DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

DIREITO PENAL EMPRESARIAL, PROTEÇÃO DE DADOS PESSOAIS E O COMPLIANCE DIGITAL

CORPORATE CRIME, PERSONAL DATA PROTECTION, AND DIGITAL COMPLIANCE

Artur de Brito Gueiros Souza[1]

Pedro Teixeira Gueiros[2]

RESUMO

Discorre-se sobre a proteção dos dados pessoais como sendo um dever não somente do Direito Civil, como igualmente do Direito Penal. Além de propor a criação de um crime específico para a violação desse direito, o artigo analisa a atuação das pessoas jurídicas que exploram comercialmente os dados dos cidadãos, enfatizando a importância do aprimoramento dos mecanismos de *compliance* no tratamento de dados pessoais.

Palavras-chave: Dados Pessoais. Direito Penal. Grandes Corporações. *Compliance* Digital.

ABSTRACT

The article discusses protecting personal data as a duty under Civil and Criminal Law. It proposes creating a specific crime for violating this right. It analyzes the actions of legal entities that commercially exploit citizens' data, emphasizing the importance of improving compliance mechanisms in processing personal data.

Keywords: Personal Data. Criminal Law. Big Techs. Digital Compliance.

1 Professor Titular de Direito Penal da UERJ; Coordenador do CPJM; Subprocurador-Geral da República. E-mail: *arturgueiros@uerj.br*.

2 Professor Substituto da UFRJ; Professor Assistente no Ibmec-RJ; Advogado. E-mail: *ptgueiros@gmail.com*.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

1. INTRODUÇÃO

Há bem mais de um século, muito antes do início da era digital, a questão da privacidade pessoal foi tema de um artigo científico na *Harvard Law Review*, escrito por Samuel Warren e Louis Brandeis – este último vindo a se tornar um famoso juiz da Suprema Corte dos EUA. Uma das preocupações do artigo estava relacionada com a circulação não autorizada de retratos de pessoas privadas:

> "Fotografias instantâneas e empresas jornalísticas invadiram os recintos sagrados da vida privada e doméstica; e numerosos dispositivos mecânicos ameaçam tornar realidade a previsão de que o que é sussurrado no armário será proclamado dos telhados."[3]

Segundo Peter Grabosky, com uma notável presciência – isto é, 135 anos após aquela publicação –, a privacidade de dados pessoais, objeto da preocupação seminal de Warren e Brandeis, se apresenta na ordem do dia na conjuntura global. Segundo, ainda, Grabosky, as ameaças à privacidade pessoal no ambiente digital emanam de três fontes principais: (1) criminosos cibernéticos individuais; (2) ações governamentais; e (3) organizações empresariais.[4]

Relativamente às finalidades do presente trabalho, importa discorrer sobre a terceira dessas ameaças. Vale dizer, objetiva-se refletir sobre a proteção penal dos dados pessoais diante da atuação de pessoas jurídicas no território brasileiro.

Para tanto, serão feitas considerações dogmáticas e político-criminais a respeito da tutela dos dados e informações dos cidadãos – considerados bens jurídicos de dignidade constitucional –, bem como sobre os tipos penais envolvendo as atividades de tratamento de dados sensíveis, os percalços do *enforcement* diante do poderio das grandes corporações, e, por fim, a relevância do aprimoramento dos mecanismos de *compliance* digital.

3 WARREN, Samuel; BRANDEIS, Louis. *The Right of Privacy. In* Harvard Law Review. N. 4, 1890, p. 195.

4 GRABOSKY, Peter. *Cybercrime. Keynotes in Criminology and Criminal Justice Series.* New York: Oxford University Press, 2016, pp. 87-88.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

2. A PROTEÇÃO DE DADOS PESSOAIS NA ESFERA EXTRAPENAL

Desde a promulgação da Lei Geral de Proteção de Dados (LGPD), pela Lei nº 13.709/2018, a sistemática em torno do uso das informações pessoais viu-se notadamente renovada. Plenamente em vigor, desde 2021, a LGPD trouxe verdadeiramente oxigenação à atual valoração dos dados pessoais, enquanto um importante atributo da pessoa humana. Fato este que pode ser corroborado com a consequente aprovação da Emenda Constitucional nº 115/2022, que elevou a proteção dos dados pessoais ao rol de direitos fundamentais.[5]

Dessa forma, ao disciplinar suas diretrizes a todo e qualquer agente que realize tratamento de dados pessoais, seja pessoa física ou pessoa jurídica, a LGPD traz uma regra clara e transversal à coletividade. Tratando-se da padaria da esquina ou de um grande conglomerado econômico, o uso de informações pessoais relacionadas com os cidadãos exige atenção, cautela e respeito.

Nesse sentido, pode afirmar que:

> "[D]iante do crescente fluxo informacional, a tutela dos dados pessoais passou a demandar maiores cautelas nesse marcante processamento massificado. A partir da edição da LGPD, o panorama sobre o controle dos dados parece ter sido transformado, ou, ao menos, vocacionado a isso. A norma tem como foco a tutela dos direitos fundamentais, tais como os de liberdade, privacidade e livre desenvolvimento da personalidade humana (art. 1º, LGPD). Sob essa égide, um dos preceitos talvez mais evidentes seja o da autodeterminação informativa."[6]

Mesmo calcada em fundamentos (art. 2º, LGPD) e princípios (art. 6º, LGPD), hipóteses legais para o tratamento (art. 7º, LGPD), distinções relevantes, como dados sensíveis (art. 11, LGPD) e dados de crianças e adolescentes (art. 14, LGPD), critérios para transferências internacionais (art. 33, LGPD) e boas práticas de governança (art. 50, LGPD), a LGPD deixou – como efeito indireto – um inevitável gargalo. De acordo com o art. 4º, III, "d", do novel diploma, dentre outras

5 Dispõe o inciso LXXIX do art. 5º, CF: "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

6 GUEIROS, Pedro Teixeira. *Internet e consentimento: autogestão de dados e exercício do controle informacional*. São Paulo: Tirant Lo Blanch Brasil. 2024, p. 48.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

situações excepcionais, seu estatuto legal não se aplica às finalidades relacionadas às atividades de investigação e repressão de infrações penais. Ou seja, ele é despido de conteúdo penal.

3. A PROTEÇÃO DOS DADOS PESSOAIS PELO DIREITO PENAL

Muito embora a LGPD seja aplicável a toda Administração Pública, direta ou indireta, e às pessoas jurídicas de direito privado ou às pessoas físicas, quaisquer atividades de tratamento de informações, que venham a ser realizadas por agentes no âmbito das atividades de repressão e infração penal, dispensam a observância de como estes dados venham a ser utilizados. Por exemplo, no caso de investigados, réus, vítimas, testemunhas, dentre outros intervenientes nos procedimentos judiciais ou extrajudiciais – em especial aqueles em posição de vulnerabilidade –, é preciso que eles recebam o devido cuidado para evitar o mau uso de caracteres que tragam maior exposição.[7]

Não se desconhece, por óbvio, a existência de outras legislações esparsas que desempenham funções relevantes em matéria penal – ainda que não completamente relacionadas com a tutela de dados –, no âmbito da proteção de elementos pessoais. Tem-se, por exemplo, a Lei de Interceptação Telefônica (Lei nº 9.296/1996), que cria restrições relevantes quanto à quebra deste sigilo telefônico,[8] ou a Lei de Identificação Criminal (Lei nº 12.037/2009), que limita o acesso quanto às formas de identificação civil da pessoa condenada em processo criminal.[9] É possível citar ainda, o Marco Civil da Internet (Lei nº

7 A título de exemplo, de acordo com o Considerando nº 75 do Regulamento Geral de Proteção de Dados da União Europeia (RGPD), o maior risco para direitos e liberdades de titulares dados incluem: "quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas".

8 Conforme preconiza o art. 3º, *verbis*: "Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses: I - não houver indícios razoáveis da autoria ou participação em infração penal; II - a prova puder ser feita por outros meios disponíveis; III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção."

9 Nos termos do 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."

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

12.965/2014), que autoriza a quebra de sigilo telemático, dentro de determinados parâmetros, para instruir processos cíveis ou criminais.[10]

Todavia, não há na contemporaneidade uma legislação aos moldes da LGPD, que discipline, de forma ampla e adequada, como o uso de dados pessoais deve ser dar nesse contexto tão relevante para a sociedade.

A propósito, tramita no Congresso Nacional, desde 2020, o denominado Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal (LGPD-Penal), formalizado à época por uma Comissão de Juristas. Na Exposição de Motivos para a criação desse diploma legal, é feita menção à ausência de: (1) padrões internacionais de cooperação e integração do Brasil em matéria de investigação penal; e (2) transparência nos processos de tratamento de dados na esfera penal, potencializados pelas tecnologias de vigilância, progressivamente invasivas.[11]

No que diz respeito ao primeiro item – apesar dos pesares –, não há dúvidas de que o Brasil avançou na integração supranacional. Após um lapso de mais de duas décadas, o País promulgou a Convenção de Budapeste sobre o Cibercrime, de 2001, através do Decreto nº 11.491/2023.[12] A tratativa multilateral visa aperfeiçoar a cooperação jurídica internacional envolvendo a tipificação e a investigações de crimes cibernéticos, incluindo a obtenção de provas eletrônicas armazenadas em outros países. Não obstante o Brasil seja o segundo

10 Similar à racionalidade da Lei de Interceptação Telefônica, diz o art. 22: "A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I - fundados indícios da ocorrência do ilícito; II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros."

11 EXPOSIÇÃO DE MOTIVOS DA LGPD-PENAL (Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal), *passim*. Disponível em https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 09/01/2025.

12 Decreto nº 11.491/2023, Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 09/01/2025.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

lugar com mais ataques cibernéticos registrados no mundo – de acordo com o relatório *Cost of a Data Breach 2024*, da IBM[13] – o País vem adotando estratégias de estruturação e resiliência cibernética, como, *v.g.*, a disciplina trazida com a edição do E-Ciber, por intermédio do Decreto nº 11.856/2023.[14]

Relativamente ao segundo item – o crescimento da vigilância por instrumentos tecnológicos –, há de fato um cenário preocupante e opaco. Seja por câmeras de reconhecimento facial, sistemas de vigilância interna e externa, proliferação de *drones*, dentre outros aparatos instrumentalizados por Inteligências Artificiais (IA), o uso de informações pessoais coletadas de forma massiva é capaz de projetar situações que não permitem o devido controle, particularmente na esfera penal. Nesse sentido, há algum tempo o Intercept Brasil vem trazendo à tona verdadeiros escândalos envolvendo a violação da privacidade através de empresas contratadas por órgãos públicos, que compartilhariam dados pessoais sem qualquer esclarecimento oficial.

Na mesma direção, em 2023, foi revelado que a companhia estadunidense especializada em captar imagens com reconhecimento facial – a Clearview AI – compartilhou mais de três bilhões de fotos de brasileiros, em reuniões a portas fechadas com as Polícias Militar e Civil de São Paulo, além da Polícia Federal e do próprio Ministério da Justiça.[15]

No ano passado, foi noticiada a chamada "farra" dos dados, levada a efeito pela ferramenta *Snap Sinapses Desktop* – pertencente à empresa Techbiz Forense Digital –, que analisa os dados de qualquer

13 NAKAMURA, João. *Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo*. Disponível em: <https://www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-cyberneticos-com-1-379-golpes-por-minuto-aponta-estudo/>. Acesso em: 09/01/2025.

14 Dentre outras medidas, o Decreto cria a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança e institui o Comitê Nacional de Cibersegurança. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 09/01/2025.

15 MARTINS, Laís. *14 fotos por ser humano. Exclusivo: em reuniões secretas, Clearview ofereceu 3 bilhões de imagens de brasileiros para polícias e Ministério da Justiça*. Disponível em: <https://www.intercept.com.br/2023/05/16/em-reunioes-secretas-clearview-policias-ministerio-da-justica/>. Acesso em: 09/01/2025.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

pessoa por meio do cruzamento em mais de 50 plataformas e redes sociais diferentes, expertise esta já disponibilizada à mais de 15 órgãos públicos em 10 Estados da Federação.[16]

4. CRIMES ENVOLVENDO AS ATIVIDADES DE TRATAMENTO DE DADOS PESSOAIS

No bojo desta palpitante realidade, uma pergunta revela-se necessária: como é possível responsabilizar penalmente as pessoas jurídicas – notadamente as que tratam e até mesmo exploram comercialmente as informações pessoais dos cidadãos –, pelas infrações ao dever de proteção de dados?

A indagação é relevante por vários motivos. Inicialmente, na esteira da lacuna intencionalmente projetada pela LGPD, isto é, quanto à sua não incidência às atividades exclusivamente de repressão e investigação penal, não houve a criação de um tipo penal específico para reforçar seus fundamentos e princípios. De acordo com a LGPD, incidem apenas sanções administrativas, passíveis de serem aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD),[17] ou, naturalmente, a via da tradicional responsabilidade civil, por meio do ajuizamento de ações indenizatórias individuais ou coletivas pelos titulares de dados.[18]

Nessa seara, no âmbito do citado Anteprojeto de LGPD-Penal, objetiva-se criar e enxertar no Código Penal, o seguinte tipo penal:

16 AMENO, Fernando. *Farra com dados. Uso de ferramenta que cruza conexões do Facebook e dados da polícia explode no país*. Disponível em: <https://www.intercept.com.br/2024/03/12/uso-de-ferramenta-que-cruza-conexoes-do-facebook-e-dados-da-policia-explode-no-pais/>. Acesso em: 09/01/2025.

17 De acordo com o recente levantamento da Autoridade, "até o momento, a ANPD já analisou e emitiu sanções em 6 (seis) processos administrativos sancionadores face a agentes públicos e privados e atualmente está analisando outros 3 (três) processos administrativos sancionadores". AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Balanço 4 anos*. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd-balanco-4-anos.pdf>. Acesso em: 09/01/2025.

18 Para maiores informações sobre a quantidade de ações judiciais envolvendo a LGPD, sugere-se acompanhar o Painel LGPD nos Tribunais, desenvolvido pelo Centro de Direito, Internet e Sociedade do IDP em parceria com o Jusbrasil. Disponível em https://painel.jusbrasil.com.br/2023 . Acesso em: 09/01/2025.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

> "**Capítulo V - Dos crimes contra a proteção de dados pessoais**
>
> *Transmissão ilegal de dados pessoais*
>
> Art. 154-C. Transmitir, distribuir, usar de forma compartilhada, transferir, comunicar, difundir dados pessoais ou interconectar bancos de dados pessoais sem autorização legal para obter vantagem indevida ou prejudicar o titular dos dados ou a terceiro a ele relacionados:
>
> Pena - Reclusão, de 1 (um) a 4 (quatro), anos e multa.
>
> Parágrafo único. Aumenta-se a pena de um a dois terços se:
>
> I - os dados pessoais forem sensíveis ou sigilosos;
>
> II - o crime for praticado por funcionário público em razão do exercício de suas funções."[19]

É de se louvar a iniciativa parlamentar. Atualmente, não há nenhum dispositivo penal destinado a prevenir e reprimir, *diretamente*, as transgressões à garantia constitucional da proteção de dados pessoais. E isso em face de condutas ilícitas, comissivas ou omissivas, dolosas ou culposas, perpetradas por pessoas físicas ou pessoas jurídicas.

Tangencialmente, há tipos penais que, em tese, poderiam ser aplicados, como, *v.g.*, os crimes previstos nos arts. 153, § 1º-A (*divulgação de segredo*), 154-A (*invasão de dispositivo informático*), 218-C (*divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia*), 325, § 1º, I (*violação de sigilo funcional*), e 359-K (*espionagem*), todos do Código Penal. Da legislação especial, merece referência os arts. 240, § 1º, II, 241, 241-A, 241-B e 241-C, do Estatuto da Criança e do Adolescente ("Lei nº 8.069/1990"), com as alterações dadas pela Lei nº 11.829/2008, visando o aprimoramento do combate à produção, venda, distribuição, aquisição e posse de pornografia infantil no âmbito digital.

Sobre o assunto, pode-se observar a existência de países com uma melhor regulação penal. Por exemplo, a Argentina pode ser considerada uma das nações da América Latina mais avançadas em matéria de proteção de dados pessoais. De fato, com a edição da *Ley de Protección de Datos Personales* (PDPA), isto é, a *Ley 25.326/2000*, foi feita a compatibilização normativa da proteção de dados com os mais avançados

19 EXPOSIÇÃO DE MOTIVOS DA LGPD-PENAL..., cit., p. 33.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

sistemas jurídicos, como, *v.g.*, o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, considerado o mais robusto do mundo.[20] Demais disso, a PDPA incluiu, no Código Penal da Argentina, tipos penais voltados à proteção de dados (arts. 117-*bis* e 157-*bis*).

5. A PROTEÇÃO DE DADOS PESSOAIS DIANTE DO PODERIO DAS CORPORAÇÕES

Diante do que foi até aqui apresentado, os brasileiros não podem fechar os olhos para os graves abusos na indevida utilização de dados pessoais, que têm sido praticados por grandes corporações – as chamadas *Big Techs.* Na verdade, elas se aproveitariam não somente da anomia de tipos penais direcionados à proteção de dados pessoais, mas, igualmente, da igual ausência de previsão da responsabilidade penal da pessoa jurídica frente aos riscos – e efetivas lesões – contra esse bem jurídico-penal.[21]

Como bem observado por um dos mais emblemáticos *whistleblowers* dos tempos recentes – Edward Snowden –, acerca do panorama derivado da vigilância massiva do mundo on-line:

> "A pressa inicial de transformar o comércio em comércio eletrônico levou rapidamente a uma bolha e, logo depois da virada do milênio, a um colapso. Depois disso, as empresas perceberam que as pessoas que acessavam a Internet estavam muito menos interessadas em gastar do que em compartilhar, e que a conexão humana que ela possibilitava podia ser monetizada."[22]

Nesse terreno, Celso Antonio Pacheco Fiorillo e Christiany Pegorari Conte analisam a tutela penal dos dados pessoais no âmbito daquilo que integraria o chamado "meio ambiente digital". Segundo

20 Entre os países latino-americanos, apenas a Argentina e o Uruguai possuem decisões de adequação às regras da União Europeia para transferências internacionais de dados pessoais — um dos sistemas mais maduros em proteção de dados. Essas decisões permitem o fluxo transfronteiriço livre entre sistemas jurídicos com níveis compatíveis de proteção às informações pessoais. EUROPEAN COMMISSION. *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection*. Disponível em: <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em: 09.01.2025.

21 Detalhadamente sobre o assunto: SOUZA, Artur de Brito Gueiros. *Tratado de Direito Penal Econômico e Empresarial.* São Paulo: Tirant lo Blanch, 2025, ***passim.***

22 SNOWDEN, Edward. *Eterna vigilância. Como montei e desvendei o maior sistema de espionagem do mundo.* São Paulo: Planeta do Brasil, 2019, p. 10.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

os Autores, a Constituição Federal contemplaria, nos arts. 220 a 224, vetores fundamentais que deveriam ser observados pelo legislador penal. Vale dizer, é preciso proteger a sociedade digital, estabelecendo marcos penais para velar, adequadamente, as informações produzidas pelas interações humanas realizadas através dos computadores e outros componentes eletrônicos.[23]

Efetivamente, o meio ambiente digital trataria, no nosso ordenamento jurídico, dos deveres, direitos, obrigações e regime de responsabilidades inerentes à manifestação de pensamento, criação, expressão e informação, realizados pela pessoa humana com a ajuda de computadores. Fiorillo e Conte aduzem, ainda, que o pleno exercício desses direitos deve ser assegurado aos brasileiros e estrangeiros residentes no País, nos termos dos princípios constitucionais fundamentais.[24]

Diante disso, o dever de regular a responsabilidade penal da pessoa jurídica exploradora do meio ambiente digital estaria positivado pela citada garantia do direito à proteção dos dados pessoais (em especial os dados digitais). Da mesma maneira, pela atribuição à União Federal da organização e fiscalização da proteção e do tratamento de dados pessoais, nos termos da lei (art. 21, inc. XXVI, CF/1988), bem como pela prerrogativa de legislar privativamente sobre a proteção de dados pessoais (art. 22, inc. XXX, CF/1988).

Na mesma direção, a mencionada Convenção de Budapeste – como visto, já vigorante no País –, institui a responsabilidade penal corporativa, pelos crimes definidos no seu *corpus*. De fato, o art. 12, n. 1, da Convenção, prevê a punição do ente moral, quando a infração for cometida em seu benefício por qualquer pessoa física em posição de direção, que atue individualmente ou como integrante de um órgão da própria pessoa jurídica, como base: (1) no poder de representação da pessoa jurídica; (2) na autoridade de tomar decisões em nome da pessoa jurídica; e (3) na autoridade de exercer controle interno na pessoa jurídica.

23 FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. *Crimes no meio ambiente digital e a sociedade da informação.* 2ª ed. São Paulo: Saraiva, 2016, pp. 19-20.

24 *Idem,* p. 21.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

Como se pode observar, cuida-se de imputação penal por intermédio do modelo de heterorresponsabilização. Segundo a doutrina, essa forma de imputação – também denominada de responsabilidade derivada ou vicarial – pressupõe que as empresas são responsabilizadas pelas condutas ilícitas realizadas por seus dirigentes ou prepostos no exercício de suas atividades laborativas. O modelo se funda na concepção de que, como a pessoa jurídica é constituída de agentes individuais que dirigem as suas atividades no ambiente social, sua punição somente pode ser admitida como decorrente da conduta individual de seus integrantes no exercício de seus misteres.[25]

No mesmo sentido, Damásio E. de Jesus e José Antonio Milagre observam que há casos de violação de dados pessoais praticados pelas empresas provedoras de acesso à Internet, visto que, o usuário brasileiro nunca sabe o que existe dentro dos códigos das aplicações disponibilizadas por tais provedores, bem como se estes, de alguma forma, procedem com acesso indevido aos dados dos mesmos. Ademais, os Autores ressaltam que a pessoa jurídica pode responder pela omissão imprópria, nos casos em que o cidadão alerta que está sendo vítima de tentativas de invasão por parte do cliente do provedor, e este nada faz.[26]

6. O *COMPLIANCE* DE DADOS DIGITAIS

Conforme o exposto neste ensaio, há uma demanda político-criminal no sentido da assertiva tutela de dados pessoais no Brasil. Enquanto a (necessária) regulação penal não ganha vida, talvez fosse o caso dos doutrinadores e aplicadores do Direito dirigirem uma atenção especial para as estratégias de *compliance* que, na atualidade,

25 GALVÃO, Fernando. *Teoria do Crime da Pessoa Jurídica.* Belo Horizonte: D'Plácido, 2020, pp. 22-23. Sobre os modelos de imputação penal ao ente moral (heterorresponsabilização, autorresponsabilização e modelos ecléticos), vide: SOUZA, Artur de Brito Gueiros. ***Tratado...***, cit., pp. 399-406.

26 JESUS, Damásio E. de; MILAGRE, José Antonio. *Manual de Crimes Informáticos.* São Paulo: Saraiva, 2016, p. 95.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

têm dominando o espaço jurídico-penal.[27]

Com efeito, o estado da arte da *lex mercatoria* aconselha a necessidade e a importância do *compliance* também nessa temática. Nesse sentido, dispõe a LGPD que, o tratamento de dados pessoais implica em uma série de deveres, para os quais os agentes de tratamento – controladores e operadores – devem adotar programas de governança em privacidade:

> "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais."

Consoante, ainda, os termos da LGPD, o programa de *compliance* de tratamento de dados pessoais deve começar pelo comprometimento do controlador ou operador de dados em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, das normas de boas práticas na proteção e tutela dos dados. De acordo com o art. 45, § 2º da LGPD, as medidas voltadas à segurança e privacidade dos dados pessoais devem ser adotadas desde a concepção de produtos e serviços até a sua execução.

Por oportuno, esclarece-se que o dispositivo em destaque reforça o postulado internacionalmente conhecido como *Privacy by Design*, idealizado, ainda nos anos 1990, por Ann Cavoukian – Comissária de Privacidade de Ontário/Canadá – envolvendo sete

27 Considera-se ***compliance*** (ou integridade) como sendo o conjunto de medidas de autocontrole ou de autovigilância adotadas por empresas, consoante as diretrizes fixadas pelo poder público, para que seus dirigentes e empregados cumpram com as normativas, tanto internas como externas, objetivando a evitação de infrações de diversas ordens, inclusive as de natureza criminal. O ***compliance*** também compreende os protocolos de investigação de infrações já ocorridas, sancionando-se, internamente, os seus responsáveis, bem como comunicando tais ocorrências aos órgãos fiscalizadores estatais. (SOUZA, Artur de Brito Gueiros. ***Programas de compliance e a atribuição de responsabilidade individual nos crimes empresariais. In*** Revista Portuguesa de Ciência Criminal. Núm. 1-4, 2015, p. 118).

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

princípios nevrálgicos a esta metodologia:

> "(1) *Proativo, não reativo; preventivo, não corretivo*: A privacidade deve ser antecipada e prevenida antes de que ocorram problemas. O foco está na prevenção de violações de privacidade, não na correção posterior. (2) *Privacidade como configuração padrão*: Os sistemas devem garantir que os dados pessoais estejam automaticamente protegidos, sem que o usuário precise tomar nenhuma ação. A privacidade é o estado padrão, não é algo que precisa ser ativado. (3) *Privacidade incorporada ao design*: A privacidade deve ser uma parte essencial da arquitetura do sistema, não um aspecto opcional. Deve ser considerada desde o início do processo de design, e não adicionada posteriormente. (4) *Funcionalidade total; ganhos positivos e soma positiva, não soma zero*: A implementação da privacidade não deve sacrificar a funcionalidade ou outros interesses. O objetivo é criar soluções que beneficiem todas as partes envolvidas, evitando o que se chama de *trade-offs* entre privacidade e outros valores. (5) *Segurança de ponta a ponta; proteção completa do ciclo de vida dos dados*: A proteção de dados deve ocorrer durante todo o ciclo de vida da informação, desde a coleta até a exclusão, com fortes medidas de segurança para garantir a proteção contínua. (6) *Visibilidade e transparência; manter-se aberto*: As práticas e políticas em torno da privacidade devem ser visíveis, claras e verificáveis. Usuários e interessados devem ser capazes de verificar como os dados estão sendo protegidos. (7) *Respeito pela privacidade do usuário; foco no usuário*: Todas as decisões e processos devem ser centrados nos interesses e direitos dos usuários, garantindo que suas informações pessoais sejam tratadas com respeito."[28]

Ademais, o *compliance* digital deve contemplar mecanismos de supervisão, com planejamento de respostas para incidentes e remediação de problemas, além de atualização constante, nos termos do respectivo código de conduta ética.

Por fim, para a efetivação do programa e do plano de cumprimento normativo em matéria de dados pessoais, a LGPD prevê a figura do Encarregado pela Proteção de Dados (*Data Protection Officer* ou DPO). Trata-se de outra terminologia para oficial de *compliance*, prevendo-se que ele deve não somente colocar em prática o programa de governança em privacidade, como deve, igualmente, atuar na

28 CAVOUKIAN, Ann. *Privacy by design: the 7 foundational principles. In* hppt://www.ipc.on.ca/wp-content/uploads/resouces/7foundationalprinciples.pdf). Acesso em: 09/01/2025. (grifou-se).

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

relação triangular, como canal de comunicação entre o controlador, os titulares de dados e a Autoridade Nacional de Proteção e Dados.[29]

7. CONSIDERAÇÕES FINAIS

À guisa de conclusão, observa-se que a intersecção entre a tutela da proteção de informações sensíveis e o Direito Penal possuem nuances de relevo. Muito embora a atual sistemática outorgada pela LGPD não tenha trazido, de forma ampla, a sua aplicação no âmbito das atividades desenvolvidas na esfera penal, o País passa por um notável avanço, particularmente em atenção ao desenvolvimento de mecanismos eficazes de *compliance* empresarial e a responsabilização dos grandes agentes do setor privado.

Nesse prisma, os contornos da confluência do sistema criminal com a proteção de dados pessoais é um edifício em construção. Ele subirá, tijolo a tijolo, por intermédio dos mecanismos de respeito à cidadania digital e de valoração das atividades de tratamento de dados no País.

REFERÊNCIAS

AMENO, Fernando. *Farra com dados. Uso de ferramenta que cruza conexões do Facebook e dados da polícia explode no país*. Disponível em: <https://www.intercept.com.br/2024/03/12/uso-de-ferramenta-que-cruza-conexoes-do-facebook-e-dados-da-policia-explode-no-pais/>. Acesso em: 09/01/2025.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. *Balanço 4 anos*. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/anpd-balanco-4-anos.pdf>. Acesso em: 09/01/2025.

29 GUEIROS, Pedro Teixeira; DALESE, Pedro. *A LGPD (13.709/18) e o sistema de proteção de dados pessoais do Brasil*. *In* https://www.migalhas.com.br/depeso/334641/a-lgpd--13-709-18--e-o-sistema-de-protecao-de-dados-pessoais-do-brasil. Acesso em: 09/01/2025.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

BRASIL. *Código Penal*. Decreto-Lei nº 2.848/1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 09.01.2025.

BRASIL. *Constituição da República Federativa do Brasil*. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 09.01.2025.

BRASIL. *Decreto nº 11.491/2023*. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 09/01/2025.

BRASIL. *Decreto nº 11.856/2023. Dispõe sobre a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança e institui o Comitê Nacional de Cibersegurança*. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 09/01/2025.

BRASIL. *Lei Geral de Proteção de Dados*. Lei nº 13.709/2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 09.01.2025.

BRASIL. *Marco Civil da Internet*. Lei nº 12.965/2014. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 09.01.2025.

CAVOUKIAN, Ann. *Privacy by design: the 7 foundational principles. In* hppt://www.ipc.on.ca/wp-content/uploads/resouces/7foundationalprinciples.pdf. Acesso em: 09/01/2025.

EUROPEAN COMMISSION. *Adequacy decisions: How the EU determines if a non-EU country has an adequate level of data protection*. Disponível em: <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em: 09.01.2025.

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

EXPOSIÇÃO DE MOTIVOS DA LGPD-PENAL. (Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal), *passim*. Disponível em https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 09/01/2025.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. *Crimes no meio ambiente digital e a sociedade da informação.* 2ª ed. São Paulo: Saraiva, 2016.

GALVÃO, Fernando. *Teoria do Crime da Pessoa Jurídica.* Belo Horizonte: D'Plácido, 2020.

GRABOSKY, Peter. *Cybercrime. Keynotes in Criminology and Criminal Justice Series.* New York: Oxford University Press, 2016.

GUEIROS, Pedro Teixeira. *Internet e consentimento: autogestão de dados e exercício do controle informacional*. São Paulo: Tirant Lo Blanch, 2024.

GUEIROS, Pedro Teixeira; DALESE, Pedro. *A LGPD (13.709/18) e o sistema de proteção de dados pessoais do Brasil*. *In* https://www.migalhas.com.br/depeso/334641/a-lgpd--13-709-18--e-o-sistema-de-protecao-de-dados-pessoais-do-brasil. Acesso em: 09/01/2025.

JESUS, Damásio E. de; MILAGRE, José Antonio. *Manual de Crimes Informáticos.* São Paulo: Saraiva, 2016.

MARTINS, Laís. *14 fotos por ser humano. Exclusivo: em reuniões secretas, Clearview ofereceu 3 bilhões de imagens de brasileiros para polícias e Ministério da Justiça*. Disponível em: <https://www.intercept.com.br/2023/05/16/em-reunioes-secretas-clearview-policias-ministerio-da-justica/>. Acesso em: 09/01/2025.

NAKAMURA, João. *Brasil é vice-campeão em ataques cibernéticos, com 1.379 golpes por minuto, aponta estudo*. Disponível em: <https://

DOI: 10.62009/Emeron.2764.9679n35/2025/413/p184-200

www.cnnbrasil.com.br/economia/negocios/brasil-e-vice-campeao-em-ataques-ciberneticos-com-1-379-golpes-por-minuto-aponta-estudo/>. Acesso em: 09/01/2025.

SNOWDEN, Edward. *Eterna vigilância. Como montei e desvendei o maior sistema de espionagem do mundo.* São Paulo: Planeta do Brasil, 2019.

SOUZA, Artur de Brito Gueiros. *Tratado de Direito Penal Econômico e Empresarial.* São Paulo: Tirant lo Blanch, 2025.

_____. *Programas de compliance e a atribuição de responsabilidade individual nos crimes empresariais. In* Revista Portuguesa de Ciência Criminal. Núm. 1-4, 2015.

UNIÃO EUROPEIA. *Regulamento Geral sobre a Proteção de Dados (RGPD)*. Disponível em https://eur-lex.europa.eu/PT/legal-content/summary/general-data-protection-regulation-gdpr.html. Acesso em: 09/01/2025.

WARREN, Samuel; BRANDEIS, Louis. *The Right of Privacy. In* Harvard Law Review. N. 4, 1890.