estar padronizada no Artigo 19, parágrafo 2, da Lei Fundamental, que proíbe qualquer invasão da essência dos direitos fundamentais[156].

Gleizer, Montenegro e Viana (2021, p.43) também abordam o tema, mas sob um sinônimo de limites a limites: “Na direção do poder legislativo, são erigidas outras barreiras. Assim, tampouco o legislador tem total liberdade para impor restrições ao exercício de direitos fundamentais. Essa ideia é conhecida como *restrições a restrições* [grifo do autor]”.

Luiz Regis Prado (2019, p. 80) ensina que “o conteúdo essencial desses direitos fundamentais – *limite dos limites* [grifo do autor] – ‘assinala uma fronteira que o legislador não pode ultrapassar, delimita um terreno que a lei limitadora não pode invadir sem incorrer em inconstitucionalidade’”. Entretanto, tal previsão não se encontra

---

[153] Tradução livre: Danach muß eine Maßnahme zur Erreichung des angestrebten Zweckes geeignet und erforderlich sein; der mit ihr verbundene Eingriff darf seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache und den vom Bürger hinzunehmenden Einbußen stehen.

[154] Tradução livre: este principio opera como un criterio metodológico, mediante el cual se pretende establecer qué deberes jurídicos imponen al Legislador las disposiciones de los derechos fundamentales tipificadas en la Constitución.

[155] Tradução livre: este ha de ser definido como um limite de los limites a los derechos fundamentales.

[156] Tradução livre: Eine Einschränkung der Grundrechte ist nur dann zulässig, wenn gegenläufigen Prinzipien im konkreten Fall gegenüber dem grundrechtlichen Prinzip ein höheres Gewicht zukommt. Man kann deshalb sagen, daß dic Grundrechte als solche Beschränkungen ihrer Einschränkung und Einschränkbarkeit sind. Eine zusätzliche Schranke der-Einschränkung und Einschränkbarkeit scheint Art. 19 Abs. 2 GG zu normieren, der die Antastung der Grundrechte in ihrem Wesensgehalt verbietet.

expressamente na Constituição brasileira, conforme consta na Lei Fundamental alemã de 1949 (art. 19, II), em Portugal (art. 18, III) e na Espanha (art. 53, I) (Gleizer; Montenegro; Viana, 2021, p. 43) mas, ainda assim, “que doutrina e jurisprudência reconhecem-no”. Dimitri e Martins (2020, p. 209), confirmando, afirmam que a teoria do conteúdo essencial do direito fundamental foi recepcionada pelo ordenamento jurídico brasileiro sob o nome de “núcleo essencial” do direito.

De fato, na ADC nº 29/DF[157], o voto do Ministro Gilmar Mendes aborda, dentre outros tópicos, o princípio da proporcionalidade:

> O princípio da proporcionalidade constitui um critério de aferição da constitucionalidade das restrições a direitos fundamentais. Trata-se de um parâmetro de identificação dos denominados *limites dos limites* (*Schranken-Schranken*) aos direitos fundamentais; um postulado de proteção de um *núcleo essencial* do direito, cujo conteúdo o legislador não pode atingir. Assegura-se uma *margem de ação* [grifos do autor] ao legislador, cujos limites, porém, não podem ser ultrapassados. O princípio da proporcionalidade permite aferir se tais limites foram transgredidos pelo legislador.

Mendes e Branco (2015, p. 211) exploram o assunto em mais detalhes em sua obra, afirmando que “da análise dos direitos fundamentais pode-se extrair a conclusão direta de que direitos, liberdades, poderes e garantias são passíveis de limitação ou restrição. É preciso não perder de vista, porém, que tais restrições são limitadas”. Trata-se precisamente dos chamados “limites dos limites (*Schranken-Schranken*)”.

Dimitri e Martins (2020, p. 208) advertem que a teoria dos limites dos limites (*Schranken-Schranken*) elaborada pela dogmática constitucional alemã apresenta uma difícil questão: determinar, precisamente, “o que seria esse conteúdo essencial de direito fundamental e as medidas estatais capazes de atingi-lo”. Ainda, segundo os autores, foram elaboradas duas teses para enfrentar o problema: “uma tese de que tal conteúdo essencial seria relativo, devendo ser fixado em cada caso específico, e a teoria de ser caráter absoluto”.

Tal problema se refletiria no cenário dogmático brasileiro que, ainda que tenha recepcionado o conceito de conteúdo essencial de um direito fundamental sob o nome de núcleo essencial, em razão de “ausência de disposição expressa, assim como a

[157] Consultor Jurídico. **ADC 29**. Disponível em: https://www.conjur.com.br/wp-content/uploads/2023/09/adc-29-30-lei-ficha-limpa.pdf. Acesso em: 16 ago. 2024.

particular dificuldade em se estabelecer o conteúdo nuclear de um direito fundamental, leva à conclusão de que *inexiste* [grifo dos autores] tal requisito limitador das intervenções legislativa".

Apesar disso, existiriam ainda diversas outras limitações ao poder do legislador de limitá-los (os direitos fundamentais), como a reserva de lei qualificada, mas, segundo Dimitri e Martins (2020, p. 209), "a isso não deve ser acrescentado um dever autônomo de preservar um suposto núcleo que aumentaria o risco de avaliações subjetivas da constitucionalidade de leis regulamentadoras".

Um pertinente esquema foi proposto por Bernal Pulido (2014) para o sistema de relações que são estabelecidos entre o sistema político e o sistema de controles jurídico-constitucionais "quando se introduzem restrições legislativas a tais direitos":

1. Objeto do limite: os direitos fundamentais.
2. Limite: a intervenção legislativa.
3. Limite do limite: o princípio da proporcionalidade (exclusivamente ou junto com outros, segundo o prescreva o ordenamento jurídico de que se trate).

Uma importante observação é trazida por Mariano da Silva (2005, p. 52) ao alertar que:

> A proporcionalidade não deve ser vista apenas sob o prisma da proibição do excesso (...). Desponta, igualmente, como corolário do princípio da proporcionalidade, a proibição da proteção deficiente, que determina ao legislador o dever de propiciar adequada e suficiente proteção aos bens jurídicos de especial importância para a sociedade.

Portanto, especialmente quanto à matéria de intervenções em direitos fundamentais a serem realizadas pelos órgãos da administração pública, faz-se necessário estabelecer o limite da intervenção, uma vez que tais intervenções, segundo a dogmática constitucional penal, devem ser realizadas por meio de reserva de lei e parlamentar, observando o princípio da proporcionalidade. Otto Lagodny (*in* Hefendehl *et al*, 2016, p. 123) assinala que "há de se determinar a legitimação jurídico-constitucional. A lei ou a norma legal há de perseguir uma finalidade legítima, ser idônea, necessária e

proporcional em sentido estrito ou adequada para a consecução de tal finalidade"[158]. Estas intervenções não podem acessar, agredir o conteúdo essencial (*Wesensgehalt*) do direito que se quer limitar, representando uma autêntica limitação aos limites a serem impostos com o legítimo objetivo de proteção dos próprios bens jurídicos tutelados pelo Direito.

4.4 Princípio da adequação ou idoneidade

O princípio da idoneidade também é conhecido como princípio da adequação Bernal Pulido, 2014). Isso é perceptível no ordenamento jurídico brasileiro, já que está disposto como princípio da necessidade no art. 6º, II, da LGPD, sendo informado como "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento".

Entretanto, de acordo com Bernal Pulido (2014), este princípio é, na verdade, o primeiro de três subprincípios do princípio da proporcionalidade. Gleizer, Montenegro e Viana (2014, p. 50) expandem ainda mais o significado do princípio da proporcionalidade ao afirmar que "todos os princípios de proteção de dados estão vinculados à ideia de proporcionalidade, ou são por ela pressupostos ou são por ela derivados".

Ainda, segundo Bernal Pulido (2014), de acordo com este "subprincípio" (da adequação ou idoneidade), "toda intervenção nos direitos fundamentais deve ser adequada para contribuir à obtenção de um fim constitucionalmente legítimo"[159]. É importante observar que demandar um "fim constitucionalmente legítimo" significa observar toda a dogmática constitucional-penal que temos colacionado ao longo deste trabalho, como a preservação do conteúdo essencial do direito fundamental ao elaborar medida interventiva que o afete.

---

[158] Tradução livre: (…) hay que determinar la legitimación jurídico-constitucional. La ley o la norma legal ha de perseguir una finalidad legítima, ser idónea, necesaria y proporcional en sentido estricto o adecuada para la consecución de tal finalidad.

[159] Tradução livre: De acuerdo con este subprincipio, toda intervención en los derechos fundamentales debe ser adecuada para contribuir a la obtención de un fin constitucionalmente legítimo.

4.5 Princípio da necessidade

De forma semelhante ao princípio da adequação (ou idoneidade), o princípio da necessidade é visto por parte dos autores como integrante do princípio da proporcionalidade, sendo deste um subprincípio.

Este princípio está disposto no art. 6º, III, da LGPD sob a forma de "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".

Adicionalmente, o princípio da necessidade tem estreito vínculo com outro princípio bastante caro ao direito penal, o princípio da intervenção mínima. Isso porque a análise do princípio da necessidade no caso concreto passa obrigatoriamente por avaliar se há outra medida menos gravosa, menos invasiva, menos prejudicial ao indivíduo e ao bem jurídico que se deseja intervir (no caso, nada menos que um direito fundamental), sempre respeitando seu conteúdo essencial. Significa analisar se a medida (ou atividade de tratamento, *Datenverarbeitung*) é realmente adequada à finalidade à qual se propõe.

Luiz Luisi (2003, p. 39), ao abordar o princípio da intervenção mínima, relembra que na Alemanha "é viva e difusa a delimitação da área de interferência penal (...)". Luisi afirma que, entretanto, "nas legislações constitucionais e penais contemporâneas o princípio em causa, em geral, não se encontra explicitado".

Um interessante caso da jurisprudência alemã que aborda o princípio da proporcionalidade, da adequação e da necessidade consta na decisão do Tribunal Constitucional Federal alemão (*Bundesverfassungsgerich*) BvR 264/95 de setembro de 1999[160]. Reclamações constitucionais foram dirigidas diretamente contra o Artigo 30, Parágrafo 1, da Lei de Estrutura da Saúde de 1992, que previa uma redução de preços e uma moratória de preços para certos medicamentos para os anos de 1993 e 1994.

O Tribunal considerou que "os regulamentos impugnados violaram o princípio da proporcionalidade. Embora fossem adequados e necessários (1), resultaram numa

[160] BVerfG, decisão da 2ª Câmara do Primeiro Senado de 1º de setembro de 1999 - 1 BvR 264/95 -, Rn 1-18. Disponível em: https://www.bverfg.de/e/rk19990901_1bvr026495.html. Acesso em: 05 ago. 2024.

interferência desproporcionada nos direitos fundamentais (2)"[161]. Apesar de existir motivação para adoção de uma medida de intervenção no direito fundamental de liberdade no exercício profissional, segundo o Tribunal alemão, quanto ao legislador, "se não tiver à sua disposição um meio proporcional para atingir os seus objetivos, deve abster-se da intervenção correspondente"[162]. Tal decisão está em perfeita consonância com a decisão do Censo alemão de 1983 realizada pelo Tribunal Constitucional Federal daquele país, quando menciona, dentre outras importantes menções sobre o tema, que "sob o princípio da proporcionalidade, uma medida deve ser adequada e necessária para a finalidade pretendida; a intensidade da intervenção que lhe está associada não deve ser desproporcional à importância da questão e aos prejuízos impostos ao indivíduo"[163].

4.6 Princípio da segurança

O princípio da segurança se encontra disposto no art. 6º, VII, da LGPD, e consiste em "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".

Se no Marco Civil da Internet, Lei 12.964/2014, a segurança foi mencionada como fundamento para o funcionamento da "rede" (internet), na LGPD encontra-se a primeira vez que segurança da informação é alçada a um princípio jurídico.

Um princípio, de acordo com (p.115) é, por definição, "mandamento nuclear de um sistema, verdadeiro alicerce dele; disposição fundamental que se irradia sobre diferentes normas, compondo-lhes o espírito e servindo de critério para sua exata compreensão e inteligência (...)". A segurança, a partir da publicação da LGPD, não pode ser considerada mais mero benefício ou expectativa, mas constitui um "alicerce" de um sistema de proteção de dados pessoais destinado a proteção de um direito fundamental.

---

[161] Tradução livre: Die angegriffenen Regelungen verletzten allerdings das Gebot der Verhältnismäßigkeit. Sie waren zwar geeignet und erforderlich (1), bewirkten jedoch einen unverhältnismäßigen grundrechtlichen Eingriff (2).

[162] Tradução livre: Steht ihm aber ein verhältnismäßiges Mittel zur Erreichung seiner Ziele nicht zur Verfügung, so muß er von dem entsprechenden Eingriff Abstand nehmen.

[163] Tradução livre: Danach muß eine Maßnahme zur Erreichung des angestrebten Zweckes geeignet und erforderlich sein; der mit ihr verbundene Eingriff darf seiner Intensität nach nicht außer Verhältnis zur Bedeutung der Sache und den vom Bürger hinzunehmenden Einbußen stehen.

Humberto Ávila (2021, p. 157), esclarece que:

> Os princípios são, portanto, normas que atribuem fundamento a outras normas, por indicarem fins a serem promovidos, sem, no entanto, preverem o meio para sua realização. Eles apresentam, em razão disso, alto grau de indeterminação, não no sentido de mera vagueza, presente em qualquer norma, mas no sentido específico de não enumerar exaustivamente os fatos em presença dos quais produzem a consequência jurídica ou de demandarem a concretização por outra norma, de modos diversos e alternativos.

Apesar dos destinatários da norma ou os titulares do direito por vezes demandarem que a lei seja – bem – mais específica que é, detalhando quais medidas técnicas, administrativas ou procedimentais seriam consideradas “adequadas” para demonstração do cumprimento legal, é precisamente por essa razão colacionada por Ávila que o princípio da segurança contido na LGPD não possui essa “enumeração exaustiva”, propositalmente sendo sua regulamentação propositalmente confiada às instituições competentes, seja o parlamento na forma de lei, seja a Autoridade Nacional de Proteção de Dados na forma de regulamentos, guias e orientações. Ocorre que, conforme já abordado ao longo deste trabalho, especialmente em matéria jurídico-penal, tais medidas não são suscetíveis de regulamentação por meio de outra forma que não seja por meio de reserva de lei e parlamentar.

Conforme já mencionado em nosso trabalho, há diversos tipos de tratamento de dados a serem adequadamente regulamentados, diferentemente de uma abordagem generalista em “atividades de tratamento” (*Datenverarbeitung*) e bem além do tradicional foco na coleta de dados, cuja terminologia mais adequada consideramos levantamento de dados (*Datenerhebung*). Tão importantes quanto o levantamento de dados, também são a modificação de dados (*Datenveränderung*), o armazenamento de dados, (*Datenspeicherung*), o compartilhamento dos dados (*Datenübermittlung*), a transmissão de dados (*Weitergabe*) e o uso dos dados (*Datennutzung*). Em observância do princípio da segurança, constatamos que além da regulamentação das atividades de tratamento de modo específico, também devem ser regulamentadas suas respectivas medidas de segurança para cada situação interventiva.

Tomemos como primeiro exemplo a interceptação telefônica, (precariamente) regulamentada pela Lei 9.296/1996. Apesar de ter sido modificada pelo chamado pacote

anticrime (Lei 13.964/2019), a Lei 9.296 data do ano de 1996 e a primordial preocupação do legislador (e talvez única à época da edição da lei) era regulamentar as condições sob as quais as comunicações telefônicas poderiam ser interceptadas. Não há qualquer menção sobre medidas de segurança a serem adotadas por ocasião do armazenamento das informações levantadas (que constituem dados pessoais, propriamente ditos), compartilhamento ou comunicação dos dados com outros órgãos da administração pública (poder judiciário, peritos etc.) e, como se sabe, não havia (e ainda não há) regulamentação alguma sequer quanto às diversas formas de tratamento dos dados pessoais levantados em matéria jurídico-penal.

Medidas que seriam cabíveis e adequadas para as formas de tratamento específicas de dados pessoais seriam, por exemplo, a adoção de padrões criptográficos de elevada resistência às técnicas de força bruta para armazenamento e compartilhamento destes dados e, também, para assinaturas digitais dos agentes desses órgãos para as diversas movimentações dos dados ao longo de etapas do procedimento (por exemplo, atividades realizadas ao longo da cadeia de custódia dos elementos de prova, movimentação das diversas etapas ao longo do procedimento jurídico-penal etc.).

Para que se tenha uma ideia da relevância atribuída pelos Estados Unidos ao assunto, note-se que o NIST (*National Institute of Standards and Technology*, ou Instituto Nacional de Padrões e Tecnologia, em tradução livre) tem investido desde 2016 no desenvolvimento de ferramentas criptográficas que sejam concebidas para resistir ao futuro computador quântico, que potencialmente poderia superar a segurança usada para proteger a privacidade nos sistemas digitais atuais[164]. O resultado desta "competição" em pesquisa foi publicado[165] em 2022, ao anunciar seus "primeiros quatro algoritmos criptográficos resistentes ao quantum"[166].

---

[164] Tradução livre: (…) encryption tools that are designed to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on every day.

[165] NIST. **NIST Announces First Four Quantum-Resistant Cryptographic Algorithms**. Disponível em: https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms. Acesso em: 08 ago. 2024.

[166] Tradução livre: First Four Quantum-Resistant Cryptographic Algorithms.

Em agosto de 2024, o NIST publicou seus primeiros 3 padrões post-quantum[167], celebrando um marco histórico no tema e encorajando todos os administradores de sistemas a iniciarem a transição para os novos padrões assim que possível pois a "corrida" que os pesquisadores no mundo inteiro travam na construção de "computadores quânticos que operam de maneira radicalmente diferentes dos computadores padrão e podem quebrar a criptografia atual que fornece segurança e privacidade para praticamente tudo que fazemos online"[168]. Essa iniciativa tem a finalidade de proteger a privacidade dos dados atuais (e, também, a confidencialidade dos dados e informações em geral) de uma técnica de violação de segurança[169] chamada de "colete agora, descriptografe depois"[170], técnica a qual pode acarretar sérios problemas de diversas naturezas jurídicas, uma vez que há obrigações legais de manutenção de dados e sua confidencialidade por prazos bastante extensos. O Decreto nº 7.724/2012, que regulamenta a Lei de Acesso à Informação (Lei 12.527/2011), em seu artigo 55, I, determina, por exemplo, a imposição de sigilo de até cem anos a contar da data de sua produção quanto "as informações pessoais relativas à intimidade, vida privada, honra e imagem detidas pelos órgãos e entidades". Além disso, a Lei de Acesso à Informação prevê acesso restrito também pelo prazo de cem anos em seu art. 31, §1º, I:

> Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
> § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem.

---

[167] NIST. **NIST Releases First 3 Finalized Post-Quantum Encryption Standards**. Disponível em: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards. Acesso em: 13 ago. 2024.
[168] Tradução livre: (…) quantum computers that would operate in radically different ways from ordinary computers and could break the current encryption that provides security and privacy for just about everything we do online.
[169] GovCio Media & Research. **NIST Releases First Post-Quantum Cryptography Standards.** Disponível em: https://govciomedia.com/nist-releases-first-post-quantum-cryptography-standards. Acesso em: 08 ago. 2024.
[170] Tradução livre: Harvest now, decrypt later.

Os atuais padrões criptográficos (tipicamente RSA e ECC – *Elliptic Curve Cryptography*, ou Criptografia de Curva Elíptica, em tradução livre) utilizam, de modo geral, comprimentos que variam de 1024 a 2048-bit. Entretanto, enquanto os atuais padrões podem ser considerados seguros quanto aos ataques de força bruta realizados por computadores disponíveis atualmente, provavelmente tais padrões não serão suficientes para proteção de segurança contra ataques realizados utilizando computadores quânticos, que estima-se que possa violar uma chave criptográfica RSA de 2048-bit dentro de meras oito horas, de acordo com pesquisa publicada por Gidney e Ekerå (2021, p. 1). Já há algum tempo, o NIST explicitamente recomenda a adoção de chaves de 3072-bit como parte de seus guias publicados com orientações sobre criptografia quântica. Nitidamente, o Brasil necessita de uma política mais robusta de investimentos em ciência e tecnologia para se tornar um protagonista em novos campos de pesquisa que moldarão o mundo em breve, ao invés de se tornar mero consumidor dessas tecnologias (fragilizando sua própria segurança e soberania). EUA e China lideram atualmente os investimentos no tema, somando US$ 42 bilhões já investidos, enquanto o Brasil possui investimentos na ordem de 60 milhões de Reais[171], algo em torno de 0,001% do montante investido por estes dois países.

O princípio da segurança tem conexão com outro direito fundamental reconhecido na Alemanha, mas que não temos seu correspondente no ordenamento jurídico brasileiro. Trata-se do direito fundamental à proteção da confidencialidade e integridade dos sistemas de tecnologia da informação (*Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*).

O direito fundamental à proteção da confidencialidade e integridade dos sistemas de tecnologia da informação é destinado a limitar o poder do Estado quanto à sua atividade de monitoramento, acesso, extração e análise de dados, especialmente nas operações de infiltração encobertas por parte de agentes estatais. Esse “novo” direito

[171] Ministério da Ciência, Tecnologia e Inovação. **Cientistas apresentam possibilidades para desenvolver a computação e internet quântica no Brasil.** Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/08/cientistas-apresentam-possibilidades-para-desenvolver-a-computacao-e-internet-quantica-no-brasil. Acesso em 08 ago. 2024.

fundamental (a decisão BVerfGE 120, 274[172] é de fevereiro de 2008) reconhecido pelo *Bundesverfassungsgericht* tem suas razões explicadas pelo próprio Tribunal.

A decisão do Tribunal Constitucional Federal alemão passa por analisar que a proteção jurídica aos direitos de personalidade deve considerar que a utilização da tecnologia da informação adquiriu "significado imprevisível para a personalidade e o desenvolvimento do indivíduo"[173]. Enquanto a moderna tecnologia da informação "abre novas oportunidades para indivíduos, também cria novas ameaças à sua personalidade"[174].

Assim, reconhece o Tribunal, o desenvolvimento recente da tecnologia da informação conduziu a uma situação em que os sistemas de tecnologia da informação se tornaram "onipresentes" e "seu uso, central para as vidas de muitas pessoas"[175]. Essa pertinente e adequada percepção do Tribunal sobre a tomada da sociedade contemporânea pela tecnologia foi essencial para que se reconhecesse a necessidade de um direito fundamental à proteção da confidencialidade e integridade dos sistemas de tecnologia da informação, dada a onipresença e centralidade destes dispositivos na vida dos indivíduos na sociedade da informação[176].

O desenvolvimento tecnológico, a acessibilidade à tecnologia e essa centralidade na vida dos indivíduos conduziu às práticas de armazenamento e comunicação de grandes volumes de dados por meio destes dispositivos. Como consequência, explica a decisão do Tribunal, a análise de tamanha quantidade de dados permite desvendar, obter extensas conclusões sobre a personalidade destes indivíduos que foram destinatários da

---

[172] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 -, Rn 1-333. Disponível em: https://www.bverfg.de/e/rs20080227_1bvr037007.html. Acesso em 08 ago. 2024.
[173] Tradução livre: Die Nutzung der Informationstechnik hat für die Persönlichkeit und die Entfaltung des Einzelnen eine früher nicht absehbare Bedeutung erlangt.
[174] Tradução livre: Die moderne Informationstechnik eröffnet dem Einzelnen neue Möglichkeiten, begründet aber auch neuartige Gefährdungen der Persönlichkeit.
[175] Tradução livre: Die jüngere Entwicklung der Informationstechnik hat dazu geführt, dass informationstechnische Systeme allgegenwärtig sind und ihre Nutzung für die Lebensführung vieler Bürger von zentraler Bedeutung ist.
[176] O termo sociedade da informação foi cunhado na virada do século para descrever uma sociedade na qual tecnologias de informação e comunicação (TICs) se tornaram uma parte integral da vida diária. Tradução livre de: The term 'information society' was coined at the turn of the century to describe a society in which information and communication technologies (ICTs) have become an integral part of daily life. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000133021. Acesso em: 18 ago. 2024.

investigação, ainda que tais conclusões não tenham relação alguma com a suspeita que motivou a autorização da infiltração.

Essas violações atingem outro direito fundamental de central importância na sociedade da informação, o direito à autodeterminação informacional (*Informationelle Selbstbestimmung*). De acordo com Luís Greco (*in* Wolter, 2018, p. 44), a autodeterminação informacional "é o direito da pessoa de se autoapresentar em sociedade, de se desvincular dos estereótipos construídos por terceiros, isto é, de forma heterônoma". E este direito fundamental é protegido "não apenas pela reserva de lei (qualificada, pelos princípios da vinculação a fim e seus correlatos), como também por uma série de *garantias processuais ou procedimentais* [grifo do autor]" (*in* Wolter, 2018, p. 44).

O método de infiltração encoberta tende a ter sua utilização cada vez maior pelos agentes estatais. Isso porque, apesar da infiltração ser associada a dificuldades consideráveis quando o alvo da medida de intervenção tiver tomado as devidas precauções técnicas (como instalar software de proteção, utilização de VPN – *Virtual Private Network*, dentre outras medidas) e mantido atualizado seu sistema operacional atualizado[177], caso o agente realmente obtenha o acesso ao dispositivo informático do titular por meio da infiltração, ele terá importantes vantagens com relação aos métodos convencionais de investigação.

De modo bastante instrutivo para uma decisão judicial, o Tribunal Constitucional Federal alemão explica um aspecto técnico fundamental para a justificativa da infiltração encoberta: o indivíduo pode (dentro de sua faculdade de autoproteção) somente armazenar os dados de forma criptografada e ao se infiltrar no dispositivo informático, o agente estatal pode acessar os dados no mesmo formato legível que o usuário do sistema (o indivíduo titular dos dados) os utiliza no momento em questão[178]. Essa vantagem obtida também é uma maneira de "contornar" a comunicação criptografada durante as

[177] Tradução livre: Der heimliche Zugriff auf ein informationstechnisches System kann mit erheblichen Schwierigkeiten verbunden sein. Dies ist insbesondere der Fall, wenn der Nutzer des Zielsystems technische Sicherheitsvorkehrungen getroffen hat und sein Betriebssystem regelmäßig aktualisiert.
[178] Tradução livre: Soweit der Nutzer eines Rechners Daten nur in verschlüsselter Form ablegt, können solche Daten im Rahmen einer „Online-Durchsuchung" gegebenenfalls in unverschlüsselter Form erhoben werden. Denn durch die Infiltration des Rechners kann die Behörde in der Weise auf die Daten zugreifen wie der Nutzer sie im fraglichen Zeitpunkt verwendet.

comunicações pela internet (que frequentemente é o caso), em que essa comunicação só pode ser monitorada de maneira eficaz acessando o dispositivo.

A decisão do Tribunal ainda menciona o princípio da proporcionalidade, que "estabelece limites a uma regulamentação legal que autorize o acesso encoberto aos sistemas de tecnologia da informação, na medida em que existam requisitos especiais para o motivo da intervenção"[179]. A infiltração encoberta, enquanto medida de intervenção em direitos fundamentais, só pode ser considerada enquanto fundamental para tratar de um perigo concreto para um bem jurídico extremamente importante, como a vida, integridade física e a liberdade. Bens jurídicos de interesse público considerados de tal importância são aqueles "cuja ameaça afete os fundamentos ou a existência do Estado, ou das pessoas".

Portanto, de acordo com a decisão, para proteger bens jurídicos que não representem tal ameaça existencial, "o Estado deve limitar-se a outros poderes de investigação que lhe sejam conferidos pela lei especializada aplicável na área preventiva"[180]. Adicionalmente, também é necessário que estes perigos concretos estejam baseados em elementos fáticos, com probabilidade suficiente de realização, e tal medida deve ser autorizada judicialmente. E, por fim, e aqui o aspecto de mais difícil execução, a medida de intervenção deve preservar o núcleo de esfera privada (*Kernbereich privater Lebensgestaltung*) com precauções legais minimamente suficientes.

De acordo com o *Bundesverfassungsgericht*, "as medidas encobertas de monitoramento por parte das autoridades estatais devem proteger um núcleo central intocável da esfera privada, cuja proteção resulta do artigo 1.º, n.º 1 GG"[181]. Isso porque o Tribunal reconhece que o desenvolvimento da personalidade neste núcleo da esfera privada de um indivíduo incluir exprimir sua interioridade, seus sentimentos, pensamentos, opiniões, e "experiências de natureza altamente pessoal, sem o receio de

---

[179] Tradução livre: Der Verhältnismäßigkeitsgrundsatz setzt einer gesetzlichen Regelung, die zum heimlichen Zugriff auf informationstechnische Systeme ermächtigt, zunächst insoweit Grenzen, als besondere Anforderungen an den Eingriffsanlass bestehen.
[180] Tradução livre: Zum Schutz solcher Rechtsgüter hat sich der Staat auf andere Ermittlungsbefugnisse zu beschränken, die ihm das jeweils anwendbare Fachrecht im präventiven Bereich einräumt.
[181] Tradução livre: Heimliche Überwachungsmaßnahmen staatlicher Stellen haben einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt.

que as autoridades estatais estejam o monitorando"[182]. E, em razão da execução da própria medida interventiva, "como parte do acesso encoberto a um sistema de tecnologia da informação, existe o risco de que a autoridade estatal que a execute levante dados pessoais que possam ser atribuídos à essa área nuclear"[183].

Aqui reside interessante situação que está bastante relacionada ao momento histórico de desenvolvimento tecnológico do mundo quando foi proferida tal decisão pelo Tribunal Constitucional Federal alemão. O Tribunal estabeleceu que os requisitos constitucionais para a organização específica da proteção das áreas nucleares da personalidade podem variar dependendo do tipo de levantamento de informações e das informações que ela abrange.

Assim, uma autorização legal para uma medida de busca que possa afetar a área central da vida privada deve garantir, na medida do possível, que os dados relativos ao núcleo da personalidade não sejam coletados. Portanto, os dados encontrados e coletados relativos às áreas nucleares devem ser eliminados imediatamente e a sua utilização excluída (conforme BVerfGE 109, 279 <318>; 113, 348 <391 f.>). Ocorre que o levantamento de dados em uma infiltração encoberta a um dispositivo ou sistema informático será predominantemente automatizado e, quando comparado com a investigação realizada por uma pessoa humana, essa automatização torna mais difícil distinguir os dados com e sem referência à área nuclear da personalidade.

Portanto, segundo o Tribunal, de acordo com a opinião unânime dos especialistas ouvidos pelo Senado, "os mecanismos técnicos de busca ou exclusão para determinar a relevância da área nuclear da personalidade quanto aos dados pessoais não funcionam de forma tão confiável que, com o seu auxílio, uma proteção eficaz da área nuclear possa ser alcançada"[184].

---

[182] Tradução livre: (...) Erlebnisse höchstpersönlicher Art ohne die Angst zum Ausdruck zu bringen, dass staatliche Stellen dies überwachen.

[183] Tradução livre: Im Rahmen eines heimlichen Zugriffs auf ein informationstechnisches System besteht die Gefahr, dass die handelnde staatliche Stelle persönliche Daten erhebt, die dem Kernbereich zuzuordnen sind.

[184] Tradução livre: Technische Such- oder Ausschlussmechanismen zur Bestimmung der Kernbereichsrelevanz persönlicher Daten arbeiten nach einhelliger Auffassung der vom Senat angehörten sachkundigen Auskunftspersonen nicht so zuverlässig, dass mit ihrer Hilfe ein wirkungsvoller Kernbereichsschutz erreicht werden könnte.

De fato, é perfeitamente crível que à época da decisão proferida (no ano de 2008), a tecnologia não estivesse suficientemente desenvolvida para promover a proteção do núcleo da personalidade ao longo da realização da medida de intervenção da infiltração encoberta e seu levantamento de dados. Entretanto, o nível atual de desenvolvimento de algoritmos e sistemas de inteligência artificial pode, de maneira surpreendentemente eficaz, realizar esse levantamento automatizado eliminando automaticamente, em poucos segundos após a coleta, dados pessoais que não sejam úteis ao objeto da infiltração encoberta iniciada mediante autorização judicial e devidamente regulamentada por meio de reserva legal e parlamentar, como tanto temos insistido ao longo desse trabalho.

Tal possibilidade se apresenta atualmente em razão de que os sistemas de inteligência artificial baseados em *machine learning* (aprendizado de máquina, em tradução livre) se baseiam em algoritmos exaustivamente treinados com dados similares aos que se encontrará em tais levantamentos. De acordo com Russel e Norvig (2020, p. 651), um conceito simplificado de *machine learning* é "um computador que observa alguns dados, constrói um modelo baseado nos dados, e usa o modelo tanto como uma hipótese sobre o mundo, quanto como um pedaço de software que pode resolver problemas"[185]. Oliveira e Figueiredo (2024, p. 14), por sua vez, explicam que:

> Em *machine learning*, o conjunto de exemplos utilizados para treinar um sistema é chamado conjunto de treinamento e o conjunto de exemplos posteriormente apresentados ao sistema para testar seu desempenho é chamado conjunto de testes. Uma vez treinado, o sistema pode ser usado muitas vezes para prever saídas a partir de novos valores de entrada, sem a necessidade de treinamento adicional[186].

O treinamento dos algoritmos de aprendizado de máquina e inteligência artificial pode ser realizado utilizando dados sintéticos como forma de preservar a privacidade dos

[185] Tradução livre: a computer observes some data, builds a model based on the data, and uses the model as both a hypothesis about the world and a piece of software that can solve problems.
[186] Tradução livre: In machine learning, the set of examples used to train the system is called the training set and the set of examples later presented to the system to test its performance is called the test set. Once trained, the system can be used many times to predict outputs from new input values, without the need for additional training.

indivíduos. Dados sintéticos[187] permitem gerar dados artificiais que imitam de perto dados do mundo real, enquanto preserva a privacidade[188]. Portanto, essa seria uma abordagem de utilização de tecnologia e metodologia como formas de aumentar, estender a privacidade e proteção de dados pessoais (também chamada de PET – *Privacy-Enhancing Tecnology*) em uma medida de intervenção jurídico-penal do Estado, nomeadamente a infiltração encoberta (ou infiltração *on-line*). O que é ainda mais interessante é que essa tecnologia baseada em *machine learning* e treinada a partir de conjuntos de dados sintéticos para a proteção da privacidade e de dados pessoais pode ser adotada em qualquer outro tipo de medida de intervenção baseada no levantamento encoberto (no Brasil utilizada a nomenclatura de infiltração), desde que respeitados os requisitos que temos abordado ao longo deste trabalho.

Este feixe de direitos fundamentais conectados à realidade do indivíduo, o direito fundamental à confidencialidade e integridade dos sistemas de tecnologia da informação (ou informáticos), o direito fundamental à autodeterminação informacional, o direito fundamental ao sigilo das telecomunicações, o direito fundamental do sigilo de correspondência, todos esses direitos integram o direito fundamental à proteção de dados pessoais e, de diversos modos, ao direito fundamental de proteção da intimidade e da vida privada.

Enfim, se faz necessário conectar o princípio da segurança a este feixe de direitos fundamentais que conformam o direito à proteção de dados. Este princípio possui natureza dúplice, espelhada: enquanto estabelece um dever para o agente de tratamento de dados pessoais (no nosso caso, o aparato jurídico-penal estatal), estabelece de maneira reflexiva um direito para o indivíduo titular dos dados. Tal direito, o direito à segurança em todo o ciclo de tratamento dos dados pessoais, tem estreita relação com estes direitos fundamentais abordados, uma vez que na eventualidade de o agente de tratamento jurídico-penal não fornecer as adequadas medidas de segurança para as diversas formas de tratamento (medidas intervencionais essas independentes e que necessitam de autorização específica para cada uma delas: armazenamento,

---

[187] Decentriq. **What are privacy-enhancing technologies (PETs)?**. Disponível em: https://www.decentriq.com/article/what-are-privacy-enhancing-technologies. Acesso em: 10 ago. 2024.
[188] Tradução livre: Synthetic data allows organizations to generate artificial data that closely mimics real-world data, while still preserving privacy.

compartilhamento, comunicação etc.), tais fragilidades poderão acarretar diversos incidentes como modificações e divulgações não autorizadas. A repercussão desses incidentes na vida social, familiar e profissional destes indivíduos afetados pode simplesmente ser de impossível reparação.

No Brasil, tal direito fundamental não é reconhecido e a medida de intervenção da infiltração encoberta ainda sequer encontra previsão legal, conforme já abordado neste trabalho, tendo sido objeto de uma arguição de descumprimento de preceito fundamental (ADPF 1143) proposta pela Procuradoria-Geral da República, que aponta a ausência de atuação normativa do Congresso Nacional "na regulação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal".

Uma audiência pública foi convocada no âmbito da ADPF 1143 pela Procuradoria-Geral da República (PGR), sendo que a subprocuradora-geral da República (Elizeta Ramos) mencionou que o "direito fundamental informático" vem sendo debatido no alto comissariado da Organização das Nações Unidas na defesa dos direitos humanos[189]. Tal direito fundamental informático é, precisamente, o direito fundamental de confidencialidade e integridade dos sistemas de tecnologia de informação abordado em nosso trabalho e, de fato, há menção a esses padrões (de confidencialidade e integridade de sistemas de TI) na Carta de Direitos Humanos e Princípios para a Internet do Alto Comissariado das Nações Unidas[190], onde há expressão manifesta de que "o direito à privacidade deve ser protegido por padrões de confidencialidade e integridade de sistemas de TI, fornecendo proteção contra acesso de terceiros sem o consentimento"[191].

O princípio da segurança associado com os próprios deveres de segurança a serem instituídos por meio de lei (uma vez que a Lei 13.709/2018, art. 4º, III, afasta a aplicabilidade da lei para tratamento de dados pessoais realizados para fins exclusivos

---

[189] Supremo Tribunal Federal. **STF abre audiência pública sobre uso de ferramentas de monitoramento secreto.** Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idconteudo=546437. Acesso em: 08 ago. 2024.

[190] United Nations Human Rights Office of the High Commissioner. **The Charter of Human Rights and Principles for the Internet**. Disponível em: https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf. Acesso em: 08 ago. 2024.

[191] Tradução livre: The right to privacy must be protected by standards of confidentiality and integrity of IT-Systems, providing protection against others accessing IT-Systems without consent.

de: a) segurança pública; b) defesa nacional; c) segurança do Estado; d) atividades de investigação e repressão de infrações penais) é de primordial importância para a regulamentação da atividade jurídico-penal do Estado.

Já há alguns anos existe uma intensa variação na disponibilidade de registros criminais para atividades não legais chamadas de *background checks* (verificação de antecedentes, em tradução livre). Segundo Sarah Lageson (2024), os Estados Unidos são "uma exceção notável ao permitirem um acesso quase ilimitado aos registos criminais, enquanto países na Europa restringem acesso público a condenações criminais e coloca alguns limites no uso de verificação de antecedentes criminais em configurações não legais"[192].

Enquanto isso, na Europa, há um crescimento significativo no uso de *background checks* criminais ao longo dos anos (Pijoan, 2014, p. 52). Somente nos Estados Unidos, há uma estimativa de que mais de 31 milhões de pessoas ao ano sejam questionadas sobre registros criminais em uma candidatura para vaga de emprego (Denver *et al*, 2018, p. 20). De modo geral, conforme Marti Rovira (2020, p. 1), recrutadores de emprego do mundo todo estão cada vez mais conduzindo *criminal background checks* (CBC), procurando coletar informações de condenações criminais prévias tidas por candidatos antes de decidir pela contratação[193].

Enquanto no passado a busca por registros de condenações criminais "demandaria horas de pesquisa por entre microfichas ou cópias de publicações amareladas armazenadas em um depósito de alguma biblioteca local"[194] (Maruna; Lageson, 2017, p. 114), atualmente essa busca está a alguns cliques a partir do advento e crescimento exponencial da internet e sua conectividade. De acordo com Sarah Lageson (2017, p. 114), como resultado, o potencial para negação de transgressões passadas era alto (por parte do indivíduo que cumpriu a pena) e, embora pudesse haver

[192] Tradução livre: The United States is a notable outlier in allowing nearly unfettered access to criminal records, while countries in Europe restrict public access to criminal convictions and put some limits on the use of criminal background checks in non-legal settings.
[193] Tradução livre: Worldwide, employment recruiters are increasingly conducting criminal background checks (CBCs), seeking to gather information on previous criminal convictions held by applicants prior to the hiring decision.
[194] Tradução livre: (…) would require hours of research trawling through microfiche or yellowed back-copies of newspaper warehoused at a local library.

“fofocas e rumores”, o indivíduo poderia “realizar um ‘novo começo’ se mudando de cidade ou mudando seu círculo social”[195].

O estigma na forma de uma pegada digital é indiscutivelmente mais difícil que nunca de escapar[196] (Maruna; Lageson, 2017, p. 113) e a digitalização dos dados das instituições (que antes eram armazenados em papel e gradualmente passam ao formato digital em uma velocidade impressionante) aumentam o risco de incidentes de segurança da informação envolvendo tais bases de dados. O encarceramento (como resultado de uma política de criminalização e punição) conduz a “um número de consequências por toda a vida, incluindo nas áreas de emprego, moradia, educação e vida familiar”[197] (Lageson, 2024) e “graduais evidências sugerem que o contato com o sistema criminal pode conduzir a uma redução substancial em oportunidades econômicas”[198] (Pager, 2003, p. 939).

Mesmo que a discussão criminológica sobre a estigmatização e *labeling* (etiquetamento, em tradução livre) não seja o objeto direto desse trabalho, se faz necessário compreender as gravíssimas consequências que seguiriam divulgações não autorizadas de tais informações e dados pessoais de indivíduos em razão de incidentes de segurança envolvendo os agentes jurídico-penais do Estado. O respeito ao princípio da segurança e o cumprimento de mandamentos legais que deverão constar em regulamentação própria são, conforme abordamos ao longo deste tópico, essenciais para minimizar riscos de incidentes e a consequente violação ao direito fundamental de proteção de dados pessoais em âmbito criminal (e demais direitos fundamentais conexos).

---

[195] Tradução livre: (…) make a “fresh start” by moving cities or changing social networks

[196] Tradução livre: (…) stigma in the form of a digital footprint is arguably more difficult than ever to escape.

[197] Tradução livre: (…) a criminal conviction can lead to a number of lifelong consequences, including in the arenas of employment, housing, education, and family life.

[198] Tradução livre: (…) growing body of evidence suggests that contact with the criminal justice system can lead to a substantial reduction in economic opportunities.

4.7 Princípio da responsabilização e prestação de contas

O princípio contido no art. 6º, X, refere-se à capacidade de “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”.

Ainda que a responsabilização dos agentes nos entes públicos em caso de descumprimento legal esteja principalmente vinculada à improbidade administrativa na qualidade de realização de ato ilegal ou contrário aos princípios básicos da Administração Pública, cometido por agente público, durante o exercício de função pública, conforme definido pela Lei 8.429/92, há condutas tipificadas no Código Penal brasileiro que poderiam configurar crime contra a inviolabilidade dos segredos.

O art. 153 do Código penal dispõe:

> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
> Pena - detenção, de um a seis meses, ou multa, de trezentos mil réis a dois contos de réis.
> §1º Somente se procede mediante representação.
> §1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:
> Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.
> § 2º Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.

Apesar da conduta típica descrita no caput do artigo não ter nenhuma qualificação específica do agente que realiza a conduta configurando um crime classificado como comum, tal conduta é passível de realização pelo agente público no exercício de suas funções, especialmente após a modificação introduzida pela Lei 9.983 de 2000 com a inserção do parágrafo 1º-A, onde há menção específica de “informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública”.

O art. 154 do Código Penal brasileiro dispõe:

> Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem:
> Pena - detenção, de três meses a um ano, ou multa de um conto a dez contos de réis.
> Parágrafo único - Somente se procede mediante representação.

Já o art. 325 do Código Penal brasileiro, que está localizado no capítulo que trata dos crimes praticados por funcionário público contra a administração em geral, dispõe:

> Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:
> Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.
> § 1º Nas mesmas penas deste artigo incorre quem:
> I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública;
> II – se utiliza, indevidamente, do acesso restrito.
> § 2º Se da ação ou omissão resulta dano à Administração Pública ou a outrem:
> Pena – reclusão, de 2 (dois) a 6 (seis) anos, e multa.

Estas condutas tipificadas possuem especial relevância no contexto das medidas de intervenção realizadas pelos agentes estatais nos direitos fundamentais de privacidade e proteção de dados pessoais. O artigo 154 tipifica a violação do segredo profissional, entretanto, o artigo 325 dispõe sobre revelação de “fato” de que tem ciência em razão do cargo e que deva permanecer em segredo. Ambos são inteiramente aplicáveis aos agentes estatais de diversos entes da administração pública, entretanto o artigo 154 tem em seu tipo penal a menção de dano que se possa produzir em outra pessoa decorrente da revelação, sem justa causa, de segredo que conheceu em razão do desempenho de sua função ou profissão. Já o tipo penal do artigo 325 se refere a “fato” que pode, ou não, se referir a uma pessoa. Não se referindo o fato a alguma pessoa, não há de se falar de violação à privacidade ou à proteção de dados pessoais, configurando violação de mero dever de sigilo geral decorrente do desempenho da função pública.

A título de exemplo de obtenção de segredo ou informação sigilosa sobre um indivíduo, as informações obtidas em razão de desempenho de atividade de infiltração encoberta (ou *online*), uma vez devidamente regulamentada no ordenamento jurídico brasileiro e mediante autorização judicial, contêm inúmeros segredos (plenamente

configurados como dados pessoais), conforme já reconhecido há anos pela experiência dogmática e jurisprudencial alemã (BVerfGE 120, 274[199]) ao fixar que “as medidas encobertas de monitoramento por parte das autoridades estatais devem proteger um núcleo central intocável da esfera privada, cuja proteção resulta do artigo 1.º, n.º 1 GG”[200].

Já um outro exemplo em que há meramente “fato” que se tenha ciência em razão do cargo e que deva permanecer em segredo, mencionemos o agente público que divulgue rotas de patrulhamento diárias da polícia militar de determinada cidade. Este fato, caso revelado a outros, representa potencial grave impacto na segurança pública, podendo acarretar a ocorrência de diversas tentativas de crimes contra o patrimônio que, em razão de conhecimento prévio do fato revelado, terá sua repressão prejudicada, já que não haverá patrulhamento disponível naquela localidade especialmente selecionada para a realização da conduta criminosa.

No artigo 153 há certa conexão com o disposto no art. 154, entretanto, dispensado o requisito que se tenha ciência em razão de função, ministério, ofício ou profissão (configurando o crime definido no art. 154 como crime próprio), tornando-o um crime cuja conduta é de incidência mais ampla (na condição de crime comum). Uma vez que haja divulgação, sem justa causa, de documento particular ou correspondência confidencial que seja detentor, haverá tipicidade. Aqui há a conexão com o art. 154 que, no fim das contas, apenas torna a pena base mais grave ao representar qualificadora em razão da violação do segredo profissional.

Ocorre que o art. 61, II, g, do Código Penal brasileiro estabelece que “são circunstâncias que sempre agravam a pena, quando não constituem ou qualificam o crime, ter o agente cometido o crime com abuso de poder **ou violação de dever inerente a cargo, ofício, ministério ou profissão** [grifo nosso]”. Por fim, tendo o agente realizado as condutas típicas dispostas nos arts. 153 e 154, entendemos que deverá ser considerado o princípio da consunção (*lex consumens derogat lex consumptae*), devendo

[199] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 -, Rn 1-333. Disponível em: https://www.bverfg.de/e/rs20080227_1bvr037007.html. Acesso em 12 ago. 2024.
[200] Tradução livre: Heimliche Überwachungsmaßnahmen staatlicher Stellen haben einen unantastbaren Kernbereich privater Lebensgestaltung zu wahren, dessen Schutz sich aus Art. 1 Abs. 1 GG ergibt.

o agente ser punido por apenas um crime, a não ser que a conduta típica realizada se amolde à descrição típica do §1º-A.

No parágrafo §1º-A do art. 153 reside questão essencial e diretamente conectada ao objeto deste trabalho, uma vez que o texto penal tipifica a "divulgação, sem justa causa, de informações sigilosas ou reservadas, **assim definidas em lei** [grifo nosso], contidas ou não nos sistemas de informações ou bancos de dados da Administração Pública".

Apesar do entendimento por parte da dogmática penal brasileira[201] de que a Lei de Acesso à Informação (Lei 12.527/2011) fornece regulamentação aproveitável à atividade jurídico-penal quanto às questões de sigilo e responsabilização, entendemos que referida lei tem como fundamento o direito administrativo e seu processo sancionador próprio, apresentando lacunas importantes quanto ao tema abordado neste trabalho.

Uma vez que a própria Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018), que se apresenta como o regulamento geral da matéria de proteção de dados pessoais no ordenamento brasileiro, afasta a aplicabilidade da lei para tratamento de dados pessoais realizados para fins exclusivos de atividades de investigação e repressão de infrações penais (Art. 4º, III, d), resta esperar que a devida regulamentação das medidas interventivas em matéria de privacidade e proteção de dados pessoais no âmbito jurídico-penal nos termos da reserva de lei e parlamentar, como apontamos ao longo deste trabalho, seja priorizada pelo legislador.

4.8 Demais princípios da Lei Geral de Proteção de Dados

Abordamos nos princípios anteriores os principais princípios quanto à sua adequação às atividades de tratamento de dados pessoais a serem realizadas por autoridades estatais no âmbito jurídico-penal. Os princípios restantes no art. 6° da LGPD são de menor relevância ou, até mesmo, inaplicabilidade no contexto das atividades de tratamento de dados pessoais jurídico penais, tal com o princípio da transparência (art. 6º, VI) como a "garantia, aos titulares, de informações claras, precisas e facilmente

[201] Consultor Jurídico. **Lei de Acesso à Informação pode iluminar as sombras do processo penal.** Disponível em: https://www.conjur.com.br/2016-jan-01/limite-penal-lei-acesso-informacao-iluminar-sombras-processo-penal. Acesso em: 12 ago. 2024.

acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial“ ou o princípio da não discriminação (art. 6º, IX) como “impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos”.

5 O DIREITO PENAL E SUA INTERVENÇÃO NA ERA DA SOCIEDADE DA INFORMAÇÃO

A transformação tecnológica imposta à sociedade transformou também a criminalidade. De acordo com a *European Union Agency for Law Enforcement Cooperation* (2024, p. 6), “o número de criminosos cibernéticos entrando no mercado continua a crescer, graças à adoção de novas tecnologias como também à crescente complexidade das infraestruturas digitais, que expandem a potencial superfície de ataque”[202]. É possível inferir, a partir da afirmação desta agência europeia, que há, simultaneamente, duas situações que impactam diretamente no apetite criminal pela era digital. A sociedade adota o que o mercado despeja de tecnologia, e essa mesma demanda exige investimento em infraestrutura computacional (lógica e equipamentos, *software* e *hardware*) para sustentar essa inovação permanente, tão característica da era digital, e que separa as organizações que permanecerão no futuro das que serão lembradas como existentes no passado.

A título de exemplo, a Kodak, organização dominante em “filmes fotográficos” para revelação de fotos em papel por meio de processos químicos, perdeu sua janela de oportunidade ao não apostar na tecnologia como o caminho para o futuro. Curiosamente, a Kodak abrigou a invenção da primeira câmera digital por Steve Sasson enquanto trabalhava para a Kodak em 1975[203]. Tal erro estratégico conduziu a gigante americana a um pedido de falência em janeiro de 2012 (o que a permitiu reestruturar parte da operação)[204]. Por outro lado, a Samsung, fundada em 1938, iniciou seus negócios vendendo desde seguros até têxteis, sendo seu produto mais “exótico”, a venda de peixes desidratados da Korea para a China[205]. Atualmente, vale mais de 275B de dólares tendo

---

[202] Tradução livre: The number of cybercriminals entering the market continued to grow steadily, thanks to the adoption of new technologies as well as the increasing complexity of digital infrastructures, which expands the potential attack surface.
[203] Forbes. **How Kodak Failed**. Disponível em: https://www.forbes.com/sites/chunkamui/2012/01/18/how-kodak-failed. Acesso em: 22 dez. 2024.
[204] Abc27 News. **On This Date: Kodak declares bankruptcy**. Disponível em: https://www.abc27.com/digital-originals/on-this-date-kodak-declares-bankruptcy-10-years-later. Acesso em: 22 dez. 2024.
[205] World Economic Forum. **Then and now: A bizarre history of the world's biggest tech companies**. Disponível em: https://www.weforum.org/stories/2020/11/tech-technology-company-bizarre-history. Acesso em 22 dez. 2024.

foco na indústria de tecnologia e é considerada uma das líderes globais deste mercado. O investimento (certo ou errado) em tecnologia terá direto impacto na sobrevivência das organizações no futuro.

Ainda, sobre a necessidade permanente de inovação, a evolução da estrutura tecnológica de apoio acaba por dificultar a manutenção do passo em sua absorção por parte dos indivíduos. Não é incomum a adoção de novas tecnologias por parte da sociedade seja por imposição do mercado (por meio da obsolescência "forçada") ou simplesmente pela "tendência". Lidar com tecnologias que se conhece parcialmente (ou, pior, se desconhece) favorece a atuação cibercriminosa, especialmente nos crimes envolvendo fraudes das mais simples às mais complexas.

De acordo com o Instituto de Pesquisa DataSenado[206], "os golpes digitais vitimaram 24% dos brasileiros com mais de 16 anos nos últimos 12 meses. São mais de 40,85 milhões de pessoas que perderam dinheiro em função de algum crime cibernético, como clonagem de cartão, fraude na internet ou invasão de contas bancárias". Entretanto, apesar de tais crimes representarem um negativo impacto na vida dessas pessoas, há outros crimes cibernéticos (também chamados de crimes informáticos, de tipo próprio ou impróprio) com impactos ainda mais profundos (Europol, 2024, p. 10): CSAM (*Child Sexual Abuse Material*, ou material de abuso sexual infantil em tradução livre), CSE (*Child Sexual Exploitation*, ou exploração sexual infantil em tradução livre), *romance fraud* (ou fraude de romance, em tradução livre).

Ainda, há a utilização de diversas técnicas, tecnologias e procedimentos com o objetivo de facilitar ou realizar o crime, tais como inteligência artificial, criptomoedas, criptografia, dentre várias outras.

[206] Senado Notícias. **Golpes digitais atingem 24% da população brasileira, revela DataSenado**. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado. Acesso em: 22 dez. 2024.

5.1 Organizações criminosas na era digital

O custo mundial dos crimes cibernéticos, de acordo com o Fórum Econômico Mundial, é estimado em US$ 10,5 Trilhões anualmente em 2025[207]. Ainda, de acordo com o mesmo Fórum Econômico Mundial, caso fosse considerado o produto de uma "nação", a economia dos crimes cibernéticos seria considerada a terceira maior economia do mundo, atrás apenas de Estados Unidos e China[208]. A criminalidade contemporânea está atenta aos avanços tecnológicos, incorporando-os no desenvolvimento e oferta de CaaS – Crime as a Service (crime como serviço, em tradução livre). O CaaS seria, portanto, uma modalidade de oferta de "serviços" de tecnologia desenvolvidos para a realização primariamente de atividades criminosas das mais diversas naturezas, dada a escassez de mão-de-obra qualificada (ironicamente, para a realização de atividades lícitas ou ilícitas).

São diversos tipos de ofertas para a realização de crimes cibernéticos, preenchendo de comodidade a vida do cibercriminoso: utilização de *malware* previamente elaborado para diversas finalidades, campanhas de *phishing* (distribuição de e-mails com conteúdo malicioso), exploração de vulnerabilidades conhecidas e desconhecidas pelos fabricantes de tecnologia, institutos e agências de controle, dentre outras.

Ainda, inacreditavelmente, há estratégias de mercado utilizadas pelos fornecedores de CaaS, como um "programa de afiliados", conforme descrito pela Europol em seu relatório "*Cyber-Attacks: the apex of Crime-as-a-Service*", onde o contratante utiliza toda a estrutura do fornecedor do *ransomware* (*malware* destinado a criptografar todo o conteúdo eletrônico de determinada vítima, inutilizando-o até que seja pago um "resgate" ao cibercriminoso, geralmente na forma de criptomoedas para evitar sua rastreabilidade).

De acordo com o mesmo relatório, grupos criminosos possuem diversos componentes com diversas habilidades e conhecimentos específicos: programadores,

---

[207] World Economic Forum. **Why we need global rules to crack down on cybercrime**. Disponível em: https://www.weforum.org/stories/2023/01/global-rules-crack-down-cybercrime. Acesso em: 23 dez. 2024.
[208] Critical Start. **Cybercrime: The World's 3rd Largest Economy**. Disponível em: https://www.criticalstart.com/cybercrime-the-worlds-3rd-largest-economy. Acesso em: 23 dez. 2024.

criptógrafos, especialistas em infraestrutura de servidores, redes e sistemas operacionais, engenheiros, *pentesters*, negociadores, recrutadores, gestores de recursos humanos e experts legais. Há, literalmente, uma organização, uma divisão do trabalho e uma hierarquia definida para a condução das atividades ilícitas no submundo da internet e com abrangência global. Ainda, todo este serviço é executado em infraestrutura (servidores, switches de rede, links de dados etc.) própria, especialmente localizada em jurisdições "construídas para serem resilientes ao rastreamento e interrupção oriundos da aplicação da lei"[209], combinando recursos disponíveis em jurisdições "não-cooperativas" com recursos "alugados" em provedores legítimos localizados na Europa e na América do Norte (Europol, 2023, p. 16).

A oferta de crimes como serviços (CaaS) conforme descrito se amolda ao escopo de incidência da Lei 12.850/2013, onde em seu art. 1º, § 1º, temos:

> Art. 1º Esta Lei define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal a ser aplicado.
> § 1º Considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional.
> § 2º Esta Lei se aplica também:
> I - às infrações penais previstas em tratado ou convenção internacional quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;
> II - às organizações terroristas, entendidas como aquelas voltadas para a prática dos atos de terrorismo legalmente definidos.

As infrações penais nesta atividade (CaaS) são diversas: estelionato (Art. 171 do Código Penal), invasão de dispositivo informático (Art. 154-A do Código Penal), dentre outras classificadas como crimes informáticos próprios (aqueles que afetam diretamente sistemas informáticos) ou impróprios (aqueles que usam os sistemas ou a internet como meio, com seus efeitos repercutindo a realidade da vida). Além disso, há "infrações penais previstas em tratado ou convenção internacional" referentes à Convenção de

[209] Tradução livre: The infrastructure of cybercrime services is built to be resilient to law enforcement tracing and disruption.

Budapeste, cuja adesão foi ratificada pelo Brasil por meio do Decreto nº 11.491/2023 de 12 de abril de 2023.

A Convenção de Budapeste foi firmada em 23 de novembro de 2001 e, na atualidade deste estudo, já possui mais de 20 anos, ou seja, a adesão brasileira ocorre quando a própria convenção já se encontra em provável necessidade de revisão frente à toda a evolução tecnológica e social ocorrida nestas mais de duas últimas décadas. Os crimes descritos na Convenção (e consequentemente no Decreto 11.491/2023) possuem certa equivalência com tipos penais existentes no ordenamento jurídico brasileiro.

Assim, de acordo com a Convenção, em seu artigo 6:

> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para tipificar como crimes, em sua legislação interna, as seguintes condutas, quando dolosas e não autorizadas:
> a. a produção, venda, aquisição para uso, importação, distribuição ou a disponibilização por qualquer meio de:
> i. aparelho, incluindo um programa de computador, desenvolvido ou adaptado principalmente para o cometimento de quaisquer dos crimes estabelecidos de acordo com os artigos de 2 a 5;
> ii. uma senha de computador, código de acesso, ou dados similares por meio dos quais se possa acessar um sistema de computador ou qualquer parte dele, com a intenção de usá-lo para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5; e
> b. a posse de qualquer dos instrumentos referidos nos parágrafos a.i ou ii, com a intenção de usá-los para a prática de quaisquer dos crimes previstos nos artigos de 2 a 5. Qualquer Parte pode exigir, por lei, a posse de um número mínimo de tais instrumentos, para que a responsabilidade criminal se materialize.

Nesse sentido, a atividade descrita como CaaS comportaria do Brasil tipificação específica para alcançar (dentre outras atividades) a disponibilização (remunerada ou não) de hardware ou software desenvolvidos ou adaptados principalmente para o cometimento dos crimes de acesso ilegal, interceptação ilícita, violação de dados e interferência em sistema, conforme descritos nos artigos 2 a 5 da Convenção de Budapeste.

Já uma inconsistência com o ordenamento jurídico brasileiro é o mandamento contido no artigo 12 da Convenção de Budapeste, que determinada que “cada Parte adotará medidas legislativas e outras providências necessárias para assegurar que pessoas jurídicas possam ser consideradas penalmente responsáveis por crimes

tipificados de acordo com esta Convenção (...)". A responsabilização penal de pessoas jurídicas é, atualmente, incompatível com a dogmática e ordenamento jurídico brasileiros.

A Lei 12.850/2013 que "define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal" possui em seu bojo diversas disposições que afetam diretamente a privacidade e a proteção dos dados pessoais dos indivíduos investigados. Em seu art. 3º, com exceção dos incisos I e III, todos os seguintes meios de obtenção de prova têm direta afetação ao tema:

> Art. 3º Em qualquer fase da persecução penal, serão permitidos, sem prejuízo de outros já previstos em lei, os seguintes meios de obtenção da prova:
> I - colaboração premiada;
> II - captação ambiental de sinais eletromagnéticos, ópticos ou acústicos;
> III - ação controlada;
> IV - acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais;
> V - interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica;
> VI - afastamento dos sigilos financeiro, bancário e fiscal, nos termos da legislação específica;
> VII - infiltração, por policiais, em atividade de investigação, na forma do art. 11;
> VIII - cooperação entre instituições e órgãos federais, distritais, estaduais e municipais na busca de provas e informações de interesse da investigação ou da instrução criminal.

Apesar do legislador ter realizado disposições sobre essas medidas nas seções subsequentes da lei, há muito que ser devidamente legislado para a apropriada condução do procedimento investigativo como, por exemplo, no art. 10-A, que trata da admissão de infiltração virtual dos agentes de polícia para investigação dos crimes previstos nesta lei e a eles conexos. Neste artigo, em seu parágrafo 4º, há a disposição de renovações de autorização do prazo por até 720 dias (quase 2 anos) para a manutenção da infiltração apenas com única (e vaga) condição de que "seja comprovada sua necessidade". Não há nenhum critério objetivamente estabelecido para tal comprovação, nem requisitos obrigatórios para o juízo de tal necessidade.

5.2 Banco de dados de perfis genéticos

A identificação criminal do civilmente identificado é disciplinada pela Lei nº 12.037/2009 e afastada quando houver a disponibilização de determinados documentos listados no art. 2º da lei, embora seja cabível diante de determinadas condições dispostas em seu art. 3º. O artigo 5º da referida lei estabelece o processo datiloscópico e fotográfico para a identificação criminal na prisão em flagrante ou no inquérito policial (ou outra forma de investigação), entretanto, por meio da Lei nº 12.654/2012, houve a inclusão de parágrafo único prevendo a possibilidade de "coleta de material biológico para a obtenção do perfil genético".

A mesma lei incluiu, por meio do art. 5º-A, a obrigatoriedade de armazenamento em "banco de dados de perfis genéticos, gerenciado por unidade oficial de perícia criminal". Em seu parágrafo segundo, há a atribuição de caráter sigiloso aos dados contidos neste banco de dados, indicando a responsabilização penal a aquele que "permitir ou promover sua utilização para fins diversos dos previstos nesta Lei ou em decisão judicial".

Não há, nesta lei, indícios de qual seria a responsabilização criminal adequada à realização da conduta. Entretanto, entendemos que essa conduta se amoldaria ao tipo penal indicado no art. 325 do Código Penal brasileiro, sob o título de "violação de sigilo funcional":

> Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:
> Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.

O art. 7º-B informa que "a identificação do perfil genético será armazenada em banco de dados sigiloso, conforme regulamento a ser expedido pelo Poder Executivo". Fundamentado nesse mandamento, o Decreto nº 7.950/2013 (posteriormente modificado pelo Decreto nº 9.817/2019) instituiu o Banco Nacional de Perfis Genéticos (BNPG) e a Rede Integrada de Bancos de Perfis Genéticos (RIBPG), que tem como objetivo (Art. 1º, § 1º) "armazenar dados de perfis genéticos coletados para subsidiar ações destinadas à apuração de crimes".

Além da Lei nº 12.037/2009, a Lei nº 7.210/1984 (Lei de Execução Penal) determina que indivíduos condenados pelos crimes dispostos em seu Art. 9º-A tenham, obrigatoriamente, seu perfil genético coletado (ou catalogado). Mas foi efetivamente a partir de 2018, com o "Projeto de Coleta de Amostra de Condenados", que houve um incremento significativo no número de perfis de referência criminal no BNPG: de 7.872 perfis cadastrados para mais de 163 mil perfis genéticos de condenados cadastrados.

Conforme o "XX Relatório da Rede Integrada de Bancos de Perfis Genéticos – RIBPG" de maio de 2024 (apresentando dados estatísticos e resultados entre o período de novembro de 2023 e maio de 2024), a RIBPG compreende "uma ação conjunta entre Secretarias de Segurança Pública (ou instituições equivalentes), Secretaria Nacional de Segurança Pública (SENASP) e Polícia Federal (PF)". Ainda, além de realizarem confrontos entre os dados genéticos coletados e o BNPG da RIBPG, também "são realizados confrontos estaduais com perfis gerados por 23 laboratórios de genética forense (que compõem a RIPBG) e com perfis encaminhados de outros países por intermédio da INTERPOL". O relatório ainda revela que a partir de ano de 2018, a RIBPG passou a ter uma participação mais ativa no compartilhamento internacional de informações, inserindo periodicamente perfis genéticos nas bases de dados da Interpol, tendo enviado 28.024 perfis de vestígios de crimes e 9.367 perfis de restos mortais não identificados até maio de 2024.

De acordo com o relatório, há, até o dia 28 de maio de 2024, 220.565 perfis catalogados no BNPG, sendo Minas Gerais o Estado com maior contribuição absoluta, com 28.618 perfis catalogados. Ainda, segundo o relatório, a taxa de coincidência de perfis genéticos no Brasil é de aproximadamente 6,5%, entretanto, "bases de dados internacionais, estabelecidas há mais tempo e que contam com maior número de referências criminais (amostras de indivíduos), possuem taxas de coincidência maiores (51,37% no NDIS dos EUA e mais que 60% no NDNA do Reino Unido)".

Sobre os aspectos de proteção de dados pessoais na operação do BNPG na RIBPG, o "Manual de Procedimentos Operacionais da Rede Integrada de Bancos de Perfis Genéticos", publicado pelo Comitê Gestor da Rede Integrada de Bancos de Perfis Genéticos, em sua sexta versão até o momento deste estudo, não apresenta orientações minimamente satisfatórias no tocante à segurança da informação (pessoas, tecnologias

e procedimentos). A única menção à proteção de dados pessoais está na seguinte informação:

> A fim de garantir o sigilo das informações e atender às determinações legais, incluindo o respeito à Lei Geral de Proteção de Dados Pessoais (LGPD), os Bancos de Perfis Genéticos que compõem a RIBPG utilizam dados anonimizados, ou seja, os perfis genéticos são armazenados em bancos de dados dissociados de informações identificadoras dos indivíduos a partir dos quais foram gerados. O processo de anonimização dos dados contidos nos bancos apenas é revertido quando ocorre uma coincidência envolvendo o perfil genético nele armazenado. Neste momento, o laboratório detentor dos dados identificadores informa às instâncias competentes sobre as características e origem do perfil genético.

Ocorre que há um erro conceitual grave na informação prestada pelo manual e, consequentemente, na arquitetura de privacidade e proteção de dados pessoais desenhada pelo órgão. De acordo com a Lei 13.709/2018, Art. 5º, III, o conceito de dado anonimizado é “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” e o conceito de anonimização (contido no inciso XI) é “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”.

Portanto, se um processo de “anonimização” pode ser revertido a qualquer momento, este não se trata verdadeiramente de anonimização, mas de qualquer outra característica técnica que tenha como objetivo auxiliar na proteção de dados pessoais. A rigor técnico, este banco de dados não poderia realmente ser anonimizado, uma vez que perderia sua utilidade, não servindo para absolutamente nada caso não houvesse mais possibilidade de identificação de indivíduos a partir dos perfis genéticos catalogados. Portanto, pode ser que o Comitê Gestor se refira a característica de mascaramento de dados, onde os dados se encontram mascarados até o momento em que haja uma coincidência entre o perfil investigado e os perfis cadastrados no Banco Nacional de Perfis Genéticos (BNPG).

O Manual de Procedimentos Operacionais informa, ainda, que “a coleta de condenados pode ocorrer após condenação em primeira instância, não sendo necessário o trânsito em julgado, ressalvadas decisões em contrário”. Entendemos que esta determinação viola princípios corolários do Direito Penal, especialmente o princípio da

presunção de inocência ou princípio da não-culpabilidade, instituído pelo direito fundamental disposto na CRFB, Art. 5º, CRFB, LVII, em que “ninguém será considerado culpado até o trânsito em julgado de sentença penal condenatória”. Viola, também, o direito fundamental da proteção dos dados pessoais, conforme disposto no Art. 5º, LXXIX, da CRFB, uma vez que a submissão de indivíduo a tal procedimento operacional de inclusão no Banco de Dados de Perfis Genéticos (BDPG) antes de trânsito em julgado da condenação criminal representa medida excessivamente danosa, já que a exclusão de perfis genéticos dos bancos de dados ocorrerá somente nas seguintes condições dispostas no Art. 7º-A da Lei 12.037/2009:

> Art. 7º-A. A exclusão dos perfis genéticos dos bancos de dados ocorrerá:
> I - no caso de absolvição do acusado; ou
> II - no caso de condenação do acusado, mediante requerimento, após decorridos 20 (vinte) anos do cumprimento da pena.

Nessas condições, o indivíduo condenado em primeira instância permanecerá catalogado no BDPG ao longo de todo o desenvolvimento do processo penal, o que pode levar literalmente anos até a sua conclusão com o trânsito em julgado de sentença condenatória. Trata-se de verdadeira contradição com a própria lei, já que em seu Art. 6º há a seguinte vedação:

> Art. 6º É vedado mencionar a identificação criminal do indiciado em atestados de antecedentes ou em informações não destinadas ao juízo criminal, antes do trânsito em julgado da sentença condenatória.

Ainda, é de especial relevância analisar a segunda possibilidade de exclusão dos perfis genéticos dos bancos de dados (Art. 7º-A, II), em que decorridos 20 anos de cumprimento da pena, a exclusão pode ser realizada mediante requerimento.

Um importante questionamento se refere ao prazo de 20 anos após o cumprimento da pena para manutenção de perfis genéticos do condenado, seria esta determinação uma imposição de medida excessivamente onerosa ao indivíduo?

De acordo com o Código Penal brasileiro, Art. 64, I:

> Art. 64: para efeito de reincidência

> I - não prevalece a condenação anterior, se entre a data do cumprimento ou extinção da pena e a infração posterior tiver decorrido período de tempo superior a 5 (cinco) anos, computado o período de prova da suspensão ou do livramento condicional, se não ocorrer revogação.

Entretanto, por meio do julgamento do Tema 150 de repercussão geral (RE 593.818/SC), o STF pacificou o entendimento de que seria "plenamente possível a utilização de condenações anteriores para valoração dos maus antecedentes na primeira fase da dosimetria da pena, mesmo que tenha sido ultrapassado período superior a 05 (cinco) anos da extinção da pena".

Ainda que a inclusão do perfil genético do indivíduo no Banco Nacional de Perfis Genéticos seja em razão de condenação "por crime doloso praticado com violência grave contra a pessoa, bem como por crime contra a vida, contra a liberdade sexual ou por crime sexual contra vulnerável", é necessário avaliar se há justificativa suficiente para manutenção por longos períodos, ou até mesmo de forma permanente, de tais registros para acompanhamento por parte do Estado com a finalidade de prevenção de delitos de maior potencial ofensivo.

Nos paradigmáticos casos *Kansas v. Hendricks*[210] (521 U.S. 346 1997) e *United States v. Comstock*[211] (560 U.S. 126 2010), a Suprema Corte dos Estados Unidos determinou que seria constitucional a adoção de procedimentos para a interdição civil "permanente" (na forma de internação) de condenados pode crimes sexuais e que sejam considerados perigosos à sociedade em razão de "anormalidade mental"[212].

No caso de repercussão geral no Recurso Extraordinário 973.837 (RE 973.837[213]) de Minas Gerais, o Ministro Gilmar Mendes enfrenta os argumentos trazidos pela defesa de um condenado por crimes com violência contra a pessoa e crimes hediondos, em que defendem que a criação do banco de dados com perfis genéticos violaria o princípio constitucional da não autoincriminação, bem como ao art. 5º, II, da CFRB. Segundo o Ministro:

---

[210] Justia – U.S. Supreme Court. **Kansas v. Hendricks, 521 U.S. 346 (1997)**. Disponível em: https://supreme.justia.com/cases/federal/us/521/346/. Acesso em: 05 jan. 2025.
[211] Justia – U.S. Supreme Court. **United States v. Comstock, 560 U.S. 126 (2010)**. Disponível em: https://supreme.justia.com/cases/federal/us/560/126/. Acesso em: 05 jan. 2025.
[212] Tradução livre: Mental abnormality.
[213] Supremo Tribunal Federal. **RE 973837**. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4991018. Acesso em: 27 dez. 2024.

> A criação de banco de dados com material genético do apenado não viola o princípio da não autoincriminação (*nemo tenetur se detegere*), vez que decorre de condenação criminal transitada em julgado. Não se cogita violação ao princípio da irretroatividade da lei penal, ainda, por se tratar de norma que prevê mero procedimento de identificação criminal.

O RE 973.837 foi considerado o *leading case* do Tema de repercussão geral nº 905[214], em que é abordada a "constitucionalidade da inclusão e manutenção de perfil genético de condenados por crimes violentos ou por crimes hediondos em banco de dados estatal". O caso ainda não havia transitado em julgado no momento da realização dessa pesquisa.

Também na Ação Direta de Inconstitucionalidade 6.620 (ADI 6620[215]), o Ministro Alexandre de Moraes enfrentou os argumentos do autor da ação em que a criação dos cadastros de pedófilos com fotos das pessoas investigadas ou condenadas "desrespeitava direitos e garantias das pessoas expostas, tais como o direito à intimidade e à privacidade, a dignidade da pessoa humana e o direito à imagem e à honra".

O Ministro Alexandre de Moraes reconheceu que:

> Os cadastros podem ter dados pessoais e fotos dos condenados por crimes sexuais ou de violência doméstica, desde que a condenação seja definitiva (quando não cabe mais recurso). As pessoas que sejam apenas investigadas por esses crimes, ou que ainda estejam recorrendo de uma condenação, não podem ser incluídas no cadastro, porque o art. 5º, LVII, da Constituição determina que ninguém será considerado culpado até a condenação definitiva (presunção de inocência).

Assim, é flagrante a inadequação da orientação contida no Manual de Procedimentos Operacionais da Rede Integrada de Bancos de Perfis Genéticos com a própria Lei 12.037/2009, com a jurisprudência e os princípios constitucionais penais em tela.

---

[214] Supremo Tribunal Federal. **Tema 905 - Constitucionalidade da inclusão e manutenção de perfil genético de condenados por crimes violentos ou por crimes hediondos em banco de dados estatal**. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=4991018&numeroProcesso=973837&classeProcesso=RE&numeroTema=905. Acesso em: 27 dez. 2024.

[215] Supremo Tribunal Federal. **ADI 6.620**. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/Informaosociedade.ADI6620.cadastrodepedfilosRev.FSPLC.pdf. Acesso em 27 dez. 2024.

A Lei 12.037/2009 ainda autoriza, em seu Art. 7º-C, a criação do chamado “Banco Nacional Multibiométrico e de Impressões Digitais” (BNMID), que teria 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”. Este banco de dados seria alimentado “quando colhidos em investigações criminais ou por ocasião da identificação criminal”, conforme parágrafo terceiro do mesmo Art. 7º-C, ou quando o indivíduo se encontrar na condição de preso provisório, “quando não tiverem sido extraídos por ocasião da identificação criminal”, conforme parágrafo quarto.

De acordo com o parágrafo primeiro do Art. 7º-C da Lei 12.037/2009, “a formação, a gestão e o acesso ao Banco Nacional Multibiométrico e de Impressões Digitais serão regulamentados em ato do Poder Executivo federal”. Ocorre que esta regulamentação do Poder Executivo Federal nunca ocorreu, ou seja, ainda não houve a criação deste banco de dados (de fato, sequer poderia ocorrer, uma vez que não há regulamentação).

Entretanto, alguns representantes parlamentares já querem se antecipar propondo modificações à Lei 12.037/2009 e aqui encontramos uma alarmante situação de risco à privacidade e proteção de dados dos indivíduos, assunto que será abordado no próximo tópico.

5.3 A prática de *fishing expedition*

À época desta pesquisa, temos em curso os Projetos de Lei nº 1.392/2021 e 2.784/2022.

O PL 1.395/2021[216] propõe a seguinte modificação:

> Art. 1º Altera a redação do § 11 do art. 7º-C da lei 12.037 de 1º de outubro de 2009 (Lei de identificação criminal do civilmente identificado), que passa a vigorar com a seguinte redação:
> “Art. 7º-C, § 11: A autoridade policial e o Ministério Público, para fins de instrução de inquérito ou de procedimentos investigatórios criminais, poderão requisitar o acesso ao Banco Nacional Multibiométrico e de Impressões Digitais”. (N.R.)
> Art. 2º Esta lei entra em vigor na data de sua publicação.

[216] Câmara dos Deputados. **PL 1395/2021**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2278012. Acesso em: 23 dez. 2024.

Ou seja, a autoridade policial e o Ministério Público poderiam requisitar acesso ao Banco Nacional Multibiométrico e de Impressões Digitais para fins de instrução de inquérito ou de procedimentos ainda na fase investigatória criminal, ao contrário de "requerer ao juiz competente, no caso de inquérito ou ação penal instaurados", conforme atual redação do parágrafo 11. A justificativa contida no Projeto de Lei 1.395/2021 é simples e direta: "cuida-se de medida que visa facilitar o acesso ao banco de dados a fim de identificar pessoas que tenham cometido crimes, o que facilitaria a investigação criminal (...), decerto estas medidas contribuirão para o melhor desenvolvimento do processo penal e da Justiça".

Ainda, o texto apresentado no PL 1.395/2021 afirma ter por escopo "aperfeiçoar o projeto do Ministério da Justiça e Segurança Pública, consubstanciado no texto do §11 do art. 7º-C em vigência, haja vista não se tratar de matéria sujeita à reserva de jurisdição".

Em 2024, foi apensado ao PL 1.395/2021 o PL 524/2024, de proposição do então deputado Kim Kataguiri, que visa alterar justamente a Lei 12.850/2013 (Lei das organizações criminosas) incluindo, dentre outras modificações, a permissão de uso de *malware* ou *software* espião como meio de obtenção de prova. Dentre as disposições do Projeto de Lei 524/2024[217], agora apensado ao Projeto de Lei 1.395/2021, um dos artigos propostos que mais chamam a atenção no tocante à privacidade e proteção de dados pessoais é o Art. 21-C:

> Art. 21-C O juiz poderá autorizar o acesso a computadores que não os do investigado, mas que estão sendo por ele utilizados para comunicação ou para armazenar dados, ou mesmo equipamentos que não estão sendo utilizados pelo suspeito, mas que contêm dados importantes para a investigação.

Diversas questões sobre a privacidade e proteção de dados pessoais em investigações criminais se impõem sobre tais argumentos apresentados como

[217] Câmara dos Deputados. **PL 542/2024**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2419194. Acesso em: 23 dez. 2024.

justificativas ao referido Projeto de Lei. À época da proposição do PL 1.395/2021, a bem da verdade, a Emenda Constitucional 115 ainda não havia sido promulgada[218].

O Art. 21-C proposto pelo PL 524/2024 apensado ao PL 1.395/2021 admitiria "o acesso a computadores que não os do investigado, mas que estão sendo por ele utilizados para comunicação ou para armazenar dados, ou mesmo equipamentos que não estão sendo utilizados pelo suspeito, mas que contêm dados importantes para a investigação".

Tal disposição configuraria a proibida prática de *fishing expedition*, onde se empreende investigações especulativas, indeterminadas e indiscriminadas, sem objetivo certo, na esperança de encontrar qualquer elemento de prova que subsidie uma acusação. Esta prática em nada se equipara à serendipidade, ou encontro fortuito de elementos de prova de modo inesperado, que ocorre no decorrer de uma investigação legalmente autorizada.

De acordo com Rosa, Da Silva e Silva (2022, p. 50):

> É possível definir pescaria probatória (*fishing expedition*) como a apropriação de meios legais para, sem objetivo traçado, "pescar" qualquer espécie de evidência, tendo ou não relação com o caso concreto. Trata-se de uma investigação especulativa indiscriminada, sem objetivo certo ou declarado que, de forma ampla e genérica, "lança" suas redes com a esperança de "pescar" qualquer prova para subsidiar uma futura acusação ou para tentar justificar uma ação já iniciada.

Alexandre Morais da Rosa[219] complementa:

> O termo se refere à incerteza própria das expedições de pesca, em que não se sabe, antecipadamente, se haverá peixe, nem os espécimes que podem ser fisgados, muito menos a quantidade, mas se tem "convicção" (o agente não tem provas, mas tem convicção). Com o uso de tecnologia (Processo Penal 4.0), cada vez mais se obtém a prova por meios escusos (especialmente em unidades de inteligência e/ou investigações paralelas, todas fora do controle e das regras democráticas), requentando-se os "elementos obtidos às escuras" por meio de investigações de origem duvidosa, "encontro fortuito" dissimulado ou, ainda, por "denúncias anônimas *fakes*".

---

[218] Senado Notícias. **Promulgada emenda constitucional de proteção de dados**. Disponível em: https://www12.senado.leg.br/noticias/materias/2022/02/10/promulgada-emenda-constitucional-de-protecao-de-dados. Acesso em 24 dez. 2024.

[219] Conjur. **A prática de fishing expedition no processo penal**. Disponível em: https://www.conjur.com.br/2021-jul-02/limite-penal-pratica-fishing-expedition-processo-penal. Acesso em: 26 dez. 2024.

Ainda, Rosa, Da Silva e Silva (2022, p. 55) ressaltam que:

> A *fishing expedition*, ou pescaria probatória, aproveita-se 'dos espaços de exercício de poder para subverter a lógica das garantias constitucionais, vasculhando-se a intimidade, a vida privada, enfim, violando-se direitos fundamentais, para além dos limites legais'.

Apesar disso, conforme Gabriela Monico[220], frequentemente, nas investigações realizadas pelas autoridades investigativas, "o argumento dos órgãos de investigação é que tais documentos e esclarecimentos poderiam ser obtidos diretamente perante o órgão estatal responsável pela retenção de tal documento ou informação, mas que por uma agilidade, requisitam diretamente ao investigado", o que em muitas ocasiões habilitam o início de uma acusação, ou seja, com "provas" produzidas pelo próprio indivíduo.

A prática de *fishing expedition* já foi abordada na jurisprudência brasileira, mas ainda com certa controvérsia. No julgamento da Reclamação 43.479 (RCL 43.479/RJ), o Ministro Gilmar Mendes realizou a apreciação jurídica do caso em que a "autoridade reclamada determinou a realização de buscas e apreensões contra praticamente setenta escritórios e advogados com base em fundamentação genérica e não delimitada" mencionando o referido conceito também abordado no julgamento do Habeas Corpus 137.828 (HC 137.828 de 2016). Neste Habeas Corpus se discutiu a ilicitude de uma interceptação telefônica "pré-delitual" em uma verdadeira "interceptação prospectiva" com nenhuma possibilidade de sustentação de tal medida com base em razoáveis indícios de materialidade ou autoria de qualquer conduta criminosa.

Tal prática, segundo palavras do próprio Ministro, configuraria "ampla e indiscriminada devassa da privacidade que se encontra na base da compreensão da proibição do *fishing expedition*". Ainda, Rosa, Da Silva e Silva (2022, p. 57), ao abordar a publicidade frequentemente dada de modo inadequado aos "elementos de prova" obtidos pelas autoridades investigativas, denunciam que "trazer a público provas que são

[220] Conjur. **Pescaria probatória: investigação criada pelo próprio investigado**. Disponível em: https://www.conjur.com.br/2024-jun-15/pescaria-probatoria-investigacao-criada-pelo-proprio-investigado. Acesso em: 26 dez. 2024.

obtidas ilicitamente é prática típica de *lawfare*, onde o acusador emprega manobras para burlar o sistema jurídico e alcançar a condenação a qualquer custo".

No tocante às requisições de dados cadastrais para provedores de acesso ou de aplicações, o Marco Civil da Internet (Lei nº 12.965/2014) foi modificado pelo Decreto 8.771/2016 para conferir maior proteção à privacidade e proteção de dados pessoais de indivíduos. Seu Art. 11 passou a ter a seguinte redação:

> Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.
> § 1º O provedor que não coletar dados cadastrais deverá informar tal fato à autoridade solicitante, ficando desobrigado de fornecer tais dados.
> § 2º São considerados dados cadastrais:
> I - a filiação;
> II - o endereço; e
> III - a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.
> § 3º Os pedidos de que trata o caput devem especificar os indivíduos cujos dados estão sendo requeridos e as informações desejadas, sendo vedados pedidos coletivos que sejam genéricos ou inespecíficos.

Assim, são expressamente proibidos pedidos coletivos que sejam genéricos ou inespecíficos, convertendo em obrigatoriedade a especificação dos indivíduos sobre os quais dados são requeridos.

No Recurso em Mandado de Segurança 62.562 (RMS 62.562), a Quinta Turma determinou a destruição de todo o material apreendido em uma empresa em razão do reconhecimento de *fishing expedition* durante diligência de busca e apreensão.

De acordo com o processo, "no curso da investigação de suposta organização criminosa que estaria envolvida em desvios de patrimônio do município de Poconé (MT), foi determinada a cópia de todo o banco de dados de uma empresa responsável pelo gerenciamento eletrônico de abastecimento e manutenção da frota da prefeitura".

O Ministro Reynaldo Soares da Fonseca, ressaltou que não foi indicado nenhum indício de participação da empresa nos delitos investigados. O Ministro destacou trecho do processo segundo o qual "a autoridade policial afirmou que somente após a análise dos *e-mails* coletados se poderia verificar a existência ou não de conluio fraudulento entre a empresa e os servidores da prefeitura". Ainda, afirma o Ministro:

> Os indícios de autoria antecedem as medidas invasivas, não se admitindo em um Estado Democrático de Direito que primeiro sejam violadas as garantias constitucionais para só então, em um segundo momento, e eventualmente, se justificar a medida anterior, sob pena de se legitimar verdadeira *fishing expedition*, conhecida como pescaria probatória, ou seja, "a procura especulativa, no ambiente físico ou digital, sem 'causa provável', alvo definido, finalidade tangível ou para além dos limites autorizados (desvio de finalidade), de elementos capazes de atribuir responsabilidade penal a alguém".

Já em sentido diferente do abordado no RCL 43.479 e no RMS 62.562, no julgamento do Recurso em Habeas Corpus 157.143 (RHC 157.143), a Sexta Turma considerou que o acesso aos dados telemáticos extraídos dos celulares de advogados investigados em uma operação policial não configurou investigação especulativa (*fishing expedition*), tampouco serendipidade.

O caso se tratava de advogados que utilizariam seus aparelhos celulares para coagir testemunhas a prestarem depoimentos falsos em juízo, em audiência da ação penal decorrente de investigação policial que apurou a prática de diversos crimes (concussão, estelionato, falsidade ideológica, facilitação à fuga de preso, usurpação de função pública).

Ao STJ, os advogados pediram a limitação do conteúdo dos dados a serem extraídos dos celulares apreendidos, sob o fundamento de preservação do sigilo profissional. Segundo o relator do caso, Ministro Sebastião Reis Junior, “estava clara no processo a impossibilidade técnica de extração parcial dos dados, sendo necessário o processamento integral e a posterior análise do material para a coleta do que interessava à investigação”. Ainda, “o mesmo raciocínio poderia perfeitamente ser aplicado quando do acesso aos dados telemáticos dos celulares, os quais foram apreendidos em razão da existência de sérios indícios da prática de crime por meio dos aparelhos”.

Esta análise que se apresenta como “impossível tecnicamente” para o Ministro, seria uma típica oportunidade para análise sem maiores dificuldades técnicas a ser realizada por sistemas de inteligência artificial (conforme ainda abordaremos oportunamente neste capítulo), dada a grande quantidade de dados em formato não estruturado (conversas em aplicativos de mensagens) e a necessidade de identificação de condutas criminosas específicas.

5.4 A infiltração encoberta virtual de agentes

O Direito Penal na era da sociedade da informação não conseguiria deixar de render-se à aplicação de técnicas ofensivas geralmente utilizadas pelos cibercriminosos para a obtenção de dados e informações que subsidiem suas investigações.

A obtenção de dados telemáticos de indivíduos investigados pode ser executada de diversas maneiras, a depender do que se busca e das dificuldades encontradas ao longo do procedimento. Observando apenas os aspectos técnicos, em praticamente nada se difere dos procedimentos utilizados pelos cibercriminosos ou pelos *pentesters* (profissionais especializados em segurança da informação ofensiva que prestam serviços de testes de intrusão).

Neste sentido, a ação policial de infiltração encoberta virtual (ou suas outras diversas nomenclaturas: infiltração online, infiltração virtual etc.) se valerá do *framework* desenvolvido por Lockheed Martin[221], o chamado "*Cyber Kill Chain*" ou de outro equivalente. De acordo com Meredith (2022, p. 21), "o *Cyber Kill Chain* (CKC) são passos que traçam estágios de um ataque, a partir do reconhecimento até a extração de dados"[222]. Estas etapas, de acordo com o autor, são compostas por: reconhecimento, armamento, entrega (do armamento), exploração, instalação, comando e controle, e ações e objetivos.

A infiltração online no Brasil, enquanto técnica autorizada de investigação a ser utilizada pela autoridade policial (em determinados casos, sob determinadas condições), se encontra em um verdadeiro "limbo" regulatório no momento da elaboração desta pesquisa.

A instituição da técnica de "infiltração de agentes de polícia na internet" pela Lei nº 13.441/2017 pode ser considerada como o início de um debate jurídico que ainda não se encerrou (até o momento). Esta lei regulamenta a "infiltração de agentes de polícia para a investigação de crimes contra a dignidade sexual de criança e de adolescente" nos

[221] Lockheed Martin. **The Cyber Kill Chain**. Disponível em: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. Acesso em: 28 dez. 2024.
[222] Tradução livre: The Cyber Kill Chain (CKC) are steps that trace stages of an attack, right from reconnaissance through to exfiltration of data.

meios “cibernéticos”, modificando a Lei nº 8.069/1990 (Estatuto da Criança e do Adolescente), acrescentando a Seção V-A ao seu escopo regulatório.

A infiltração de agentes encobertos não é novidade no ordenamento jurídico, tendo sido admitida previamente na lei nº 11.343/06 (lei de combate ao tráfico de drogas) e na lei nº 12.850/13 (lei de combate às organizações criminosas). Entretanto, a infiltração virtual é o aspecto inovador da lei nº 13.441/2017. A admissão da infiltração encoberta online, segundo esta lei, deverá ser precedida de autorização judicial, que estabelecerá os limites da infiltração para obtenção de prova (Art. 190-A, I). Requerimento do Ministério Público deverá demonstrar a sua necessidade, o alcance das condutas policiais e dados de identificação dos policiais (Art. 190-A, II) e esta medida poderá ser renovada a cada 90 dias, desde que o total não exceda 720 dias (Art. 190-A, III). Tal técnica investigativa introduzida pela Lei nº 13.441/2017 é destinada exclusivamente os crimes contra a dignidade sexual de criança e adolescente (Arts. 240, 241, 241-A, 241-B, 241-C e 241D da lei nº 8.069/1990 e os crimes dispostos nos Arts. 271-A, 218, 218-A, 218-B e 154-A do Código Penal brasileiro).

O tipo contido no Art. 154-A do Código Penal brasileiro se refere ao crime de invasão de dispositivo informático. Este tipo penal não é destinado exclusivamente aos crimes cometidos contra a dignidade sexual de menores, entretanto, apesar de existir argumentação que afirme que a técnica investigativa de infiltração encoberta online possa ser utilizada na investigação de crimes gerais de invasão a dispositivo informático[223], a melhor interpretação, em nosso entendimento, é que esta técnica investigativa somente poderia ser utilizada (no escopo desta lei) quando o crime de invasão a dispositivo informático estiver conectado com os crimes contra a dignidade sexual de criança e adolescente (dispostos nos tipos supracitados). Há, inclusive, à época da elaboração desta pesquisa, projeto de lei para modificação do Estatuto da Criança e do Adolescente para comportar a infiltração virtual de agentes policiais para

[223] Conjur. **Lei 13.441/17 instituiu a infiltração policial virtual**. Disponível em: https://www.conjur.com.br/2017-mai-16/academia-policia-lei-1344117-instituiu-infiltracao-policial-virtual. Acesso em: 28 dez. 2024.

investigação de “qualquer” crime cometido contra crianças e adolescentes (Projeto de Lei nº 2.891/2020[224])

Contudo, o escopo de aplicação da técnica investigativa restrita aos crimes contra a dignidade sexual de crianças e adolescentes encontra, na contemporaneidade, forte apelo para a remoção dessa restrição para que seja aplicável à investigação de crimes em geral de maior potencial ofensivo. Nesta esteira, a promulgação da Lei nº 13.964/2019 (chamada de pacote anticrime) modificou a Lei nº 12.850/2013 (Lei de combate às organizações criminosas) para permitir a utilização de agentes policiais infiltrados virtualmente a fim de investigar os crimes previsto nesta lei e a eles conexos, praticados por organizações criminosas, com disposições relativamente semelhantes às introduzidas no Estatuto da Criança e do Adolescente.

A falta de legislação que regulamente essa técnica investigativa de modo geral ensejou a proposição de Ação Direta de Inconstitucionalidade por Omissão de nº 84 (ADO 84) pelo então Procurador-Geral da República em 13 de dezembro de 2023, arguindo-se a ausência de atuação normativa do Congresso Nacional “na regulação do uso, por órgãos e agentes públicos, de programas de intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal”. Por requerimento do próprio órgão ministerial, tal ADO foi convertida na Arguição de Descumprimento de Preceito Fundamental de nº 1143 (ADPF 1143). Tal ação tem como ministro relator o Ministro Cristiano Zanin e não havia sido julgada à época desta pesquisa.

Argumenta a PGR que:

> É que, a partir dos mais recentes avanços tecnológicos, houve uma proliferação global de ferramentas de intrusão virtual, utilizadas no âmbito de **serviços de inteligência e de órgãos de repressão estatais** [grifo do autor], para a vigilância remota, secreta e invasiva de dispositivos móveis de comunicação digital, sob o pretexto do combate ao terrorismo e ao crime organizado.
> Tais ferramentas tecnológicas são aptas a interceptar comunicações telefônicas e telemáticas, a partir da “infecção” de dispositivos eletrônicos por um programa espião *(spyware*) e, com isso, possibilitar aos intrusos monitorar conversas, escutar o som ambiente pelo microfone do dispositivo; captar imagens por meio das câmeras frontal e traseira; determinar a localização em tempo real, por meio do sistema de GPS; capturar as imagens da tela e acompanhar em tempo real

[224] Senado Federal. **Projeto de Lei nº 2891, de 2020**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/142121. Acesso em: 29 dez. 2024.

> tudo o que é digitado (*keylogger*) ou visualizado pelo usuário, funcionalidades que podem vir a ser obtidas sem qualquer intervenção do usuário-vítima ("*zero click*").

O autor ainda aponta a "ocorrência não só de violações à garantia do sigilo de dados e de comunicações, como também às garantias da intimidade, da vida privada e do devido processo legal (...)", graves impactos a direitos fundamentais advindos da utilização desregulada e ilegítima desses recursos por parte do poder público, conforme relatório produzido pelo Gabinete do Alto Comissariado da Nações Unidas para os Direitos Humanos (A/HRC/51/17)[225].

O relatório A/HRC/51/17 (*The right to privacy in the digital age*, ou "o Direito à privacidade na era digital", em tradução livre) aborda, dentre outros assuntos, a utilização de ferramentas de monitoramento virtual (*spyware*), que:

> (...) uma vez instalados, garantem completo e irrestrito acesso a todos os sensores e informações nos dispositivos infectados, efetivamente transformando a maioria dos smartphones em verdadeiros dispositivos de vigilância 24-horas, acessando a câmera e microfone, dados de geolocalização, e-mails, mensagens, fotos e vídeos, bem como todas as aplicações. [226]

Como abordamos no início deste tópico, a utilização de software especialmente elaborado para realização de ações nos objetivos é frequente no caminho de intrusão (*Cyber Kill Chain*) nas etapas de armamento, exploração, instalação e obtenção dos objetivos. Esta não é a única maneira de se obter acesso ao conteúdo das comunicações, por exemplo, uma vez que outras técnicas poderiam ser utilizadas, como a interceptação das comunicações (técnica chamada *Man in the Middle*, ou "homem no meio", em tradução livre) em que o agente captura a comunicação entre dois (ou mais) dispositivos de interlocutores simplesmente obtendo acesso à estrutura de rede (*switches, wireless access points, firewalls*, dentre outros).

---

[225] United Nations Digital Library. **The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights**. Disponível em: https://digitallibrary.un.org/record/3985679?ln=en&v=pdf. Acesso em: 28 dez. 2024.

[226] Tradução livre: (...) once installed, grants complete and unrestricted access to all sensors and information on infected devices, effectively turning most smartphones into 24-hour surveillance devices, accessing the camera and microphone, geolocation data, e-mails, messages, photos and videos, as well as all applications.

Ocorre que, justamente com o objetivo de preservar o aspecto da confidencialidade das comunicações, várias técnicas criptográficas são cada vez mais utilizadas para tornar “ilegível” a comunicação entre dois interlocutores. Assim, de nada adianta o sucesso na interceptação dos dados trafegados entre dois dispositivos envolvidos em uma comunicação criptografada de ponta a ponta, uma vez que os dados interceptados não estarão em um formato compreensível e o agente interceptador não possui acesso às chaves criptográficas aptas a decodificar aquela comunicação (ao menos em tese não deveria ter acesso).

Outra técnica criptográfica comumente utilizada de forma complementar à técnica de criptografia das comunicações, é a criptografia do próprio conteúdo a ser comunicado no dispositivo originário para que seja decodificado quando já tiver sido recebido pelo (legítimo) destinatário. É fundamental que se distinga adequadamente as duas técnicas: na primeira técnica abordada, o canal de comunicação é criptografado. Na segunda técnica, o conteúdo comunicado já se encontra criptografado. É perfeitamente possível combinar as duas técnicas para se obter melhor e maior segurança.

Nestas situações, o agente policial investigativo tem menos opções à sua disposição e é aqui que a técnica de infiltração virtual no dispositivo do investigado toma lugar. O “*Hacking* Governamental”, segundo Dutra *et al*. (2023, p. 13), seria:

> No âmbito das investigações criminais realizadas pelo poder público, as medidas sociais e tecnológicas de exploração de vulnerabilidades em bancos de dados, programas de computador, sistemas computacionais, redes de comunicação ou dispositivos eletrônicos a fim de acessar dados digitais sem a autorização do responsável pelo ambiente digital ou da pessoa afetada”.

Uma vez que a comunicação entre os dispositivos esteja criptografada, a maneira mais comum de se obter acesso “encoberto” aos dados que se busca extrair é por meio da instalação de software espião (*spyware*) no dispositivo do investigado. Assim, por meio do monitoramento online, a criptografia aplicada nas comunicações em nada protegerá os indivíduos, uma vez que o agente se encontrará infiltrado diretamente no próprio dispositivo originário, ou seja, terá acesso aos dados diretamente na fonte deles. E a criptografia de conteúdo também não terá efeito de segurança dos dados, uma vez que o software espião instalado utiliza de acesso privilegiado ao dispositivo e consegue

acesso a todos os dados armazenados no dispositivo como se fosse o próprio indivíduo proprietário dos dados.

Dutra *et al*. (2023, p. 16) afirmam que “resumidamente, o uso do *hacking* governamental pressupõe uma exploração às vulnerabilidades já existentes nos sistemas de segurança, e é incitado como alternativa para possibilidade de acesso aos dados criptografados”, entretanto, a realidade é ainda mais preocupante, já que dentro das metodologias disponíveis para intrusão, há outras maneiras de o agente fragilizar a segurança dos sistemas dos dispositivos do alvo da investigação para serem acessados posteriormente na obtenção de seus objetivos sem o conhecimento do proprietário ou detentor. O *phishing*, por exemplo, é “uma técnica de ataque que combina ‘engenharia social’ e métodos de manipulação técnica para persuadir usuários de internet a ‘fornecer informações sensíveis (...)’”[227] (Ribeiro; Guedes; Cardoso, 2024, p. 2). Adicionalmente, no ataque baseado em *phishing*, é perfeitamente possível que o agente realize a instalação de software RAT[228] (*Remote Access Trojan* ou Trojan de Acesso Remoto, em tradução livre) para, assim, permitir sua intrusão.

Com a utilização de software espião, o agente infiltrado consegue ler, acessar, copiar, espelhar, transferir, comunicar, extrair e até mesmo modificar ou eliminar o conteúdo armazenado no dispositivo. Em razão disso, a Procuradoria-Geral da República argumenta na ADPF 1143 (convertida a partir da ADO 84):

> O ponto central da controvérsia que a presente ação cinge-se ao uso secreto e abusivo desses softwares e ferramentas, sem autorização judicial, tampouco limites ou salvaguardas, de forma contrária à tutela do interesse público e aos deveres de proteção dos direitos fundamentais, que se impõem em um Estado de direito. (...) Ao não estabelecer a disciplina regulamentadora da utilização, por órgãos e agentes públicos, de programas para intrusão virtual remota e de ferramentas de monitoramento secreto e invasivo de aparelhos digitais de comunicação pessoal– smartphones, tablets e dispositivos eletrônicos similares– o legislador nacional incide em omissão contrária à exigência imposta no art. 5º, X e XII, da CF, provocando redução arbitrária e injustificada do nível de proteção das garantias fundamentais previstas naquelas normas constitucionais, com ofensa ao princípio da proporcionalidade, derivado do postulado do devido processo legal (art. 5º, LIV, da CF), em sua dimensão substantiva.

[227] Tradução livre: A phishing attack is a combination of “social engineering” and technical manipulation methods to persuade Internet users “into giving away sensitive information (…)”.
[228] Fortinet. **Cavalo de Troia de acesso remoto (RAT)**. Disponível em: https://www.fortinet.com/br/resources/cyberglossary/remote-access-trojan. Acesso em: 30 dez. 2024.

Como exemplo dos extensos danos e violações a direitos fundamentais, um *spyware* que tomou conta da discussão global sobre o assunto foi o chamado “Pegasus”, criado pelo NSO Group (inclusive mencionado pela ADPF 1143). Segundo sua página oficial na internet, o NSO Group trabalha com “cyber inteligência para segurança e estabilidade global”[229], criando “tecnologia que ajuda agências governamentais a prevenir e investigar terrorismo e crimes para salvar milhares de vidas ao redor do mundo”[230].

Entretanto, por meio do chamado *Pegasus Project* (ou Projeto Pegasus, em tradução livre), segundo a Anistia Internacional[231], houve uma “investigação colaborativa que envolveu mais de 80 jornalistas de 17 organizações de mídia em 10 países coordenado por *Forbidden Stories* com o suporte técnico da *Amnesty International’s Security Lab*”. A pesquisa realizada “trouxe à tona vigilância ilícita, ampla, persistente e contínua, e abusos a direitos humanos perpetrados utilizando o *spyware* Pegasus do NSO Group”[232].

Apesar da falta de regulamentação específica, há utilização de diferentes tipos e fabricantes de *spyware* (ou software espião) pela administração pública brasileira. De acordo com um estudo realizado em 2022 e reproduzido em Nota Técnica produzida pelo IP.rec – Instituto de Pesquisa em Direito e Tecnologia do Recife (2024, p. 2), foram “identificados 209 contratos entre o poder público e empresas privadas vendedoras de ferramentas de intrusão a dispositivos informáticos, (...) tanto a nível federal como a nível estadual (...)”. Em resposta à omissão legislativa (ADPF 1143), foi encaminhado o Projeto de Lei nº 402/2024[233] no Senado, de autoria do Senador Alessandro Vieira, com o objetivo de “disciplinar a utilização de ferramentas de monitoramento remoto de terminais de comunicações pessoais por órgãos e agentes públicos, civis e militares”, entretanto, ainda de modo bastante insuficiente.

---

[229] Tradução livre: Cyber intelligence for global security and stability.
[230] Tradução livre: technology that helps government agencies prevent and investigate terrorism and crime to savethousands of lives around the globe.
[231] Amnesty International. **Forensic Methodology Report: How to catch NSO Group’s Pegasus**. Disponível em: https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/#_ftn1. Acesso em: 29 dez. 2024.
[232] Tradução livre: This research has uncovered widespread, persistent and ongoing unlawful surveillance and human rights abuses perpetrated using NSO Group’s Pegasus spyware.
[233] Senado Federal. **Projeto de Lei nº 402, de 2024**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/162146. Acesso em: 30 dez. 2024.

Enquanto isso, em 2023, por meio do Agravo em Recurso Especial nº 2.309.888-MG (AREsp 2.309.888-MG), o Ministro Reynaldo Soares da Fonseca atribuiu legitimidade ao uso da técnica de infiltração encoberta virtual no combate à criminalidade moderna, admitindo sua utilização para qualquer crime "quando a prova não puder ser produzida por outros meios disponíveis, desde que comprovada sua necessidade". No caso apreciado, o Ministro concebe como plausível a equiparação do "espelhamento autorizado via software Whatsapp Web à modalidade de infiltração do agente, (...) respeitados os parâmetros de proporcionalidade, subsidiariedade, controle judicial e legalidade, calcado pelo competente mandado judicial".

É um entendimento diametralmente oposto ao proferido pela Ministra Laurita Vaz, relatora da Sexta Turma do STJ, no julgamento realizado referente ao Recurso em Habeas Corpus nº 99.735/SC (RHC 99.735/SC) em 2018, em que considerou inválida a prova obtida pelo espelhamento de conversas via WhatsApp Web pelas seguintes razões:

> Primeiro: ao contrário da interceptação telefônica, no âmbito da qual o investigador de polícia atua como mero observador de conversas empreendidas por terceiros, no espelhamento via WhatsApp Web o investigador de polícia tem a concreta possibilidade de atuar como participante tanto das conversas que vêm a ser realizadas quanto das conversas que já estão registradas no aparelho celular, haja vista ter o poder, conferido pela própria plataforma online, de interagir nos diálogos mediante envio de novas mensagens a qualquer contato presente no celular e exclusão, com total liberdade, e sem deixar vestígios, de qualquer mensagem passada, presente ou, se for o caso, futura.
> (...)
> Segundo: ao contrário da interceptação telefônica, que tem como objeto a escuta de conversas realizadas apenas depois da autorização judicial (*ex nunc*), o espelhamento via Código QR viabiliza ao investigador de polícia acesso amplo e irrestrito a toda e qualquer comunicação realizada antes da mencionada autorização, operando efeitos retroativos (*ex tunc*).
> Terceiro: ao contrário da interceptação telefônica, que é operacionalizada sem a necessidade simultânea de busca pessoal ou domiciliar para apreensão de aparelho telefônico, o espelhamento via Código QR depende da abordagem do indivíduo ou do vasculhamento de sua residência, com apreensão de seu aparelho telefônico por breve período de tempo e posterior devolução desacompanhada de qualquer menção, por parte da Autoridade Policial, à realização da medida constritiva, ou mesmo, porventura – embora não haja nos autos notícia de que isso tenha ocorrido no caso concreto –, acompanhada de afirmação falsa de que nada foi feito.

Entendemos que o espelhamento do *WhatsApp Web* não permite observar fatores essenciais na produção de elementos de prova válidos juridicamente e que respeitem

integralmente a manutenção da integridade da cadeia de custódia. Isto porque o agente policial poderia enviar mensagens e depois apagá-las “somente para si”, ou seja, somente na conta que possui acesso, mas deixando que os efeitos se operem no interlocutor. Por exemplo, um agente policial poderia “provocar” a abordagem de um assunto enviando uma mensagem que toque no assunto junto ao interlocutor, mas de modo que não deixe claro que foi ele quem iniciou a conversa, e depois apagá-la “somente para si”, de modo que a conversa flua com o interlocutor e os elementos de prova sejam, então, produzidos. Além disso, seria impossível distinguir quem efetivamente realizou a conversa, podendo ser alegado a qualquer momento que não foi o proprietário do aparelho que o fez.

No AREsp 2.309.888-MG, o Ministro Reynaldo Soares da Fonseca afirmou que:

> No caso dos autos, não houve comprovação de qualquer adulteração no decorrer probatório, nenhum elemento veio aos autos a demonstrar que houve adulteração da prova, alteração na ordem cronológica dos diálogos ou mesmo interferência de quem quer que seja, a ponto de invalidar a prova, salvo, naturalmente, a eventual ingerência e interação que decorre da atuação na ação controlada e da condição de agente infiltrado aqui reconhecida, não podendo referida invalidade ser presumida.

Realmente seria uma tarefa extremamente onerosa para o investigado ou réu realizar tal comprovação, uma vez que a Meta (organização que controle o WhatsApp) afirma ter implementada a criptografia ponta-a-ponta e que não possui acesso ao conteúdo das mensagens, conforme sua política de privacidade[234]. Seria necessário, como última alternativa, recorrer ao interlocutor, para que este disponibilize seu dispositivo para ser periciado, caso ainda possua as mensagens armazenadas em seu dispositivo.

Além disso, a infiltração encoberta virtual quase sempre estará acompanhada do monitoramento e vigilância não somente do suspeito (investigado), mas, também, de insuspeitos (ou não suspeitos), estes, em um número muito maior que o de suspeitos. Isso é dotado de certa obviedade: ao obter acesso ao dispositivo do investigado, obtém-se acesso ao seu “mundo” de dados estáticos e dinâmicos (em movimento). Arquivos, e-

[234] WhatsApp. **Política de Privacidade do WhatsApp**. Disponível em: https://www.whatsapp.com/legal/privacy-policy. Acesso em: 29 dez. 2024.

mails, mensagens, fotos, vídeos etc., o investigador não possui restrição prévia ao que terá acesso (como, por exemplo, restrição à interceptação telefônica e restrita às comunicações realizadas com terceiros conectados às suspeitas e investigações). Assim, possui acesso irrestrito em escopo (conteúdo) e tempo, já que também poderá acessar conteúdo existente desde sua criação, mesmo que tenha sido criado muito antes da autorização judicial para a intervenção no direito fundamental à privacidade e proteção de dados pessoais (investigação por meio de infiltração encoberta virtual).

A coleta massiva de dados (especialmente envolvendo insuspeitos) a partir de provedores de conteúdo tem recebido atenção por parte da comunidade de juristas e pesquisadores, especialmente em razão do caso do assassinato de uma vereadora do Rio de Janeiro, em que no âmbito das investigações foi determinada a quebra de sigilo de todas as pessoas que fizeram pesquisas relacionadas ao seu nome e à sua agenda nos dias anteriores ao crime.

A Justiça do Rio de Janeiro ordenou que o Google fornecesse, sem especificar quem seria objeto da busca, os endereços IP ou a identificação de aparelhos que realizaram pesquisa de alguns termos específicos. O Google, então, interpôs recurso e a relatora do caso, a Ministra Rosa Weber, elencou argumentos não admitindo tal fornecimento. O Recurso Especial 1.301.250 (RE 1301250) fixará o “Tema 1148” de título “Limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas”[235]. Heloisa Estellita e Orlandino Gleizer afirmam[236], sobre o caso e investigação penal que atinge insuspeitos por meio da coleta massiva de dados, que “os problemas da decisão não são a gravidade do crime e a importância do êxito da investigação, mas a falta de autorização democrática e o custo desproporcional da medida para essa finalidade”.

O termo utilizado para essa coleta massiva de dados nos Estados Unidos por meio de mandados de identificação de suspeitos indeterminados que tenham realizado

[235] Supremo Tribunal Federal. **Tema 1148**. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/tema.asp?num=1148. Acesso em: 29 dez. 2024.
[236] Folha de São Paulo. **A investigação penal de insuspeitos – STF fere direitos ao exigir coleta massiva de dados**. Disponível em: https://www1.folha.uol.com.br/opiniao/2020/09/a-investigacao-penal-de-insuspeitos.shtml. Acesso em: 29 dez. 2024.

pesquisa sobre determinadas palavras-chave ou que estiveram em algum local em particular em um período é *Dragnet Warrants* (Mandados de Arrasto, em tradução livre).

Segundo a União das Liberdades Civis de Nova York[237]:

> Esses mandados não podem ser direcionados ou específicos porque, por definição, eles dão às autoridades policiais o poder de obter registros privados sobre várias pessoas desconhecidas. Eles podem colocar centenas ou milhares de pessoas inocentes e insuspeitos na mira da aplicação da lei, ameaçando seus direitos de se livrar de buscas irracionais do governo.[238]

A regulamentação das atividades de infiltração encoberta virtual, monitoramento e vigilância online tem sido constantemente demandada não somente no Brasil (como por meio da ADPF 1143), mas também internacionalmente, como veremos no tópico a seguir.

5.5 A demanda internacional por adequada regulamentação

Conforme Marx (1988, p. 17):

> As práticas contemporâneas de infiltração podem ser mais bem compreendidas ao visualizá-las em um contexto histórico notando que fatores sociais, legais e técnicos os afetam. (...) Engano, tentação e informantes são formas antigas e praticamente universais de controle social.”[239].

Enquanto o estudo aprofundado do instituto de investigações encobertas não é o principal objetivo desta pesquisa, vale mencionar que a utilização sistemática e formal de meios encobertos para investigação de crimes convencionais tanto na Europa quanto nos Estados Unidos se deve muito ao francês François Vidocq (1775-1857) (Marx; 1988, p. 18). Sua história, de forma resumida, é a de que enquanto jovem, Vidocq foi preso por um crime de menor potencial ofensivo, escapou da prisão e procurou proteção contra policiais junto a criminosos. Entretanto, como parte do esforço para “limpar seu nome”,

---

[237] Tradução livre: New York Civilian Liberties Union.
[238] Tradução livre: These warrants can’t be targeted or specific because, by definition, they give law enforcement the power to obtain private records about numerous unknown people. They can place hundreds or thousands of unsuspecting and innocent people in the crosshairs of law enforcement, threatening their rights to be free from unreasonable government searches.
[239] Tradução livre: Contemporary undercover practices can be better understood by looking at them in a historical context and noting what social, legal, and technical factors affect them. (…) Deception, temptation, and informers are ancient and virtually universal forms of social control.

voltou voluntariamente para a prisão como um espião da própria polícia. Permaneceu ali por 21 meses e forneceu uma grande quantidade de informações valiosas às autoridades. Seu sucesso enquanto espião lhe rendeu o ingresso na polícia como agente e Vidocq estabeleceu uma unidade para investigação criminal na polícia de Paris. Foi líder da divisão de investigações criminais de 1810 até 1827. Sua grande inovação foi a de ter agentes policiais envolvidos diretamente no mundo criminal, já que acreditava que "o crime só pode ser lutado por criminosos" e que "é necessário um ladrão para capturar um ladrão". Entretanto, problemas eventualmente apareceram. Em algumas situações, distinguir entre policiais e criminosos era praticamente impossível, e o potencial para corrupção acabou por tornar o sistema de Vidocq vulnerável e suspeito (apesar de seu sucesso) (Marx, 1988, p. 18).

As mudanças ocorridas nos padrões criminais de tempos em tempos produzem direto impacto nas táticas investigativas policiais. De acordo com Gary Marx (1998, p. 37), houve uma mudança sensível nos padrões criminais e no seu enfrentamento nos Estados Unidos durante as décadas de 1960 e 1970, quanto aos crimes de rua e às novas e mais sofisticadas formas de crimes do "colarinho branco". Tais mudanças "contribuíram para uma expansão significativa nos recursos disponíveis para a aplicação da lei em geral e meios de infiltração em particular"[240].

Ao passo que uma grande quantidade de condutas criminosas migrou do espaço físico para o ciberespaço, naturalmente uma grande proporção de investigações criminais também o fez (Grabosky; Urbas, 2023, p. 128).

Assim, em 23 de novembro de 2001, o tratado chamado "Convenção sobre o Cibercrime" (ETS nº 285), também chamado de "Convenção de Budapeste" foi disponibilizado para assinaturas pelos Estados membros da União Europeia, bem como adesão de outros Estados não-membros[241]. À época da realização desta pesquisa, A

[240] Tradução livre: These changes in crime patterns and priorities contributed to a significant expansion in the resources available for law enforcement in general and undercover means in particular.
[241] Council of Europe. Details of Treaty nº 185. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185. Acesso em: 03 jan. 2025.

Convenção de Budapeste contava com 76 Estados-membros (incluindo o Brasil) e 20 países signatários e convidados para adesão[242].

Entretanto, em um movimento a fim de amplificar a adoção e complementar a Convenção de Budapeste sobre o Cibercrime[243], as Nações Unidas celebraram o "primeiro tratado criminal internacional em 20 anos"[244] de uma nova Convenção contra o Cibercrime[245], após uma negociação por 5 anos, tendo sido adotada em uma resolução ocorrida dia 24 de dezembro de 2024 em uma Assembleia Geral de 193 países. A Convenção contra o Cibercrime será aberta para assinaturas em uma cerimônia formal a ocorrer em Hanoi, Vietnã, em 2025, e adquirirá vigência 90 dias após ser ratificada pelo 40º país signatário.

Contudo, o que mudou entre os instrumentos, distantes 20 anos um do outro? De modo resumido, em termos de escopo, a Convenção de Budapeste foca primariamente em crimes específicos. A Convenção do Cibercrime das Nações Unidas possui mais amplo escopo, buscando a prevenção do cibercrime e cooperação internacional.

Há uma espécie de "modernização" nos termos utilizados pela Convenção do Cibercrime das Nações Unidas. Há utilização de termos "ICT" e "*ICT Systems*" (sistemas de tecnologia de informação e comunicação, em tradução livre) ao invés de "computador" ou "sistemas computadorizados". Essa adaptação da nomenclatura reflete a contemporaneidade, que é repleta de diferentes tipos de tecnologias e dispositivos informáticos, alguns inexistentes ou não tão presentes no cotidiano à época (como *Internet of Things* ou Internet das Coisas em tradução livre). Com o mesmo efeito, houve a substituição de "dados computadorizados" para "dados eletrônicos".

Quanto à criminalização, a Convenção do Cibercrime das Nações Unidas possui escopo mais amplo que a Convenção de Budapeste. Enquanto algumas condutas possuem tratamento semelhante nos dois instrumentos, a nova Convenção criminaliza

---

[242] Council of Europe. Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY. Disponível em: https://www.coe.int/en/web/cybercrime/parties-observers. Acesso em: 03 jan. 2025.
[243] European Comission. **Commission reached an agreement on the new international cybercrime convention.** Disponível em: https://home-affairs.ec.europa.eu/news/commission-reached-agreement-new-international-cybercrime-convention-2024-08-13_en. Acesso em: 03 jan. 2025.
[244] United Nations. **UN General Assembly adopts milestone cybercrime treaty**. Disponível em: https://news.un.org/en/story/2024/12/1158521. Acesso em: 25 dez. 2024.
[245] United Nations General Assembly. **A/79/460 – UN Cybercrime Convention**. Disponível em: https://documents.un.org/doc/undoc/gen/n24/372/04/pdf/n2437204.pdf. Acesso em: 03 jan. 2025.

novas condutas que vão além da literalidade "*cyber*", como, por exemplo, nos crimes de lavagem de dinheiro (m*oney laundering*) e na provisão contida em seu Artigo 15, relacionada ao abuso sexual de crianças (por meio de tecnologias de informação e comunicação – ICT).

Uma importante adição realizada na Convenção do Cibercrime das Nações Unidas foram as provisões de proteção às chamadas infraestruturas críticas (água, energia, gás, petróleo etc.). Estas provisões são inexistentes na Convenção de Budapeste.

As provisões da Convenção do Cibercrime das Nações Unidas relacionadas aos "poderes procedimentais"[246] foram duramente criticadas pela sociedade civil. Isto porque esta Convenção confere demasiada confiança em leis "domésticas", dos próprios países, para estabelecer como as medidas de proteção serão implementadas. Uma crítica comum a esse modelo adotado é a de que vários países (dentre os 193 países da Assembleia Geral das Nações Unidas) possuem baixos padrões protetivos quanto aos direitos humanos, especialmente a privacidade e liberdade de expressão (preocupação comum também com a Convenção de Budapeste). De certo modo, a cooperação internacional promovida por esta Convenção pode se tornar desafiadora quanto à conciliação das leis domésticas de tantos países.

Por fim, para efeitos de comparação entre as duas Convenções, a Convenção de Budapeste (incluindo seu segundo protocolo) aborda a cooperação internacional em evidências eletrônicas para qualquer crime, enquanto a Convenção do Cibercrime das Nações Unidas optou por limitar seu escopo de cooperação internacional apenas para o que definiu como "crimes sérios" (definidos no instrumento). Estes crimes são condutas puníveis com o mínimo de quatro anos de pena privativa de liberdade, ou uma penalidade mais séria. O que as Nações Unidas consideram como "penalidade mais séria" que a pena privativa de liberdade, o instrumento não esclarece.

Assim, os objetivos da Convenção contra o Cibercrime das Nações Unidas são "promover e fortalecer medidas para prevenir e combater o cibercrime eficientemente e efetivamente"[247] (Artigo 1-a), "promover, facilitar e fornecer a cooperação na prevenção

[246] Tradução livre: Procedural powers.
[247] Tradução livre: Promote and strengthen measures to prevent and combat cybercrime more efficiently and effectively.

e combate ao cibercrime”[248] (Artigo 1-b) e “promover, facilitar e fornecer assistência técnica e capacidade para prevenção e combate do cibercrime, em particular para o benefício de países em desenvolvimento”[249] (Artigo 1-c). Seu escopo de aplicação inclui a “prevenção, investigação e persecução de ofensas criminais estabelecidas de acordo com esta Convenção (...)”[250] (Artigo 3-a) e “a coleta, obtenção, preservação e compartilhamento de evidências na forma eletrônica para o propósito de investigações criminais ou procedimentos (...)[251] (Artigo 3-b).

A Convenção contra o Cibercrime possui diversas disposições sobre os crimes cibernéticos (ou informáticos) que merecem atenção por parte dos Estados signatários. Entretanto, quanto ao nosso objeto de estudo, no Capítulo IV (*Procedural measures and law enforcement* ou Medidas procedimentais e aplicação da lei, em tradução livre) estão as disposições sobre os “deveres” dos Estados signatários quanto às investigações criminais em ambientes de sistemas de tecnologia, ou informáticos.

No Artigo 23-1 encontramos a disposição que “cada Estado deve adotar medidas legislativas como forem necessárias para definirem os poderes e procedimentos para propósito de investigações ou procedimentos criminais específicos”[252].

Já no Artigo 24-1 (Condições e salvaguardas), há uma importante disposição:

> Cada Estado assegurará que o estabelecimento, a implementação e a aplicação dos poderes e procedimentos previstos no presente capítulo estejam sujeitos às condições e salvaguardas previstas no seu direito interno, que deverá assegurar a proteção dos direitos humanos, em conformidade com as suas obrigações nos termos do direito internacional dos direitos humanos, e que deverá incorporar o princípio da proporcionalidade.[253]

---

[248] Tradução livre: Promote, facilitate and strengthen international cooperation in preventing and combating cybercrime.
[249] Tradução livre: Promote, facilitate and support technical assistance and capacity-building to prevent and combat cybercrime, in particular for the benefit of developing countries.
[250] Tradução livre: The prevention, investigation and prosecution of the criminal offences established in accordance with this Convention (…).
[251] Tradução livre: The collecting, obtaining, preserving and sharing of evidence in electronic form for the purpose of criminal investigations or proceedings (…).
[252] Tradução livre: Each State Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this chapter for the purpose of specific criminal investigations or proceedings.
[253] Tradução livre: Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this chapter are subject to conditions and safeguards provided for under its domestic law, which shall provide for the protection of human rights, in accordance with its obligations under international human rights law, and which shall incorporate the principle of proportionality.

Quanto às medidas interventivas nos direitos fundamentais, como por exemplo a busca e apreensão de dados armazenados em formato eletrônico (Artigo 28), coleta em tempo real de dados em trânsito (Artigo 29) e interceptação de dados (Artigo 30), em todos os casos há a demanda pela Convenção do Cibercrime pela adoção dos Estados signatários de introduções legislativas a fim de fundamentar e regulamentar tais medidas.

A palavra "privacidade" (*privacy*) aparece somente duas vezes no texto da Convenção contra o Cibercrime. A única menção relevante é no preâmbulo, em que o Estado signatários afirmam "reconhecer o direito à proteção contra interferência arbitrária ou ilícita na privacidade individual, e a importância da proteção de dados pessoais"[254].

Ainda, no Artigo 36 (Proteção de dados pessoais), no parágrafo 1(a), há a disposição de que:

> Um Estado que transfira dados pessoais em conformidade com a presente Convenção deverá fazê-lo em conformidade com o seu direito interno e com quaisquer obrigações que a Parte que proceda à transferência possa ter ao abrigo do direito internacional aplicável. Os Estados não serão obrigados a transferir dados pessoais em conformidade com a presente Convenção se os dados não puderem ser fornecidos em conformidade com a legislação aplicável em matéria de proteção de dados pessoais.[255]

Por meio dos dispositivos da Convenção do Cibercrime citados, é possível concluir que os países-membros e signatários terão diversas obrigações legislativas de modo a fundamentar legalmente e regulamentar o tema da persecução penal contra o cibercrime, nisto inclusas as técnicas de investigação criminais que representem medidas interventivas em direitos humanos, em nosso objeto de estudo, o direito humano à privacidade e proteção de dados pessoais. Tais direitos, no caso brasileiro, constituem, como abordado nesta pesquisa, direitos fundamentais e, portanto, merecedores de adequado tratamento compatível com tal natureza jurídica.

---

[254] Tradução livre: Acknowledging the right to protection against arbitrary or unlawful interference with one's privacy, and the importance of protecting personal data.

[255] Tradução livre: A State Party transferring personal data pursuant to this Convention shall do so in accordance with its domestic law and any obligations the transferring Party may have under applicable international law. States Parties shall not be required to transfer personal data in accordance with this Convention if the data cannot be provided in compliance with their applicable laws concerning the protection of personal data.

No contexto alemão, que é o contexto internacional que mais nos interessa na realização desta pesquisa, segundo Greco e Gleizer (2019, p. 1488), “a possibilidade da infiltração estatal, oculta e remota, em dispositivos informáticos para a investigação de crimes começou a ser discutida pelos tribunais alemães por volta de 2006”. No ano de 2007, em um caso de investigação contra suspeitos pela criação de uma organização terrorista[256] (*Urteil vom 27. Februar 2008 - 1 BvR 370/07, 1 BvR 595/07 - BVerfGE 120, 274*), o Procurador-Geral da República alemã (*der Generalbundesanwalt*) solicitou ao juízo a autorização para realização de uma busca encoberta online (*Online-Durchsuchung*) no computador do suspeito, utilizando um programa para copiar e transferir arquivos para as autoridades investigativas.

O Tribunal alemão (*Bundesgerichtshof*) entendeu, de acordo com Greco e Gleizer (2019, p. 1489) que tal intervenção tão severa em direitos fundamentais de liberdade “precisaria estar amparada por uma *norma autorizativa específica*, que, para ser constitucionalmente compatível, precisaria também se atentar aos severos pressupostos de intervenção exigidos pelo direito fundamental em questão”. Não havia, portanto, fundamento legal para tal medida de infiltração encoberta online.

Nesta decisão do Tribunal houve o reconhecimento do direito fundamental à proteção da confidencialidade e integridade dos sistemas de tecnologia da informação (ou informáticos). Segundo o Tribunal:

> Esta manifestação do direito geral de personalidade merece proteção contra a infiltração de sistemas informáticos para a extensão que a proteção não é ainda garantida por outros direitos fundamentais (...), nem pelo direito à autodeterminação informacional.

Ainda que haja alguma intervenção autorizada em tais sistemas, deve haver medidas de proteção (salvaguardas) para que não haja interferência no núcleo da vida privada (*Kernbereich privater Lebensgestaltung*) (ou núcleo da esfera privada, de acordo com a teoria das esferas de Hubmann, tópico que abordaremos apropriadamente), que goza de proteção absoluta. Isto porque, de acordo com a fundamentação do Tribunal:

---

[256] BVerfG, Urteil des Ersten Senats vom 27. Februar 2008 - 1 BvR 370/07 -, Rn. 1-333, https://www.bverfg.de/e/rs20080227_1bvr037007.

> No contexto do acesso encoberto a um sistema de tecnologia da informação, existe o risco de que a autoridade estatal em exercício colete dados pessoais que possam ser atribuídos ao núcleo da vida privada. Esse é o caso, por exemplo, quando a pessoa em questão usa o sistema para criar e armazenar arquivos com conteúdo altamente pessoal, como anotações semelhantes a diários ou arquivos privados de vídeo ou som. Esses arquivos podem gozar de proteção absoluta, assim como, entre outros, relatos escritos de experiências altamente pessoais.[257]

A extensão do que compreende este "núcleo da esfera privada" é tema controverso. Entretanto, conforme Greco e Gleizer (2019, p. 1496), "a princípio, o BVerfG nega que uma informação pertença ao núcleo da vida privada, caso ela tenha alguma relação imediata com crimes".

Assim, em julho de 2017, o legislador introduziu no Código de Processo Penal alemão a disposição contida no § 100b (*Strafprozeßordnung § 100b Online-Durchsuchung*[258]), que autoriza a infiltração encoberta online com base em determinadas exigências.

As exigências para que a medida de infiltração online (*Online-Durchsuchung*) seja lícita estão dispostas no *Strafprozeßordnung § 100b* em diante. Para que haja tal intervenção, os crimes devem constar em uma lista de crimes especialmente graves[259], disposta no § 100b Abs. 2 e a investigação dos fatos deve ser significativamente mais difícil ou impossível de outra maneira (§ 100b Abs. 1 Nr. 3).

A afetação de não investigados deve ser a exceção do procedimento, ou seja, a medida deve ser dirigida somente ao investigado (§ 100b Abs. 3), sendo admitida a afetação de outras pessoas somente se inevitável. O § 100b Abs. 4 menciona que os parágrafos 5 (com exceção do Abs. 5 Nr. 1) e 6 da seção § 100ª são aplicáveis à infiltração online, ou seja, somente os dispositivos de tecnologia da informação que sejam essenciais para a investigação poderão ser objeto da medida e o registro da cadeia de custódia dos dados levantados (identificação da técnica utilizada, do sistema informático,

---

[257] Tradução livre: Im Rahmen eines heimlichen Zugriffs auf ein informationstechnisches System besteht die Gefahr, dass die handelnde staatliche Stelle persönliche Daten erhebt, die dem Kernbereich zuzuordnen sind. So kann der Betroffene das System dazu nutzen, Dateien höchstpersönlichen Inhalts, etwa tagebuchartige Aufzeichnungen oder private Film- oder Tondokumente, anzulegen und zu speichern. Derartige Dateien können ebenso wie etwa schriftliche Verkörperungen des höchstpersönlichen Erlebens.

[258] Bundesministerium der Justiz. **Strafprozeßordnung (StPO) § 100b Online-Durchsuchung**. Disponível em: https://www.gesetze-im-internet.de/stpo/__100b.html. Acesso em: 02 jan. 2025.

[259] Tradução livre: Besonders schwere Straftaten.

as modificações realizadas, os dados coletados, quem executou a medida) deve ser cuidadosamente preparada.

O § 100d do *Strafprozeßordnung* (StPO) alemão dispõe sobre a proteção à área nuclear da esfera (ou vida) privada[260]. Desse modo, em todas as ocasiões que a medida obtiver qualquer informação que seja próprio dessa área nuclear, estes registros devem ser eliminados imediatamente e sua exclusão documentada (§ 100d Abs. 2).

O grande desafio aqui é precisamente proteger esse núcleo central da esfera privada, primeiro porque sua delimitação permanece uma incógnita até os dias atuais (além de serem mutáveis, conforme o conceito de privacidade que consideramos mais apropriado nesta pesquisa) e, segundo, porque a separação técnica do que se pode obter e o que não é admitida a obtenção é tarefa extremamente difícil de ser realizada *a priori* da execução da medida, conforme concorda Gleizer (Greco; Gleizer, 2019, p. 1505). Neste caso, idealmente, a medida deveria ser autorizada pelo juízo unicamente caso a autoridade investigativa pudesse demonstrar com o máximo grau de certeza ou probabilidade que os dados objetos da medida interventiva seriam obtidos sem "tocar" dados constitutivos da área nuclear da esfera privada do indivíduo.

5.6 A inteligência artificial aplicada ao contexto dos crimes cibernéticos

De acordo com o *Collins English Dictionary*[261], inteligência artificial é "um tipo de tecnologia de computador que se dedica a fazer máquinas trabalharem em um modo inteligente, similar ao modo que a mente humana trabalha"[262]. De acordo com Russel e Norvig (2020, p. 1), pesquisadores têm buscado diversas versões diferentes de IA (Inteligência Artificial): "alguns definiram inteligência em termos de fidelidade ao desempenho *humano* [grifo do autor], enquanto outros preferem uma definição formal, abstrata, de inteligência chamada **racionalidade** – algo como fazer a "coisa certa"[263].

---

[260] Tradução livre: Kernbereich privater Lebensgestaltung.
[261] Collins. **Artificial Intelligence**. Disponível em: https://www.collinsdictionary.com/dictionary/english/artificial-intelligence. Acesso em: 22 dez. 2024.
[262] Tradução livre: Artificial intelligence is a type of computer technology which is concerned with making machines work in an intelligent way, similar to the way that the human mind works.
[263] Tradução livre: Some have defined intelligence in terms of fidelity to human performance, while others prefer an abstract, formal definition of intelligence called rationality - loosely speaking, doing the "right thing".

Ainda, alguns consideram inteligência ser “uma propriedade de processos internos de pensamento e razão, enquanto outros foram em comportamento inteligente, uma caracterização externa”[264].

O famoso matemático e professor Alan Turing propôs, já em 1950, um teste, chamado “Teste de Turing” em uma forma experimental que responderia a vaga e filosófica questão “pode uma máquina pensar?” (Russel; Norvig, 2020, p. 1). Um computador passaria o teste caso um interrogador humano, após propor algumas questões escritas, não pudesse dizer se as respostas escritas vieram de uma pessoa ou de um computador. O computador teria que ter as seguintes capacidades, como ensina Russel e Norvig (2020, p. 1): processamento de linguagem natural; representação do conhecimento; automatizada obtenção de conclusões; e aprendizado de máquina[265].

Outros pesquisadores propuseram, segundo Russel e Norvig (2020, p. 1), um teste total de Turing, que demandaria interação com objetos e pessoas no mundo real, utilizando “visão computadorizada e reconhecimento de fala” e “robótica” para manipular objetos. Estas seis disciplinas compõem a maior parte da inteligência artificial.

O aprendizado de máquina (*Machine Learning*), de acordo com o *Collins English Dictionary*[266] é definido como “um ramo da inteligência artificial onde um computador gera regras baseadas em dados brutos pelos quais foi alimentado”[267]. Russel e Norvig (2020, p. 651) afirmam que em aprendizado de máquina “um computador observa alguns dados, constrói um **modelo** baseado nestes dados, e usa o modelo tanto como uma **hipótese** sobre o mundo e como uma peça de software que pode resolver problemas [grifos do autor]”[268].

Os três principais tipos de aprendizado, segundo Russel e Norvig (2020, p. 653) são: aprendizado supervisionado, aprendizado não-supervisionado, aprendizado de

---

[264] Tradução livre: Some consider intelligence to be a property of internal thought processes and reasoning, while others focus on intelligent behavior, an external characterization.
[265] Tradução livre: Natural language processing; knowledge representation; automated reasoning; machine learning.
[266] Collins. **Machine learning**. Disponível em: https://www.collinsdictionary.com/dictionary/english/machine-learning. Acesso em: 22 dez. 2024.
[267] Tradução livre: a branch of artificial intelligence in which a computer generates rules underlying or based on raw data that has been fed into it.
[268] Tradução livre: a computer observes some data, builds a model based on the Machine learning data, and uses the model as both a hypothesis about the world and a piece of software that can solve problems.

reforço[269]. No aprendizado supervisionado, o agente observa pares de entrada e saída e aprende uma função que mapeia da entrada para a saída. No aprendizado não-supervisionado, o agente aprende padrões na entrada sem nenhum *feedback* explícito. No aprendizado por reforço, o agente aprende a partir de séries de reforços: premiações e punições.

O aprendizado profundo (*Deep Learning*), de acordo com Russel e Norvig (2020, p. 750) é "uma ampla família de técnicas para aprendizado de máquina nas quais hipóteses tomam a forma de circuitos algébricos complexos com forças ajustáveis de conexão"[270]. A palavra "profundo" se refere aos circuitos que são tipicamente organizados em diversas camadas. Suas raízes estão em um trabalho que tentou modelar redes de neurônios no cérebro (McCulloch e Pitts em 1943) com circuitos computacionais, por isso, essas redes são comumente chamadas de redes neurais.

Entretanto, a grande "sensação" atual se chama "Inteligência Artificial Generativa"[271], ou *GenAI*. A *GenAI* nada mais é que um salto dos modelos anteriores, onde era possível reconhecer padrões, realizar estimativas numéricas etc., para modelos que podem "criar" (ou gerar) novos dados. Assim, modelos de *GenAI* podem superar respostas matemáticas e criar conteúdo, como compor músicas, pintar ou desenhar uma cena imaginária, escrever um poema, ou criar uma aplicação web. Portanto, contextualizando o tema para nossa pesquisa, uma *GenAI* poderia, por exemplo, criar uma aplicação web destinada a superar mecanismos gerais e específicos de segurança da informação implementados em outras aplicações web de qualquer natureza: militar, infraestruturas críticas (gás, água, energia, petróleo etc.), finanças, saúde... a lista é extensa e, a depender de quem analisa, pode se tornar cada vez mais dramática.

Inúmeros cenários são imaginados para o futuro da inteligência artificial no mundo. Cenário positivos, de cooperação homem-máquina (como preconiza a sociedade 5.0 que já abordamos nesse estudo), de favorecimento ao humano e suas necessidades. Por outro lado, há sempre o temor de cenários negativos, como a redução insustentável dos postos de trabalho no mundo, extinção de profissões (de custo ou razão injustificáveis

[269] Tradução livre: supervised learning, unsupervised learning, reinforcement learning.
[270] Tradução livre: Deep learning is a broad family of techniques for machine learning Deep learning in which hypotheses take the form of complex algebraic circuits with tunable connection strengths.
[271] Tradução livre: Generative Artificial Intelligence.

frente à relação eficiência-custo da inteligência artificial “popularizada”, ou até mesmo a extinção humana na eventualidade da chamada “singularidade” e utilização de armas autônomas baseadas em inteligência artificial avançada.

Kai-Fu Lee a Chen Qiufan (2021), notórios pesquisadores no tema de inteligência artificial, escreveram um livro chamado “*AI 2041: ten visions for our future*” (IA 2041: dez visões para nosso futuro, em tradução livre) onde diversos cenários para a inteligência artificial são imaginados, dentre eles, o chamado “genocídio quântico” (tradução livre de *quantum genocide*), em que a computação quântica é utilizada para a criação de armas autônomas baseadas na inteligência artificial existente à época, provocando uma ameaça existencial à humanidade.

Em resumo, *GenAI* (Inteligência Artificial Generativa) está dentro do campo de Deep Learning (Aprendizado Profundo), que está dentro do campo de Machine Learning (Aprendizado de Máquina), que por sua vez está dentro do universo de Inteligência Artificial.

Uma das características mais distintivas da inteligência artificial (quando comparada às mesmas atividades realizadas por humanos) é a velocidade de obtenção dos resultados. É evidente que a tecnologia computadorizada é quase “infinitamente” mais veloz na obtenção de obtenção de resultados oriundos de suas operações, disparidade que será absurdamente maior quando considerado o poder computacional da tecnologia quântica, ainda em desenvolvimento.

Enquanto uma abordagem aprofundada em toda a temática da Inteligência Artificial não é o objeto de estudo deste trabalho, serão abordados alguns tópicos de especial relevância para nossa pesquisa.

5.6.1 A inteligência artificial como forma preditiva em Direito Penal

Um dos apelos mais comuns quando se fala em Inteligência Artificial é a combinação entre algoritmos preditivos de tendências com os aspectos criminais. Ao

melhor estilo *Minority Report*[272], o ideal contido na prevenção de crimes antes que aconteçam permanece, até o momento, apenas no imaginário.

Apesar disso, pesquisadores se empenham em buscar algoritmos e dados que os alimentem de modo que haja resultados eficientes e comprováveis. Uma equipe de pesquisadores da Universidade de Chicago[273] afirma ter desenvolvido um "um novo modelo de computador que usa dados disponíveis publicamente para prever crimes com precisão em oito cidades dos EUA, ao mesmo tempo em que revela o aumento da resposta policial em bairros ricos às custas de áreas menos favorecidas"[274]. Segundo os dados publicados em um artigo na revista *Nature Human Behaviour*[275], a equipe de pesquisadores liderada por Ishanu Chattopadhyay apresentou "algoritmo de inferência estocástica que prevê o crime aprendendo dependências espaço-temporais a partir de relatórios de eventos, com uma área média sob a curva característica de operação do receptor de aproximadamente 90% em Chicago para crimes previstos por semana dentro de aproximadamente 1.000 pés"[276]. Para isso, "a equipe analisou registros históricos de três a cinco anos do passado. A partir disso, padrões foram desenvolvidos em um modelo desenhado para prever eventos futuros"[277] [278]. Apesar de Chattopadhyay afirmar que "não foca em previsão de comportamento individual, e não sugere que alguém seja acusado por um crime que não cometeu, ou seja encarcerado por isso"[279], a verdade é que inúmeros estudos já demonstraram o enviesamento de tais tecnologias que são, no

---

[272] History of Information. **"Minority Report": The Movie**. Disponível em: https://www.historyofinformation.com/detail.php?id=2146. Acesso em: 04 jan. 2025.
[273] The University of Chicago. **Algorithm predicts crime a week in advance, but reveals bias in police response**. Disponível em: https://biologicalsciences.uchicago.edu/news/algorithm-predicts-crime-police-bias. Acesso em: 04 jan. 2025.
[274] Tradução livre: A new computer model uses publicly available data to predict crime accurately in eight U.S. cities, while revealing increased police response in wealthy neighborhoods at the expense of less advantaged areas.
[275] Nature Human Behaviour. **Event-level prediction of urban crime reveals a signature of enforcement bias in US cities.** Disponível em: https://www.nature.com/articles/s41562-022-01372-0. Acesso em: 04 jan. 2025.
[276] Tradução livre: stochastic inference algorithm that forecasts crime by learning spatio-temporal dependencies from event reports, with a mean area under the receiver operating characteristic curve of ~90% in Chicago for crimes predicted per week within ~1,000 ft.
[277] Tradução livre: The team analyzed historical logs going back between three and five years. From there, predictive patterns were assembled into a model designed to predict future events.
[278] Wired. **AI can now predict crime before it happens.** Disponível em: https://wired.me/technology/ai-can-now-predict-crime-before-it-happens. Acesso em: 04 jan. 2025.
[279] Tradução livre: We do not focus on predicting individual behavior, and do not suggest that anyone be charged with a crime that they didn't commit, or be incarcerated for that.

fim das contas, alimentadas por dados e humanos que possuem seus próprios enviesamentos.

Por um lado, há estudos que afirmam que a disparidade da classificação de risco entre réus negros e brancos existe, entretanto não é atribuível a enviesamento, como o artigo publicado em 2016 por Skeem e Lowenkamp, em que afirmam (2016, p. 37) que "à luz de nossos resultados, parece que preocupações manifestadas sobre avaliação de risco são exageradas".

Por outro lado, em 2019, por exemplo, a polícia de Los Angeles, EUA, pôs fim em seu programa de policiamento preditivo LASER (*Los Angeles' Strategic Extraction and Restoration* ou Extração e Restauração Estratégica de Los Angeles, em tradução livre) por meio de dados em razão de preocupações sobre indicação injusta das comunidades negra e latina[280].

Tentativas para previsão de reincidência criminosa também têm sido realizadas usando sistemas e algoritmos de classificação de réus e detentos em diferentes graus de "risco". Um dos mais famosos no mundo, o estadunidense COMPAS (*Correctional Offender Management Profiling for Alternative Sanctions* ou Gestor de Perfilamento Correcional de Infratores para Sanções Alternativas, em tradução livre), foi severamente criticado por seus resultados em que réus negros tinham muito maior probabilidade de classificação incorreta de reincidência, enquanto réus brancos possuíam probabilidade muito maior de serem classificados como baixo risco de reincidência[281].

5.6.2 Análise de dados com manutenção da privacidade

A Lei de Execução Penal (Lei nº 7.210/1984) foi modificada pela Lei nº 10.792/2003 de modo que a inclusão no regime disciplinar diferenciado passou a constar nas opções de sanções disciplinares dispostas em seu Art. 53.

De acordo com o Art. 52 da lei:

---

[280] Los Angeles Times. **LAPD ends another data-driven crime program touted to target violent offenders.** Disponível em: https://www.latimes.com/local/lanow/la-me-laser-lapd-crime-data-program-20190412-story.html. Acesso em: 04 jan. 2025.

[281] Propublica. **How We Analyzed the COMPAS Recidivism Algorithm.** Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. Acesso em: 04 jan. 2025.

Art. 52. A prática de fato previsto como crime doloso constitui falta grave e, quando ocasionar subversão da ordem ou disciplina internas, sujeitará o preso provisório, ou condenado, nacional ou estrangeiro, sem prejuízo da sanção penal, ao regime disciplinar diferenciado, com as seguintes características:
I - duração máxima de até 2 (dois) anos, sem prejuízo de repetição da sanção por nova falta grave de mesma espécie;
II - recolhimento em cela individual;
III - visitas quinzenais, de 2 (duas) pessoas por vez, a serem realizadas em instalações equipadas para impedir o contato físico e a passagem de objetos, por pessoa da família ou, no caso de terceiro, autorizado judicialmente, com duração de 2 (duas) horas;
IV - direito do preso à saída da cela por 2 (duas) horas diárias para banho de sol, em grupos de até 4 (quatro) presos, desde que não haja contato com presos do mesmo grupo criminoso;
V - entrevistas sempre monitoradas, exceto aquelas com seu defensor, em instalações equipadas para impedir o contato físico e a passagem de objetos, salvo expressa autorização judicial em contrário;
VI - fiscalização do conteúdo da correspondência;
VII - participação em audiências judiciais preferencialmente por videoconferência, garantindo-se a participação do defensor no mesmo ambiente do preso.
§ 1º O regime disciplinar diferenciado também será aplicado aos presos provisórios ou condenados, nacionais ou estrangeiros:
I - que apresentem alto risco para a ordem e a segurança do estabelecimento penal ou da sociedade;
II - sob os quais recaiam fundadas suspeitas de envolvimento ou participação, a qualquer título, em organização criminosa, associação criminosa ou milícia privada, independentemente da prática de falta grave.
§ 2º (Revogado).
§ 3º Existindo indícios de que o preso exerce liderança em organização criminosa, associação criminosa ou milícia privada, ou que tenha atuação criminosa em 2 (dois) ou mais Estados da Federação, o regime disciplinar diferenciado será obrigatoriamente cumprido em estabelecimento prisional federal.
§ 4º Na hipótese dos parágrafos anteriores, o regime disciplinar diferenciado poderá ser prorrogado sucessivamente, por períodos de 1 (um) ano, existindo indícios de que o preso:
I - continua apresentando alto risco para a ordem e a segurança do estabelecimento penal de origem ou da sociedade;
II - mantém os vínculos com organização criminosa, associação criminosa ou milícia privada, considerados também o perfil criminal e a função desempenhada por ele no grupo criminoso, a operação duradoura do grupo, a superveniência de novos processos criminais e os resultados do tratamento penitenciário.
§ 5º Na hipótese prevista no § 3º deste artigo, o regime disciplinar diferenciado deverá contar com alta segurança interna e externa, principalmente no que diz respeito à necessidade de se evitar contato do preso com membros de sua organização criminosa, associação criminosa ou milícia privada, ou de grupos rivais.
§ 6º A visita de que trata o inciso III do caput deste artigo será gravada em sistema de áudio ou de áudio e vídeo e, com autorização judicial, fiscalizada por agente penitenciário.
§ 7º Após os primeiros 6 (seis) meses de regime disciplinar diferenciado, o preso que não receber a visita de que trata o inciso III do caput deste artigo poderá, após prévio agendamento, ter contato telefônico, que será gravado, com uma pessoa da família, 2 (duas) vezes por mês e por 10 (dez) minutos.

A Lei nº 13.964/2019 modificou, portanto, a Lei de Execução Penal para incluir a medida de “fiscalização do conteúdo da correspondência” do indivíduo preso (Art. 52, VI), sendo que mesmo os presos provisórios sob os quais “recaiam fundadas suspeitas de envolvimento ou participação, a qualquer título, em organização criminosa, associação criminosa ou milícia privada, independentemente da prática de falta grave” (Art. 52, § 1º, II) serão submetidos ao regime disciplinar diferenciado.

Aparentemente o legislador buscou endurecer o cumprimento de pena de indivíduos que tenham qualquer vínculo (confirmado ou com fundada suspeita) com organizações criminosas, associações criminosas ou milícias privadas.

A fiscalização do conteúdo da correspondência do preso representa medida “gravosa” a ser imposta, uma vez que suas comunicações com qualquer pessoa (incluindo filhos, pais, cônjuge, entes familiares) serão objeto de inspeção por parte da autoridade da execução penal.

O raciocínio imediato conduz à conclusão de que o preso que se “qualifique” ao cumprimento de regime disciplinar diferenciado poderá tentar comunicar conteúdo ilícito com qualquer pessoa no mundo exterior. Instruções indevidas, reprimendas, ordens de castigo ou execução de inimigos, ocultação ou destruição de elementos de prova, chantagens, coação de testemunhas, gestão de organizações criminosas, continuidade delitiva, solicitações para introduzir artigos proibidos na prisão etc., essas são algumas das situações que se busca prevenir e que justificariam a fiscalização da correspondência do preso.

Entretanto, a imposição de tal redução da proteção da privacidade do preso tem enorme potencial para atingir a chamada “área nuclear da esfera privada” destes indivíduos, de tal modo que esta fiscalização impeça qualquer comunicação espontânea entre o indivíduo preso com seus entes queridos, livre que qualquer sensação permanente de vigilância de “estranhos” e de privação deste direito mínimo de privacidade que ainda lhe resta.

Nesta ponderação entre o respeito ao direito (humano e fundamental) de privacidade e intimidade do preso e o interesse público na manutenção da segurança e combate à criminalidade, tais escolhas acabam invariavelmente recaindo na manutenção

do interesse público, ou seja, impõem-se múltiplas e cumulativas penas ao indivíduo preso (que não somente a sua privação de liberdade), tornando seu completo isolamento social um castigo que afeta não somente o indivíduo preso, mas também seus entes queridos com os quais tinha eventual vida familiar e que, certamente, poderia representar um incentivo na busca por reintegração social ao final do cumprimento de sua pena.

Neste sentido, sistemas de inteligência artificial poderiam auxiliar removendo o elemento de vigilância humana do procedimento, contando apenas com uma espécie de curadoria para os casos que "disparem" um alarme quanto ao conteúdo da comunicação realizada entre o preso e um indivíduo externo à penitenciária.

Os algoritmos de inteligência artificial seriam, então, treinados, alimentados com dados de prévias descobertas realizadas por ocasião de fiscalização do conteúdo de correspondência e outros novos dados de modo que o algoritmo de tal sistema possa identificar padrões que indiquem uma potencial violação da licitude da comunicação: códigos escritos embutidos que representem informações diversas da que se pretende aparentar, ou seja, qualquer uma das situações indicadas previamente que se pretenda prevenir com o uso dessa medida de fiscalização.

A comunicação do preso poderia, ainda, se estender para o ambiente virtual: um ambiente eletrônico inteiramente controlado e restrito pela autoridade estatal, monitorado por tais sistemas de inteligência artificial, com a preservação da privacidade do apenado. Essa é uma questão que o Estado ainda não enfrentou na execução penal: se caminhamos a passos largos para a sociedade 5.0, por que exigir que a execução penal se assemelhe em (quase) tudo ao período medieval? Se se pretende reintegração (ou ressocialização) do preso, por qual razão há interesse em apartá-lo de qualquer aparato tecnológico que era presente em seu dia a dia antes da sua condenação (desde que, claro, não represente a continuidade delitiva ou ameaça à própria execução penal)? Por que livros disponibilizados para leitura ainda são em formato físico (e com acervo extremamente limitado nos estabelecimentos de cumprimento penal), sendo que bibliotecas virtuais representariam conteúdo muito mais amplo e acessível? Estas são algumas das perguntas que uma mínima reflexão traz.

5.6.3 A regulamentação da Inteligência Artificial no Brasil e no mundo

A regulamentação do tema da Inteligência Artificial tem sido demandada em todo o mundo. As Nações Unidas (2024, p. 11), em seu relatório final de setembro de 2024 sobre governança de Inteligência Artificial (*Governing AI for Humanity* ou Governando a IA para a Humanidade, em tradução livre), indicou que "há, hoje, um déficit de governança global com respeito à IA"[282] e que "o imperativo de governança global, em particular, é irrefutável"[283].

Este relatório produzido pelas Nações Unidas concluiu, por meio de pesquisa realizada com 348 *experts* em Inteligência Artificial e 68 países em todas as regiões (2024, p. 28), que 67% dos entrevistados estão preocupados (pontuação 4 de 5) ou muito preocupados (pontuação 5 de 5) com riscos de utilização de Inteligência Artificial enviesada em decisões judiciais em âmbito criminal (tema que já abordamos em nossa pesquisa), 61% dos entrevistados estão preocupados ou muito preocupados com risco de violações à direitos humanos com o uso da Inteligência Artificial e 65% dos entrevistados estão preocupados ou muito preocupados com o risco de utilização intencional de Inteligência Artificial por agentes estatais que cause dano a indivíduos como, por exemplo, na vigilância em massa. Dentre os riscos listados no relatório, vale mencionar que a preocupação com o risco de dano à integridade informacional pelo uso de Inteligência Artificial (desinformação e *impersonation*) e risco de utilização de Inteligência Artificial em conflitos armados entre Estados (armas autônomas) lideram o ranking.

Curiosamente, a preocupação com o risco de violação a direitos autorais, risco de danos ambientais (consumo de energia acelerado e emissões de carbono, risco de danos ao (mercado de) trabalho oriundos da adoção da Inteligência Artificial e risco de ações não desejadas realizadas por sistemas autônomos de Inteligência Artificial se encontram com percentual bem menor que os listados acima.

Preocupante é, também, a constatação que as iniciativas inter-regionais em governança de Inteligência Artificial que não sejam das Nações Unidas estejam

[282] Tradução livre: There is, today, a global governance deficit with respect to AI.
[283] Tradução livre: The imperative of global governance, in particular, is irrefutable.

concentradas majoritariamente em sete países (Canadá, França, Alemanha, Itália, Japão, Reino Unido e os Estados Unidos são Parte em todas as iniciativas listadas), enquanto 118 países (primariamente no chamado Sul Global) não possuem participação em nenhuma iniciativa (2024, p. 42).

A União Europeia deu um passo muito importante nesta regulamentação, promulgando seu "*AI Act*" (*Regulation* 2024/1689) em 1º de agosto de 2024[284], que servirá, assim como ocorreu com o Regulamento Geral de Proteção de Dados europeu (GDPR – *General Data Protection Regulation*), de referência para a elaboração legislativa para o mundo.

O *Framework* regulatório europeu adotou (assim como em seu regulamento de proteção de dados pessoais) uma abordagem baseada em risco, sendo que 4 níveis de risco para sistemas de Inteligência Artificial foram definidos: risco mínimo, risco limitado, alto risco e risco inaceitável[285]. No que diz respeito ao nosso objeto de pesquisa, o *AI Act* definiu sistemas de "aplicação da lei que possam interferir em direitos fundamentais de indivíduos"[286] como sistemas de alto risco e, consequentemente, sujeitos a obrigações estritas antes que possam ser disponibilizadas no mercado.

Ainda, de acordo com o *AI Act*, todos os sistemas biométricos de identificação remota são considerados de alto risco e, portanto, sujeitos a obrigações estritas e a utilização de identificação biométrica remota em locais acessíveis publicamente para propósitos de aplicação da lei é, em princípio, proibida[287]. Entretanto, algumas exceções são autorizadas, desde que estritamente definidas e regulamentadas, tais quando necessárias para, dentre algumas opções existentes, identificar e perseguir um criminoso ou suspeito de ofensas criminais sérias, dispostas no Anexo II do regulamento.

O *AI Act*, em seu recital 42, dispõe que:

> Em consonância com a presunção de inocência, pessoas físicas na União devem sempre ser julgadas com base em seu comportamento real. Pessoas físicas

[284] European Comission. **AI Act enters into force**. Disponível em: https://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en. Acesso em: 05 jan. 2025.
[285] European Comission. **AI Act**. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. Acesso em: 05 jan. 2025.
[286] Tradução livre: law enforcement that may interfere with people's fundamental rights.
[287] Tradução livre: All remote biometric identification systems are considered high-risk and subject to strict requirements. The use of remote biometric identification in publicly accessible spaces for law enforcement purposes is, in principle, prohibited.

> nunca devem ser julgadas com base em comportamento previsto por IA com base apenas em seu perfil, traços de personalidade ou características, como nacionalidade, local de nascimento, local de residência, número de filhos, nível de dívida ou tipo de carro, sem uma suspeita razoável de que essa pessoa esteja envolvida em uma atividade criminosa com base em fatos objetivos verificáveis e sem avaliação humana dos mesmos. **Portanto, avaliações de risco realizadas com relação a pessoas físicas para avaliar a probabilidade de sua infração ou para prever a ocorrência de uma infração criminal real ou potencial com base apenas em seu perfil ou na avaliação de seus traços de personalidade e características devem ser proibidas** [grifo nosso]. Em qualquer caso, essa proibição não se refere nem aborda análises de risco que não sejam baseadas no perfil de indivíduos ou nos traços de personalidade e características de indivíduos, como sistemas de IA que usam análises de risco para avaliar a probabilidade de fraude financeira por empresas com base em transações suspeitas ou ferramentas de análise de risco para prever a probabilidade de localização de narcóticos ou mercadorias ilícitas por autoridades alfandegárias, por exemplo, com base em rotas de tráfico conhecidas.[288]

Esta proibição explicada pelo recital 42 se encontra expressamente disposta no Artigo 5 do *AI Act*:

> As seguintes práticas de IA devem ser proibidas:
> (...)
> d) A colocação no mercado, a disponibilização de serviço para este fim específico ou a utilização de um sistema de IA para efetuar avaliações de risco de pessoas naturais, a fim de avaliar ou prever o risco de uma pessoa natural cometer uma infração penal, com base exclusivamente na definição de perfis de uma pessoa natural ou na avaliação dos seus traços e características de personalidade; esta proibição não se aplica aos sistemas de IA utilizados para apoiar a avaliação humana do envolvimento de uma pessoa numa atividade criminosa, que já se baseia em fatos objetivos e verificáveis diretamente ligados a uma atividade criminosa.[289]

---

[288] Tradução livre: In line with the presumption of innocence, natural persons in the Union should always be judged on their actual behaviour. Natural persons should never be judged on AI-predicted behaviour based solely on their profiling, personality traits or characteristics, such as nationality, place of birth, place of residence, number of children, level of debt or type of car, without a reasonable suspicion of that person being involved in a criminal activity based on objective verifiable facts and without human assessment thereof. Therefore, risk assessments carried out with regard to natural persons in order to assess the likelihood of their offending or to predict the occurrence of an actual or potential criminal offence based solely on profiling them or on assessing their personality traits and characteristics should be prohibited. In any case, that prohibition does not refer to or touch upon risk analytics that are not based on the profiling of individuals or on the personality traits and characteristics of individuals, such as AI systems using risk analytics to assess the likelihood of financial fraud by undertakings on the basis of suspicious transactions or risk analytic tools to predict the likelihood of the localisation of narcotics or illicit goods by customs authorities, for example on the basis of known trafficking routes.

[289] Tradução livre: The following AI practices shall be prohibited: (...) (d) the placing on the market, the putting into service for this specific purpose, or the use of an AI system for making risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics; this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity.

Portanto, as atividades preditivas de sistemas de policiamento baseadas em algoritmos de Inteligência Artificial são, dentro do escopo de aplicação do *AI Act*, proibidos.

No Brasil, o tema da regulamentação da utilização de Inteligência Artificial, à época desta pesquisa, teve o texto aprovado pelo Senado Federal[290], como substitutivo ao Projeto de Lei 2.338/2023 (PL 2.328/2023).

No texto aprovado, apesar de ainda suscetível a modificações até sua aprovação final, foram classificados como sistemas de Inteligência Artificial de alto risco e, portanto, sujeitos a regras mais rígidas, os sistemas que vierem a ser utilizados em atividades de "análise de dados para prevenção da ocorrência de crimes", "estudo analítico de crimes" e "investigação de fatos e aplicação da lei quando houver riscos às liberdades individuais, no âmbito da administração da Justiça", em moldes semelhantes ao observado no *AI Act* europeu.

Ainda, segundo o texto aprovado, a Autoridade Nacional de Proteção de Dados (ANPD) será estabelecida como a autoridade competente para imposição de sanções, regulamentar, investigar e fiscalizar questões relacionadas à utilização de sistemas de Inteligência Artificial, coordenando o SIA (Sistema Nacional de Regulação e Governança de Inteligência Artificial) e o CRIA (Conselho de Cooperação Regulatória de Inteligência Artificial) após a sua criação.

Ainda, segundo o texto aprovado, em seu Art. 13, I, c, são vedados o desenvolvimento e implementação de sistemas de Inteligência Artificial com o propósito de "avaliar os traços de personalidade, as características ou o comportamento passado, criminal ou não, de pessoas singulares ou grupos, para avaliação de risco de cometimento de crimes, de infrações ou de reincidência".

Entretanto, no Art. 14, IX, do texto aprovado, há autorização para utilização de sistema de Inteligência Artificial para "estudo analítico de crimes relativos a pessoas naturais, permitindo às autoridades policiais pesquisarem grandes conjuntos de dados, disponíveis em diferentes fontes de dados ou em diferentes formatos, no intuito de

[290] Senado Notícias. **Senado aprova regulamentação da inteligência artificial; texto vai à Câmara**. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/12/10/senado-aprova-regulamentacao-da-inteligencia-artificial-texto-vai-a-camara. Acesso em: 05 jan. 2025.

identificar padrões e perfis comportamentais”. Tais sistemas serão classificados de alto risco e sujeitos à regulamentação mais rígida, contudo, como as autoridades estatais diferenciarão o conteúdo disposto no Art. 13, I, c, e o Art. 14, IX, será tema interessante para pesquisa futura.

6 CONSIDERAÇÕES FINAIS

Testemunhamos neste século uma profunda transformação no modo de vida, de trabalho e de organização social. As chamadas tecnologias de informação e telecomunicações (TICs) se tornaram “parte integral da vida diária”, de modo que o termo “sociedade da informação” foi cunhado para esta nova etapa do desenvolvimento humano. A sociedade da informação é uma revolução comparável à profundas transformações do mundo promovidas por poucas invenções na história da humanidade.

A introdução da Indústria 4.0 no final do século XX representou uma revolução em que a Internet das Coisas (IoT), sistemas de integração cibernética e *smart factories* (fábricas inteligentes, em tradução livre), *Big Data* e tecnologias de nuvem foram introduzidos, marcados pelo “alto nível de complexidade” com a utilização de *smart factories* e sua robótica, que são sistemas ciberfísicos controlados por sistemas de automação baseados em algoritmos de aprendizado de máquina.

Entretanto, a tecnologia avança, ainda neste quarto de século, a passos galopantes. Compartilhar informações se tornou muito mais fácil com a Indústria 4.0 e a digitalização de modo geral do mundo fez com que as informações digitais produzidas tenham superado todas as expectativas e previsões. Mal nos adaptamos aos conceitos introduzidos pela Indústria 4.0 e já estamos no alvorecer da Sociedade 5.0, também chamada de *Smart Society* (ou sociedade inteligente, em tradução livre). O conceito de *Smart Society* foi apresentado pelo Japão no escopo e emergiu do crescente desenvolvimento e utilização de sistemas inteligentes, como a Inteligência Artificial. Em resumo, a Sociedade 5.0 busca integrar elementos tecnológicos em cada processo da sociedade.

Diversas são preocupações originadas a partir dessa evolução social e o Direito, em especial o Direito Penal, tem sido provocado a “ler” a nova realidade e apresentar soluções para novos tipos de condutas lesivas a bens jurídicos. A “criminalidade moderna” e os desafios impostos ao Direito Penal são extensa fonte de preocupação sendo que juristas e autores já manifestaram sua visão de que o Direito Penal é incapaz de solucionar os modernos problemas da criminalidade, e nós temos que refletir a

respeito de algo que seja melhor, mais eficaz, que seja capaz de solucionar esses problemas.

Diversos são os desafios modernos impostos ao Direito Penal, como a criminalidade econômica difusa, a criminalidade ecológica, criminalidade no comércio exterior (com o contrabando de armas), contrabando internacional de drogas. Entretanto, um dos grandes desafios impostos à Sociedade 5.0 e, consequentemente, ao Direito, está no respeito à privacidade e à proteção de dados pessoais. Na era digital, a proteção da privacidade se tornou uma preocupação central, demandando que países e regiões ao redor do mundo publiquem abrangente legislação de privacidade.

Em uma era que *Big Data* e a Inteligência Artificial são onipresentes, algoritmos de aprendizado de máquina são cada vez mais usados para extrair informações de vastos conjuntos de dados. Entretanto, esses conjuntos de dados frequentemente possuem informações sensíveis sobre indivíduos.

Tecnologias de vigilância baseadas em reconhecimento facial, reconhecimento de íris e digitalização de digitais são parte de sistemas de identificação e autenticação contemporâneos. Adicionalmente, a coleta em massa e armazenamento de dados biométricos de diversas fontes tem sido empregados para segurança, garantia da lei e finalidades de segurança pública, comprometendo o direito à privacidade dos indivíduos.

A evolução das leis de privacidade na era digital é um processo dinâmico moldado por perspectivas históricas, avanços tecnológicos e a necessidade imperativa de estruturas jurídicas atualizadas. O equilíbrio entre o direito à privacidade e à proteção de dados pessoais e o progresso tecnológico continua delicado, exigindo uma reavaliação contínua para garantir que os sistemas normativos e jurídicos protejam efetivamente as informações pessoais em nosso cenário digital em rápida evolução.

O Direito tem sido demandado para a proteção de bens jurídicos próprios dessa nova evolução social por meio de adequada regulamentação. O Direito Penal, especificamente, tem experimentado uma pressão para seu expansionismo por meio da introdução de novos tipos legais para alcançar condutas que violem ou exponham a perigo esses bens jurídicos e, também, para se valer de todos esses recursos advindos do progresso tecnológico com o objetivo de buscar elementos que formem amplos

acervos probatórios, ainda que sem utilização imediata, sem limites bem definidos e, até mesmo, sem fundada suspeita de conduta incriminadora.

O Estado e sua manifestação em todas as etapas jurídico-penais (repressão, investigação, persecução e execução penal) tem frequentemente violado a privacidade e a proteção de dados pessoais de indivíduos, bens jurídicos da mais profunda importância para o ser humano, expressão direta da dignidade humana e sua autodeterminação informacional. Tais violações se dão por meio de medidas interventivas que buscam obter informações privilegiadas, sigilosas, utilizando desde a antiga interceptação de correspondências em meio físico (cartas) até o uso intenso do aparato tecnológico disponível para o Estado na forma de vigilância eletrônica, vigilância telemática, infiltração encoberta em dispositivos informáticos pessoais, escuta ou vigilância telefônica, captura de dados de comunicação online, levantamento (coleta, busca, obtenção) de dados em dispositivos informáticos pessoais e toda a sorte de intervenções.

A teoria do bem jurídico é central na dogmática penal e a proteção de bens jurídicos é missão fundamental do Direito Penal, que tem no conceito material de crime a violação do bem jurídico ou sua exposição a perigo. Sendo os bens jurídicos as circunstâncias reais dadas ou finalidades necessárias para uma vida segura e livre, que garanta todos os direitos humanos e civis de cada um na sociedade ou para o funcionamento estatal que se baseia nestes objetivos, é de essencial importância que seja lançada a necessária luz sobre os bens jurídicos afetados nas violações à privacidade e proteção de dados pessoais. Compreender estes bens jurídicos e sua importância para a dignidade humana e seu livre e consciente desenvolvimento é o primeiro passo para conferir adequada proteção.

A privacidade é um bem jurídico que possui extenso desenvolvimento sociológico e jurídico. Diferentemente de outros bens jurídicos, a privacidade e seus aspectos manifestam-se de diversos modos na vida humana, a depender das influências que o indivíduo decisivamente sofra de fatores culturais, religiosos, políticos, filosóficos, sem se esquecer de que as próprias circunstâncias, ou um dado momento existencial, podem permitir modificações ou novos conceitos até então inexplorados.

De tal modo, enquanto a principal proteção a ser conferida nas relações humanas do passado se relacionada ao sigilo das comunicações e inviolabilidade das

correspondências e do domicílio, os desafios contemporâneos introduziram inúmeras novas complexidades, repletas de nuances, mas que colocam exponencialmente em xeque a dignidade humana, dada a centralidade representada pela tecnologia incorporada ao cotidiano do ser humano em uma escala global.

Essa centralidade tecnológica não admite mais passos para trás. A progressão é marca registrada do avanço científico-tecnológico e os aspectos econômicos se desdobram em infinitas possibilidades na sociedade da informação e sua transição para uma sociedade inteiramente "*smart*", dotada de inteligência artificial que encurta os ciclos de transições entre estes avanços de tal maneira que até mesmo o mais tecnológico dos humanos encontra dificuldades para acompanhar.

Reconhecendo tal realidade, a Alemanha, que possui a tradição dogmática da elaboração e desenvolvimento do conceito do bem jurídico, deu significativos passos na produção de conteúdo acerca dos direitos de personalidades intimamente conectados ao tema da privacidade. Foi, também, pioneira no reconhecimento jurídico do direito à privacidade e proteção de dados pessoais com a Lei de Proteção de Dados do Estado de Hessen (*Hessisches Datenschutzgesetz*), na década de 1970. Assim, a dogmática alemã, reconhecendo a área central, nuclear, da vida privada (*Kernbereich Privater Lebensgestaltung*), não admitia possibilidade de intervenção em razão desse núcleo representar a própria expressão da dignidade humana, gozando de proteção absoluta por meio do Artigo 1(1) da Lei Fundamental alemã, conforme o próprio Tribunal Constitucional Federal alemão (*Bundesverfassungsgericht*).

A decisão do Tribunal Constitucional Federal alemão datada de 15 de dezembro de 1983 (BVerfGE 65, 1) sobre o caso envolvendo a Lei do Censo alemã (*Volkszählungsgesetz*) foi pioneira e emblemática para o tema da privacidade no mundo ocidental, reunindo diversos princípios e institutos e estabelecendo paradigmas quanto aos requisitos para tratamento dos dados pessoais dos indivíduos.

A dogmática constitucional-penal alemã dos direitos fundamentais (que serviu de grande inspiração para a dogmática brasileira), estabeleceu hipóteses autorizativas de intervenções em direitos fundamentais, autênticos limites que, caso violados, conferem o caráter de intervenção proibida a qualquer medida interventiva por parte do Estado e seus órgãos penais. E para limitar o poder do legislador em interferir nos direitos fundamentais,

a própria Constituição estabelece verdadeira reserva legal com critérios qualificados para que se limite o poder de limitar (*Schranken-Schranken*).

A União Europeia, depois de uma longa história legislativa de décadas envolvendo leis nacionais dos países membros, passando pela Diretiva 95/46/EC, culminando com seu Regulamento Geral de Proteção de Dados (*General Data Protection Regulation*), publicou sua Diretiva de Proteção de Dados 2016/680 que "trata da proteção de pessoais naturais com relação ao processamento de dados pessoais por autoridades competentes para os propósitos de prevenção, investigação, detecção ou persecução de ofensas criminais ou para a execução de penas criminais, no livre movimento de tais dados".

Tal Diretiva, de acordo com o Tratado sobre o Funcionamento da União Europeia (2016/c 202/01), tem o condão de vincular o Estado-Membro destinatário quanto ao resultado a alcançar, deixando, no entanto, às instâncias nacionais a competência quanto à forma e aos meios. Assim, é dever dos Estados-Membros a regulamentação do tema inteiramente vinculados aos objetivos da Diretiva por meio da edição de leis nacionais.

A Constituição brasileira reconhece o direito à intimidade e à vida privada, bem como o direito à proteção de dados pessoais, como direitos fundamentais. O país publicou sua Lei Geral de Proteção de Dados Pessoais com a finalidade de ser o principal regulamento infraconstitucional sobre a matéria excetuando, entretanto, a sua aplicabilidade para atividades de tratamento de dados pessoais realizadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, transferindo tal regulamentação para legislação específica sobre o assunto.

Enquanto isso, o panorama geral das medidas de intervenção em direitos fundamentais utilizadas pelas autoridades penais no país é de incerteza e insegurança. A falta de regulamentação específica escancara a evidente urgência de atuação do Poder Legislativo. Para ilustrar a dimensão do problema, o tema da infiltração online (ou infiltração encoberta, de acordo com a nomenclatura adotada pela dogmática alemã) é objeto, à época da elaboração deste trabalho, de uma Arguição de Descumprimento de Preceito Fundamental (ADPF) de número 1143, que aponta precisamente a ausência de atuação normativa do Congresso Nacional nesta regulação. Este é apenas um único tema dentre as diversas medidas de intervenção em direitos fundamentais que

necessitam de regulamentação adequada, em cumprimento à reserva legal e qualificada necessária para tal.

A Lei Geral de Proteção de Dados brasileira traz em seu bojo uma série de princípios que podem e devem ser aproveitados no trabalho de elaboração legislativa sobre o tema de tratamento de dados pessoais em matéria jurídico-penal. Entretanto, apontamos ao longo do trabalho a importância de uma regulamentação própria que, assemelhada à regulamentação realizada pela dogmática constitucional-penal alemã, especifique as atividades de tratamento de dados pessoais (levantamento, armazenamento, modificação, compartilhamento, transmissão e uso) e seus requisitos (tempo de duração, condições, tratamento de não suspeitos afetados etc.) de acordo com os princípios constitucionais-penais existentes e os demais trazidos pela legislação infraconstitucional representada pela LGPD, desde que compatíveis com a devida abordagem garantista penal.

Diante de toda a pesquisa realizada, a resposta que formulamos à questão que se impunha no início deste trabalho é de que sim, é mais que importante, é urgente a necessidade de elaboração de legislação penal específica para proteção de dados pessoais na atividade jurídico-penal do Estado.

Quanto à criminalização de condutas, apelo insistente dos adeptos de um Direito Penal expansionista, entendemos não haver necessidade de novos tipos penais distintos dos constantes na seção III do Código Penal brasileiro, que trata dos crimes contra a inviolabilidade de correspondência, e na seção IV, que trata dos crimes contra a inviolabilidade dos segredos, além do crime de violação de sigilo funcional, disposto no art. 325. Nos futuros anteprojetos e projetos de lei voltados à regulamentação da proteção de dados pessoais na esfera jurídico-penal, não se mostra necessária a criação de novos tipos penais. O foco deve estar na preservação dos direitos fundamentais, em especial os direitos à privacidade e à proteção de dados, ao longo de todo o exercício do poder penal, desde a investigação até a execução penal.

Já no tocante à execução penal, o Estado deve fazer valer minimamente o disposto no art. 93 do Código Penal, que assegura ao condenado o sigilo dos registros sobre o seu processo e condenação, utilizando todos os meios necessários e disponíveis para autenticação, controle e registros (*logs*) que apontem, imediatamente, qualquer

violação (ou sua tentativa de violação) do bem jurídico penal em questão, a confidencialidade dessas informações e o que elas representam no necessário processo de reabilitação do apenado, respondendo o agente da conduta pelos crimes pertinentes já tipificados no código penal, além da devida punição em âmbito administrativo.

REFERÊNCIAS

AIETA, Vânia Siciliano. **A garantia da intimidade**. Rio de Janeiro: Editora Lumens Juris, 1999.

ALEXY, Robert. **Theorie der Grundrechte**. Frankfurt am Main: Suhrkamp, 1986.

ALLDRIDGE, Peters; BRANTS, Crisje. **Personal Autonomy, the Private Sphere and the Criminal Law**. Portland: Hart Publishing, 2001.

AMNESTY INTERNATIONAL. **Forensic Methodology Report: How to Catch NSO Group's Pegasus**. London: Amnesty International Ltd, 2021.

ARAÚJO, José Laércio. **Intimidade, vida privada e direito penal**. São Paulo: Editora Habeas, 2000.

ÁVILA, Humberto. **Teoria dos princípios: da definição à aplicação dos princípios jurídicos**. 20. ed. rev. aum. São Paulo: Malheiros, 2021.

BADARÓ, Tatiana. **Bem jurídico-penal supraindividual**. Belo Horizonte: Editora D'Plácido, 2017.

BADARÓ, Tatiana. **Teoria do bem jurídico.** Florianópolis: Emais Editora, 2023.

BECHARA, Ana Elisa L. S. **Bem jurídico-penal.** São Paulo: Quartier Latin, 2014.

BERNAL PULIDO; Carlos. **El principio de proporcionalidad y los derechos fundamentales. El principio de proporcionalidad como criterio para determinar el contenido de los derechos fundamentales vinculante para el Legislador**. 4. Ed. Bogotá: Universidad Externado de Colombia, 2014.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed., rev., aum. e mod. São Paulo: Saraiva, 2015.

BRANDÃO, Cláudio. **Teoria Jurídica do Crime**. Coleção: Ciência Criminal Contemporânea. 5 ed. Vol. 1. Coordenação: Cláudio Brandão. Belo Horizonte: Editora D'Plácido, 2019.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF. Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 10 ago. 2024.

BRASIL. **Decreto nº 592, de 6 de julho de 1992**. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Disponível em:

https://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 14 jan. 2025.

BRASIL. **Decreto nº 11.777, de 9 de novembro de 2023**. Promulga o Protocolo Facultativo ao Pacto Internacional sobre Direitos Civis e Políticos e o Segundo Protocolo Facultativo ao Pacto Internacional sobre Direitos Civis e Políticos com vistas à Abolição da Pena de Morte, de 15 de dezembro de 1989. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11777.htm. Acesso em: 14 jan. 2025.

BRASIL. Decreto-Lei n. 2.848, de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Brasília, 31 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 10 ago. 2024.

BRASIL. **Lei nº 7.210, de 11 de julho de 1984**. Institui a Lei de Execução Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7210.htm. Acesso em: 14 jan. 2025.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 14 jan. 2025.

BRASIL. **Lei nº 10.792, de 1 de dezembro de 2003**. Altera a Lei nº 7.210, de 11 de junho de 1984 - Lei de Execução Penal e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 - Código de Processo Penal e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.792.htm. Acesso em: 14 jan. 2025.

BRASIL. **Lei nº 11.343, de 13 de agosto de 2006**. Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em: 14 jan. 2025.

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. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2009/lei/l12037.htm. Acesso em: 14 jan. 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal [...]. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 15 jul. 2024.

BRASIL. **Lei nº 12.654, de 28 de maio de 2012**. Altera as Leis nºs 12.037, de 1º de outubro de 2009, e 7.210, de 11 de julho de 1984 - Lei de Execução Penal, para prever a coleta de perfil genético como forma de identificação criminal, e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12654.htm. Acesso em: 14 jan. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 18 ago. 2024.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 14 jan. 2025.

BRASIL. **Lei nº 13.441, de 8 de maio de 2017**. Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13441.htm. Acesso em: 14 jan. 2025.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em 14 jan. 2025.

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 [...]. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 10 ago. 2024.

BRASIL. Ministério da Justiça e Segurança Pública. Comitê Gestor da Rede Integrada de Bancos de Perfis Genéticos. **XX relatório da Rede Integrada de Bancos de Perfis Genéticos (RIBPG)**: dados estatísticos e resultados: nov/2023 a mai/2024. Brasília: Comitê Gestor da Rede Integrada de Bancos de Perfis Genéticos, 2024. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/ribpg/relatorio/xx-relatorio-da-rede-integrada-de-bancos-de-perfis-geneticos-maio-2024-1.pdf/@@download/file. Acesso em: 03 jan. 2025.

BURCHARD, Christoph. **El Principio de Proporcionalidad en el 'Derecho Penal Constitucional', de el Fin de la Teoría del Bien Jurídico Tutelado en Alemania**.

Ambos/Böhm (Dir./Coord.), Desarrollos Actuales de las Ciencias Criminales en Alemania. Bogotá: Editorial Temis, 2012.

CALP, M. Hanefi; BÜTÜNER, Resul. **Society 5.0: Effective technology for a smart society**. Artificial Intelligence and Industry 4.0. [s.l.], Academic Press: 2022.

CANTON FILHO, Fábio. **Bem jurídico penal**. Rio de Janeiro: Elsevier, 2012.

COHN, Georg. **Neue Rechgüter.** Berlin: HL und Recht, 1902.

COSTA ANDRADE, Manuel. **Consentimento e acordo em Direito Penal (contributo para a fundamentação de um paradigma dualista)**. Coimbra: Coimbra Editora, 2004.

COSTA JUNIOR, Paulo José. **O direito de estar só: a tutela penal do direito à intimidade**. 3. ed. São Paulo: Siciliano Jurídico, 2004.

CUPIS, Adriano de. **Os direitos da personalidade**. 2. ed. São Paulo: Editora Quorum, 2008.

DENVER; Megan; PICKETT, Justin; BUSHWAY, Shawn. **Criminal Records and Employment: A Survey of Experiences and Attitudes in the United States**. Justice Quarterly, 35(4), 584–613, 2017.

DIMITRI, Dimoulis; MARTINS, Leonardo. **Teoria Geral dos Direitos Fundamentais**. 7. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020.

DOTTI, René Ariel. **Proteção da vida privada e liberdade de informação.** São Paulo: Ed. Revista dos Tribunais, 1980.

DUTRA, Luiza Correa de Magalhães; PEREIRA, Wilson Guilherme Dias; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Hacking Governamental: uma revisão sistemática**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, fevereiro de 2023. Disponível em: https://bit.ly/3YdVcIL. Acesso em: 30 dez. 2024.

EUROPOL. **Internet Organised Crimes Threat Assessment (IOCTA) 2024**. Luxembourg: Publications Office of the European Union, 2024.

EUROPOL. **Europol Spotlight - Cyber-Attacks: the apex of Crime-as-a-Service**. Luxembourg: Publications Office of the European Union, 2023.

EUROPEAN UNION. **The European Union – What it is and what it does**. Luxembourg: Publications Office of the European Union, 2019.

FERRAJOLI, Luigi. **Direito e razão: teoria do garantismo penal**. São Paulo: Editora Revista dos Tribunais, 2002.

FEUERBACH, P. J. Anselm R. von. **Tratado de derecho penal común vigente en Alemania**. Traducción de la 14. edición alemana por Eugenio Raúl Zaffaroni y Irma Hagemeier. Buenos Aires: Editorial Hammurabi, 1989.

FLAHERTY, David H. **Privacy in Colonial New England**. Charlottesville: University Press of Virginia, 1972.

FERNANDES, Milton. **Proteção civil da intimidade**. São Paulo: Saraiva, 1977.

GASIOLA, Gustavo. **Criação e desenvolvimento da proteção de dados na Alemanha**. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/criacao-e-desenvolvimento-da-protecao-de-dados-na-alemanha-29052019. Acesso em: 15 jun. 2024.

GAVISON, Ruth. Privacy and the Limits of Law. **The Yale Law Journal**, New Haven, vol. 89, nº 3, p. 421-471, 1980.

GIDNEY, Craig; EKERÅ, Martin. **How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits**. Quantum Journal 5, 433 (2021). Disponível em: https://doi.org/10.48550/arXiv.1905.09749. Acesso em: 08 ago. 2024.

GILL, Sukhpal *et al*. **Modern computing: Vision and challenges**. Telematics and Informatics Reports, Volume 13, 2024.

GLANCY, Dorothy. **The Invention of the right to privacy**. In: Arizona Law Review, Vol. 21, nº 1, 1979, p. 1-39.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O direito de proteção de dados no processo penal e na segurança pública**. São Paulo: Marcial Pons, 2021.

GRABOSKY, Peter; URBAS, Gregor. **Online Undercover Investigations and the Role of Private Third Parties** in: Surveillance, Law and Humanities. Edinburgh: Edinburgh University Press, 2023.

GRECO, Luís; GLEIZER, Orlandino. **A infiltração online no processo penal – Notícia sobre a experiência alemã**. Rev. Bras. de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, p. 1483-1518, set.-dez. 2019.

HASSEMER, Winfried. **Perspectivas de uma moderna política criminal**. Revista Brasileira de Ciências Criminais, São Paulo, n. 9, p. 41-51, out.-dez. 1994.

HEFENDEHL, Roland; HIRSCH, Andrew von; WOHLERS, Wolfgang. **La teoría del bien jurídico. ¿Fundamento de legitimación del Derecho penal o juego de abalorios dogmático?** Madrid: Marcial Pons, 2016.

HENKEL, Heinrich. **Der Strafschutz des Privatlebens Gegen Indiskretion: Gutachten für den 42. Deutschen Juristentag erstattet von Dr. *Heinrich Henkel*, Professor an der Universität Hamburg**. Tübingen: J. C. B. Mohr (Paul Siebeck), 1958.

HOLVAST, Jan. **History of Privacy**. In: Matyáš, V., Fischer-Hübner, S., Cvrček, D., Švenda, P. (eds) The Future of Identity in the Information Society. Privacy and Identity 2008. IFIP Advances in Information and Communication Technology, vol. 298. Berlin: Springer, 2008.

HUBMANN, Heinrich. **Das Persönlichkeitsrecht**. Köln: Böhlau, 1967.

INESS, Julie C. **Privacy, Intimacy, and Isolation**. New York: Oxford University Press, 1992.

IP.REC - INSTITUTO DE PESQUISA EM DIREITO E TECNOLOGIA DO RECIFE. **Nota Técnica: Desafios regulatórios e diretrizes acerca do uso de ferramentas de intrusão digital no contexto brasileiro**. Recife: IP.rec, 2024.

ISHIDA, Válter Kenji. **Bem jurídico penal moderno**. Salvador: Editora Juspodivm, 2017.

KOKOTT, Juliane; SOBOTTA, Christoph. **The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR**. International Data Privacy Law, Volume 3, Issue 4, November 2013, Pages 222–228.

LAGESON, Sarah. **Privacy and Rehabilitation after a Criminal Conviction in the Digital Age**. Privacy, Technology, and the Criminal Process. New York: Routledge, 2024.

LAGESON, Sarah. **Digital punishment's tangled web**. Contexts, 2016. Disponível em: https://contexts.org/articles/digital-punishments-tangled-web. Acesso em: 10 ago. 2024.

LEE, Kai-Fu; QIUFAN, Chen. **AI 2041: ten visions for our future**. New York: Crown Publishing Group, 2021.

LISZT, Franz von. **Tratado de direito penal allemão**. Tomo I. Tradução de José Hygino Duarte Pereira. Rio de Janeiro: F. Briguiet & C. Editores, 1899. (LISZT, Franz von. **Tratado de direito penal allemão**. Prefácio de Edson Carvalho Vidigal. Tradução de José Hygino Duarte Pereira. Ed. Fac-sim. Brasília: Senado Federal, Conselho Editorial e Superior Tribunal de Justiça, 2006. Coleção história do direito brasileiro. Direito Penal).

LOPES, Eduardo L. P. **Um esboço das biografias no Brasil: a liberdade de expressão, a personalidade e a Constituição de 1988**. São Paulo: Almedina, 2015.

LOPES, Mauricio A. R. **Princípios políticos do direito penal**. 2. ed. São Paulo: Editora Revista dos Tribunais, 1999.

LUISI, Luiz. **Os princípios Constitucionais Penais**. 2. ed. rev. aum. Porto Alegre: Sergio Antonio Fabris Editor, 2003.

LUSKY, Louis. **Invasion of Privacy: A Clarification of Concepts**. Political Science Quarterly, Volume 87 (2): 18 – Jun 15, 1972.

MARIANO DA SILVA, César D. **Tutela penal da intimidade**. Curitiba: Editora Juruá, 2015.

MARTINS, Leonardo (Org. e Intr.). **Cinquënta anos de jurisprudência do Tribunal Constitucional Federal alemão**. Montevideo: Konrad-Adenauer-Stiftung, 2005.

MATYÁŠ, Vashek *et al*. **The Future of Identity in the Information Society: 4th IFIP WG 9.2, 9.6, 11.6, 11.7/FIDIS International Summer School, Brno, Czech Republic, September 1-7, 2008, Revised Selected Papers**. Heildeberg: Springer Berlin, 2009.

MARUNA, Shadd; LAGESON, Sarah. **Digital degradation: Stigma management in the internet age.** Punishment & Society 2018, Vol. 20(1) 113–133, 2017.

MARX, Gary. **Undercover: police surveillance in America.** Berkeley: University of California Press, 1988.

MENDES, Gilmar; BRANCO, Paulo G. G. **Curso de Direito Constitucional**. 10. ed. rev. e atual. São Paulo: Saraiva, 2015**.**

MEREDITH, Dale. **Certified Ethical Hacker (CEH) v11 312-50 Exam Guide**. Birmingham: Packt Publishing, 2022.

NISSENBAUM, Helen. **Privacy in Context**. Stanford: Stanford University Press, 2010.

O'Brien, David M. **Privacy, law and public policy**. New York: Praeger Publishers, 1979.

OLIVEIRA, Arlindo; FIGUEIREDO, Mário. **Artificial Intelligence: Historical Context and State of the Art**. Multidisciplinary Perspectives on Artificial Intelligence and the Law – Law, Governance and Technology Series, Vol. 58. Lisboa: Springer, 2024.

PAGER, Devah. **The Mark of a Criminal Record**. American Journal of Sociology, 108 (5):937-975, 2013.

PARIKH, Deval; RADADIA, Sarangkumar; ERANNA, Raghavendra. **Privacy-Preserving Machine Learning Techniques, Challenges and Research Directions**. International Research Journal of Engineering and Technology (IRJET). Vol. 11, Issue: 03. [s.l.]: IRJET, 2024.

PARKER, Richard. **A Definition of Privacy**. Rutgers Law Review, Vol. 27, n. 2. New Jersey: Rutgers University, 1974.

PIJOAN, Elena. **Legal protections Against criminal background checks in Europe**. Punishment & Society, 16(1) 50–73, 2014.

POLITOU, Eugenia *et al*. **Privacy and Data Protection Challenges in the Distributed Era** (Vol. 26, pp. 1-185). Switzerland: Springer. 2022.

PRADO, Luiz Regis. **Bem jurídico-penal e constituição.** 8. ed. Rio de Janeiro: Editora Forense, 2019.

PUIG, Santiago Mir. **Introducción a las bases del derecho penal. Concepto y método.** 2. ed. Buenos Aires: Editorial B de F, 2003.

RAMOS, André de Carvalho. **Curso de Direitos Humanos**. São Paulo: Saraiva, 2014.

RAPOSO, Guilherme. **Teoria do bem jurídico e estrutura do delito**. Porto Alegre, Nuria Fabris Editora, 2011.

REIS, Oluwatosin *et al*. **Privacy law challenges in the digital age: a global review of legislation and enforcement.** International Journal of Applied Research in Social Sciences, Vol. 6, Issue 1. [s. l.]: Fair East Publishers, 2024.

RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Org: Maria Celina Bodin. Trad. Danilo Doneda e Luciana Doneda. Rio de Janeiro: Renovar, 2008.

ROSA, Alexandre Morais da; SILVA, Viviane Ghizoni da; SILVA, Philipe Benoni Melo e. **Fishing Expeditions e encontro fortuito na busca e apreensão: um dilema oculto no processo penal**. 2 ed. Florianópolis: Emais, 2022.

ROVIRA, Marti. **The next Pandora's Box of criminal background checks**. European Journal of Criminology, 1-17, 2020.

ROXIN, Claus. **A proteção de bens jurídicos como função do Direito Penal**. 2. ed. Porto Alegre: Livraria do Advogado Editora, 2013.

ROXIN, Claus. **Derecho Penal.** Parte General. Tomo I. Fundamentos. La estructura de la teoría del delito. Trad. Dieg-Manuel Luzón Peña, Miguel Díaz y García Conlledo e Javier de Vicente Remesal. 2. ed. Madrid: Editorial Civitas, 1997.

RUSSEL, Stuart; NORVIG, Peter. **Artificial Intelligence – A modern approach**. 4 ed. Portsmouth: Springer, 2020.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**. Belo Horizonte: Editora Livraria Del Rey, 1998.

SANTA MARIA, José Serpa de. **Direito à imagem, à vida e à privacidade**. Belém: CEJUP, 1994.

SANTOS, José Eduardo Lourenço dos; KANDA, Bruna Barbara Paiz Zeotti. INFILTRAÇÃO POLICIAL NA INVESTIGAÇÃO DE CRIMES: A LEGISLAÇÃO BRASILEIRA E O DIREITO COMPARADO. **Revista Juridica**, [S.l.], v. 1, n. 77, p. 72 - 116, abr. 2024. ISSN 0103-3506. Disponível em: https://revista.unicuritiba.edu.br/index.php/RevJur/article/view/6769. Acesso em: 28 dez. 2024.

SARLET, Gabrielle Bezerra Sales; **Separação Informacional de Poderes na Ordem Jurídico-Constitucional** - Série “Direito, Tecnologia, Inovação e Proteção de Dados num Mundo em Transformação" / Gabrielle Bezerra Sales Sarlet, Ingo Wolfgang Sarlet; coordenado por Ingo Wolfgang Sarlet, Laura Mendes, Danilo Doneda. - São Paulo: Expressa Jur, 2023.

SCHWABE, Jürgen. **Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Org: Leonardo Martins. Konrad-Adenauer-Stiftung: Berlim, 2005.

SHILS, Edward. **Privacy: Its Constitution and Vicissitudes**. Vol. 31, Nº. 2, Privacy (Spring, 1966), p. 281-306. Durham: Duke University School of Law, 1966.

SILVA, Edson Ferreira da. **Direito à intimidade**. São Paulo: Editora Oliveira Mendes, 1998.

SKEEM, Jennifer; LOWENKAMP, Christopher. **Risk, Race, & Recidivism: Predictive Buas and Disparate Impact**. Disponível em: http://dx.doi.org/10.2139/ssrn.2687339. Acesso em: 04 jan. 2025.

SOLOVE, Daniel. **Understanding Privacy**. Cambridge: Harvard University Press, 2008.

SOLOVE, Daniel. **Conceptualizing Privacy**. 90 California Law Review 1087, 2002.

SHUMAILOV, Ilia *et al*. **AI models collapse when trained on recursively generated data**. Nature 631, 755–759 (2024). https://doi.org/10.1038/s41586-024-07566-y

STORY, Joseh. **Commentaries on the Constitution of the United States in Three Volumes (1833)**. Livonia: Lonang Institute, 2005.

THOMSON, Judith J. The Right to Privacy. **Philosophy and Public Affairs**, Vol. 4, nº. 4. p. 295-314. Princeton: Princeton University Press, 1975.

UBARAYEN, Miguel. **Vida privada e información: un conflicto permanente**. Pamplona: Ediciones Universidad de Navarra, 1977.

UNESCO. **Science in the Information Society**. Paris, 2003. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000133021. Acesso em: 18 ago. 2024.

UNITED NATIONS. **Governing AI for Humanity: Final Report**. New York, 2024. Disponível em: https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf . Acesso em: 05 jan. 2025.

USTARAN, Eduardo. **European Data Protection – Law and Practice**. Portsmouth: International Association of Privacy Professionals, 2018.

VÉLIZ, Carissa. **Privacidade é poder**. Tradução: Samuel Oliveira. São Paulo: Editora Contracorrente, 2021.

WAGNER, Wienczyslaw. **Le "droit a l'intimité" aux États-Unis**. In: Revue internationale de droit comparé. Vol. 17, n°2, Avril-juin 1965. p. 365-376.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**. Harvard Law Review, Vol. 4, Nº. 5, p. 193-220, 1890.

WELZEL, Hans. **Derecho penal. Parte General**. Trad. Carlos Fontán Balestra. Buenos Aires: Roque Depalma Editor, 1956.

WELZEL, Hans. **Introducción a la filosofía del derecho: derecho natural y justicia material**. 2. ed. Trad. Felipe González Vicén. Madrid: Aguilar, 1971.

WESTIN, Alan F. **Privacy and Freedom**. New York: Atheneum, 1967.

WIMMER, Miriam. **Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia**. Revista Brasileira de Políticas Públicas, v. 11, n. 1, 2021. Disponível em: https://www.publicacoes.uniceub.br/RBPP/article/view/7136/pdf. Acesso em: 31 jul. 2024.

WOLTER, Jürgen. **O inviolável e o intocável no direito processual penal: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal.** Luís Greco (tradução, organização e introdução). Eduardo Viana e Alaor Leite (tradução). São Paulo: Marcial Pons, 2018.

ZANINI, Leonardo. **A proteção da imagem na Alemanha**. Civilistica.com. Rio de Janeiro, a. 6, n. 2, 2017. Disponível em: http://civilistica.com/a-protecao-da-imagem-na-alemanha/. Acesso em: 26 abr. 2024.

ZANINI, Leonardo; QUEIROZ, Odete N. C. **O direito geral da personalidade: do surgimento ao reconhecimento no Brasil.** Revista Brasileira de Direito Civil: RBDCivil, Belo Horizonte, n. 27, p. 15-36, jan./mar. 2021.

ZANINI, Leonardo. **O surgimento e o desenvolvimento do right of privacy nos Estados Unidos**. Revista Brasileira de Direito Civil, [S. l.], v. 3, n. 01, 2017. Disponível em: https://rbdcivil.ibdcivil.org.br/rbdc/article/view/107. Acesso em: 5 mai. 2024.