COLOMBO, Cristiano; ENGELMANN, Wilson. *Novas tecnologias e o princípio da centralidade da pessoa humana*: Anais do XIII Congreso Iberoamericano de Investigadores y Docentes de Derecho e Informática. São Leopoldo, RS: Casa Leiria, 2023.

# A PERSPECTIVA BRASILEIRA DE UM DIREITO FUNDAMENTAL À CONFIDENCIALIDADE E INTEGRIDADE DOS SISTEMAS INFORMACIONAIS

*Alisson Alexsandro Possa*[1]
*Bruna de Souza Nunes*[2]
DOI 10.29327/5321162.1-14

**Resumo**: O artigo aborda os desdobramentos da Revolução Industrial 4.0, que abriram portas para a ocorrência de crimes digitais e ameaças diretas aos sistemas digitais. Nesse cenário, a tarefa de aplicar as leis no âmbito digital tem se mostrado uma empreitada complexa para os Estados. O ato de invadir sistemas, tanto por agentes criminosos quanto por entidades estatais em busca de investigação, tornou-se uma prática corriqueira, tendo em vista a obtenção de dados pessoais ou corporativos, suscitando, por sua vez, inquietações concernentes à privacidade e à legalidade. No âmago do texto, explora-se os riscos atuais decorrentes dessa conjuntura, enaltecendo-se o papel das estruturas constitucionais ante a ascensão tecnológica. Além disso, realiza-se uma análise dos direitos fundamentais no contexto brasileiro, notadamente a importância da confidencialidade e integridade dos sistemas informacionais, tendo em vista que a proteção de dados emerge como um direito fundamental crucial. A abordagem avança para a investigação mais detalhada da salvaguarda da confidencialidade e integridade dos sistemas de informação. Examinam-se os limites desses direitos fundamentais à luz de de-

1 Advogado, Mestre em Direito Constitucional pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP), Lattes: http://lattes.cnpq.br/1795396755751129.

2 Advogada, Mestranda em *Law and Security* pela NOVA *School of Law* – Lisboa. Lattes: http://lattes.cnpq.br/7808800167110429

cisões judiciais e visões acadêmicas, objetivando equilibrar as demandas de segurança, privacidade e legalidade. O desafio reside em abordar as implicações decorrentes das tecnologias emergentes na sociedade contemporânea, estabelecendo um panorama que considera os diversos fatores em jogo.

**Palavras-chave**: Direitos Fundamentais. Proteção de Dados Pessoais. Direito Comparado.

## 1. INTRODUÇÃO

As novas tecnologias da Revolução Industrial 4.0 permitiram que atividades criminosas sejam realizadas via meios digitais e até mesmo a criação de crimes contra a estrutura de sistemas digitais. Ao mesmo tempo, os Estados passaram a verificar dificuldades para fazer valer seus ordenamentos jurídicos nesse espaço digital, seja no âmbito criminal, seja em outras áreas do Direito.

Nesse cenário, a invasão de sistemas informacionais, seja por criminosos, seja por forças estatais com fim de investigações, passaram a ser necessidade para o alcance dos fins. Essas invasões permitem acesso à dados que podem ser pessoais ou corporativos, caracterizados como segredos da atividade, e podem ser utilizados para finalidades ilícitas por criminosos ou para investigações de ilícitos pelo Estado.

Técnicas para a invasão, através de sistemas maliciosos (*malwares)* ou engenharia social, passaram a ser cotidiano dos indivíduos e das empresas, tentando identificar aquelas práticas que são verdadeiras daquelas que podem levar a danos. Recentemente, foi noticiado que o Brasil se tornou o segundo país mais afetado por ataques criminosos, segundo levantamentos de empresa de cibersegurança[3].

Por outro lado, o Estado passou a buscar técnicas periciais que permitem quebrar as barreiras de sistemas informacionais, tanto aquelas estabelecidas pelos fabricantes e

3 DEMARTINI, Felipe. Brasil foi o segundo país mais atingido por ransomware em 2022. Canaltech, 2 maio 2023. Disponível em: https://canaltech.com.br/seguranca/brasil-foi-o-segundo-pais-mais-atingido-por-ransomware-em-2022-248304/. Acesso em: 1 out. 2023.

desenvolvedores quanto aquelas estabelecidas pelos próprios usuários (como criptografia, verificação de dois fatores etc.). Inúmeras reportagens demonstram que existem empresas que fornecem sistemas voltados para a quebra desses mecanismos aos órgãos de investigação e segurança pública[4].

Entretanto, ainda que essas técnicas sejam utilizadas pelo Estado para a solução de crimes, questões acerca dos limites passam a surgir quando os órgãos públicos buscam contratar esses sistemas sem critérios de utilização que sejam claros ou que podem ser utilizados para vigilância de críticos a um determinado governo. O exemplo internacional que chama atenção é o *software* Pegasus, da empresa israelense NSO Group, e que chegou a participar de licitações no Brasil[5].

Essa situação chegou a ser objeto de discussão pelo Tribunal Constitucional da Alemanha nas Decisões de 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07, analisando a possibilidade de agentes de investigação acessarem e monitorarem sistemas informacionais[6]. A decisão levou ao reconhecimento de um direito fundamental à integridade e confidencialidade dos sistemas informacionais pelo Tribunal, declarando que tais medidas eram incompatíveis com o direito geral da personalidade da Constituição Federal da Alemanha.

Com o avanço da interconexão de objetos através da internet (internet das coisas), a manipulação de sistemas informacionais para alcançar objetivos que vão de encontro aos direitos dos cidadãos também passa a ser possibilidade para outros agentes privados. Recentemente uma empresa de crédito no Brasil passou a forçar seus clientes a instalarem

4 Ver FANTINATO, Giovanna. Cellebrite: conheça o software usado na investigação do caso Henry. *TecMundo*, 12 abr. 2021. Disponível em: https://www.tecmundo.com.br/software/215422-cellebrite-conheca-software-usado-investigacao-caso-henry.htm. Acesso em: 1 out. 2023. Também, ver RIBEIRO, Gabriel F. Perícia em Celular: Como é feita, quais as ferramentas e mais. *Tilt Uol*, 8 fev. 2021. Disponível em: https://www.uol.com.br/tilt/reportagens-especiais/pericia-em-celular-como-e-feita-quais-as-ferramentas-e-mais-/. Acesso em: 1 out. 2023.

5 VALENÇA, Lucas. Empresa de software espião Pegasus abandona licitação do governo. *UOL*, 25 maio 2021. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/25/empresa-de-software-espiaopegasus-deixa-edital-que-e-rodeado-de-incertezas.htm. Acesso em: 1 out. 2023.

6 1 BvR 370/07, 1 BvR 595/07.

um aplicativo no celular que, no caso de não pagamento das parcelas, realizava o bloqueio de todas as funcionalidades do celular[7].

Nesse contexto, o presente artigo pretende analisar uma perspectiva brasileira de proteção constitucional contra invasões à sistemas informacionais, tendo em consideração a previsão da proteção de dados pessoais como um direito fundamental previsto no art. 5°, inciso LXXIX da Constituição do Brasil.

Em um primeiro momento será analisada a possibilidade de reações jurídicas perante novos riscos à direitos e liberdades que surgem de novas tecnologias.

O primeiro capítulo abordará riscos atuais que os acessos à sistemas informacionais em sua estrutura de armazenamento e comunicação podem gerar contra direitos fundamentais e o papel das construções constitucionais nesse contexto da evolução tecnológica.

O segundo capítulo irá analisar os direitos fundamentais reconhecidos no Brasil que estão no contexto de acesso à sistemas informacionais e como eles se relacionam com a quebra de confidencialidade e integridade.

Por fim, o terceiro capítulo irá analisar a construção dogmática de uma proteção da confidencialidade e integridade dos sistemas de informação. Essa análise será baseada nos limites de direitos fundamentais existentes e na visão do professor Wolfgang Hoffman-Riem sobre o conteúdo da decisão do Tribunal Constitucional da Alemanha de 27 de fevereiro de 2008.

## 2. RISCOS APRESENTADOS PELA VIOLAÇÃO À SISTEMAS INFORMACIONAIS

As fontes de riscos à violação dos sistemas que têm o potencial de prejudicar os indivíduos no contexto do exercício

7 MIGALHAS. Financeira é proibida de usar app que bloqueia celular de inadimplente, Migalhas Quentes. 18 jul. 2023. Disponível em: https://www.migalhas.com.br/quentes/390177/financeira-e-proibida-de-usar-app-que-bloqueia-celular-de-inadimplente. Acesso em: 1 out. 2023.

de seus direitos e que serão examinadas são aquelas decorrentes de ataques criminosos ou do próprio Estado por meio de atividades de vigilância.

Os ataques contra os sistemas informáticos que afetam a confidencialidade, integridade e disponibilidade de dados pessoais prejudicam cada vez mais setores da sociedade, seja no âmbito do Estado, empresas privadas, ou uso particular de tecnologias. Com isso, surge a necessidade controlar e reduzir a ocorrência destes eventos adversos por meio ferramentas jurídicas que garantam a proteção das informações pessoais dos indivíduos.

Com a evolução dos sistemas tecnológicos, criminosos buscam aprimorar suas técnicas de ataque cibernético para aumentar suas possibilidades lucrativas. Assim como a tecnologia, o cibercrime evoluiu com o tempo. Antigamente, os ataques de *hackers* eram realizados em servidores localizados nas dependências da vítima por meio eletrônico, com a evolução dos sistemas, é possível roubar, alterar ou criptografar dados de várias vítimas ao mesmo tempo. Esse evento passou a ser permitido pelo uso do mecanismo que chamamos de nuvem, onde os dados, embora tecnicamente sub-segregados, são armazenados[8].

Nesse contexto, quatro novas tecnologias estão ganhando tração e, quando utilizadas em conjunto, estão rompendo estruturas normativas do constitucionalismo contemporâneo: inúmeras bases de dados descentralizadas como consequência do uso massificado da internet; as novas tecnologias denominadas de internet das coisas; Inteligência Artificial e novos atores privados com poderes de gerir o espaço público.

Considerando que os sistemas informacionais passaram a amplificar o exercício de direitos fundamentais através de novos mecanismos[9], esses riscos trazem possíveis danos à direitos fundamentais como o sigilo das telecomunicações,

8 WICKI-BIRCHLER, David. The Budapest Convention and the General Data Protection Regulation: acting in concern to curb cybercrime? *International Cybersecurity Law Review*, n. 1, p. 63-72, 2020. p. 65. Disponível em: https://doi.org/10.1365/s43439-020-00012-5 . Acesso em: 13 jul. 2023.

9 CELESTE, Edoardo; SANTARÉM, Paulo Rená da Silva. Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital. *Revista Brasileira de Direitos Fundamentais & Justiça*, v. 15, n. 45, p. 63-91, 2021. p. 65

proteção ao domicílio e a proteção de dados pessoais. O problema em questão é se esse arcabouço é suficiente para a proteção contra todos os tipos de danos que podem surgir.

Essas violações são conhecidas como incidentes de segurança, eventos de segurança da informação que podem ser definidos como ocorrências descobertas em sistemas, serviços ou status de rede que indiquem possíveis violações da Política de Segurança da Informação, defeito em controles ou situações desconhecidas que possam afetar significativamente a segurança de um sistema[10]

Essas violações podem afetar a integridade, confidencialidade e disponibilidade dos dados de um sistema, incluindo dados pessoais, caso em que o incidente também pode ser definido como uma violação de dados pessoais[11].

Cabe ressaltar que ataques contra o sistema informático já podem resultar em tipo penal, previsto no art. 154-A do Código Penal e descrito como "Invasão de dispositivo informático", tendo como objeto a proteção da privacidade individual[12], uma vez que está inserido no capítulo referente aos "crimes contra a liberdade individual. Considerando que os verbos do tipo penal indicam a perda de integridade, confidencialidade ou disponibilidade dos dados, a proteção se coloca, efetivamente, nos dados gerados pelo sistema, e não à infraestrutura do sistema.

As violações aos dispositivos e sistemas das organizações são cada vez mais comuns, e cada vez mais os criminosos desenvolvem novas formas e meios para cometer crimes. Um exemplo de crime que vem se desenvolvendo são os ataques a computadores com a finalidade de receber resgate. Esse crime é comumente conhecido como *ransomware*[13].

---

10 International Organization for Standardization. International Standard. ISO/IEC 27000:2014: Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2014, p. 5.

11 UNIÃO EUROPEIA. European Data Protection Board. Guidelines 9/2022 on personal data breach notification under GDPR, 2022, p. 7.

12 BITENCOURT, Cezar Roberto. *Código Penal comentado*. 8. ed. São Paulo: Saraiva, 2014. p. 679.

13 O ataque *ransomware* faz parte da família *malware*, que é uma abreviação utilizada para se referir a software malicioso, é uma espécie de programa de computador utilizado para infectar outros dispositivos que podem assumir diversas

O *malware* pode invadir e desativar computadores, dispositivos móveis e sistemas e tem a capacidade de criptografar, roubar ou excluir dados pessoais, dessa forma, os criminosos o utilizam para obter resgate da informação objeto do crime[14].

Os criminosos de *ransomware* estão cada vez mais investindo esforços para desenvolver variantes de *ransomware* mais rapidamente, a fim de torná-los mais difíceis de analisar e fazer engenharia reversa para uma operação mais lucrativa[15].

Posto isto, é possível verificar que os ataques contra a confidencialidade, integridade e disponibilidade de sistemas envolvendo dados passaram a aumentar, e com a evolução dos criminosos e das suas ferramentas tecnológicas, é possível que este cenário crescente se mantenha.

Para as organizações, este tipo de crime além de gerar danos reputacionais, pode levar à quebra de confiança não só por parte dos titulares dos dados pessoais afetados, mas também por parte de potenciais clientes que tiveram conhecimento do incidente. Para os titulares de dados pessoais, os ataquem podem resultar em danos irreparáveis, expondo-os a situações humilhantes e violando seus direitos fundamentais à vida privada e proteção de dados pessoais. Isso resulta na afetação de seu direito à proteção de dados pessoais.

De outro lado, o Estado passou a buscar meios de realizar a invasão de sistemas para o objetivo de investigações criminais, conforme notícias já citadas relativas à contratação de mecanismos que permitem a quebra de criptografia ponta-a-ponta de sistemas de mensagerias ou que ultrapassem barreiras programadas pelos desenvolvedores de aplicações.

---

formas, como vírus (reproduz-se com facilidade, trocando programas e infectando-os com seu código), *worms* (se espalham pelos computadores e podem causar danos destruindo dados e arquivos), *spyware* (ferramenta utilizada para espionar as atividades do usuário no computador e passar informações ao criador do software), entre outros. Ver KASPERSKY. Ransomware: definição, prevenção e remoção. *Kaspery*, [2023?]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 14 jul. 2023.

14 KASPERSKY, [2023?], *op. cit.*

15 CISCO TALOS. Talos Year in Review 2022. *Cisco Talos*, 14 dez. 2022. p. 32-35. Disponível em: https://blog.talosintelligence.com/talos-year-in-review-2022/. Acesso em: 15 jul. 2023.

Esses agentes estatais podem usar o *software* para espionar ou manipular o sistema sem que a pessoa afetada perceba, privando-a da capacidade de se proteger eficazmente.

Tais práticas podem dar ensejo à vigilância em massa e, mecanismo que é amplamente debatido em nossa sociedade, pois a noção de monitoramento generalizado suscita preocupações quanto à preservação da privacidade e liberdades civis[16].

Nesse ponto, a previsão do Código Penal não alcança as atividades dos órgãos investigadores. Assim, o cidadão precisa contar com outras proteções quanto aos danos que derivam dessas práticas.

Ainda, a interconexão de objetos através da internet (internet das coisas) também possibilita que a quebra da confidencialidade e/ou integridade dos dispositivos eletrônicos permita danos não por acesso à dados, mas também por garantir o controle dos dispositivos por parte de outros agentes como forma de induzir comportamentos.[17]

Esse contexto da ubiquidade da internet em todos os aspectos da vida privada e as possíveis interferências foi analisado inclusive pelo Tribunal Constitucional Alemão[18] no julgamento dos casos - 1 BvR 370/07, 1 BvR 595/07Os direitos fundamentais visam garantir a proteção dos direitos da personalidade, a liberdade de comunicação e a inviolabilidade da residência, tanto contra intervenções estatais como de entidades privadas. Nesse sentido, na presença de ameaça a sistemas informacionais e a dados pessoais, a liberdade de desen-

16 RICHARDS, Neil M. The Dangers of Surveillance. *Harvard Law Review*, p. 1955-1956, 2013.

17 As locadoras de carros no Brasil já conseguem bloquear os automóveis locados quando do inadimplemento por parte do consumidor, o que indica a possibilidade futura de que empresas passem a bloquear funções de dispositivos adquiridos pelos consumidores como meio de forçar o adimplemento de obrigações financeiras ou até mesmo a adquirir novos produtos. Ver RIBEIRO, Felipe. Locadoras podem bloquear carros alugados remotamente? *Canaltech*, 8 mar. 2022. Disponível em: https://canaltech.com.br/carros/locadoras-podem-bloquear-carros-alugados-remotamente-210783/. Acesso em: 1 out. 2023.

18 "Additionally, many devices used everyday by large parts of the population involve information technology components. This is increasingly true with regard to telecommunication or electronic devices in homes or motor vehicles, for instance." 1 BvR 370/07, 1 BvR 595/07, p. 7.

volvimento comunicativo é especialmente afetada, pois ela é exercida em conjunto com outras liberdades[19].

Dessa forma, a invasão de sistemas de tecnologia possibilita a alteração dos dados processados no sistema, representando fontes de perigo significativas. Assim, para que seja possível uma proteção efetiva dos direitos fundamentais face à danos que surgem dessas ameaças, também é necessário adotar uma abordagem preventiva, concentrando-se na proteção da infraestrutura utilizada. Isso porque infraestrutura em si também faz parte da garantia do exercício da liberdade[20].

Nesse cenário, diferentes níveis de perigo se apresentam. De acordo com Hoffman-Riem, alguns deles podem ser enfrentados por meio do reconhecimento do direito fundamental à autodeterminação informativa, possivelmente com modificações. Contudo, existem outros perigos que não podem ser enfrentados dessa maneira, pelo menos não de forma que leve em conta adequadamente as particularidades do risco associado ao uso dos sistemas de tecnologia da informação em si[21].

O risco de que tais violações possam facilitar a coleta de dados de maneira mais ampla passa a poder ser mitigado em vários aspectos pelo direito fundamental à proteção de dados pessoais. No entanto, a invasão em sistemas informacionais, além de permitir o acesso a processos de comunicação específicos e a dados individuais, também permite acesso a todos os outros dados arquivados no sistema de comunicação ou acessíveis por meio dele.[22]

A proteção da confidencialidade e integridade de sistemas deve ser aplicável nos cenários em que a intervenção abranja sistemas de informação que, avaliados de forma individual ou em relação às suas capacidades de conexão téc-

19 HOFFMAN-RIEM, Wolfgang. A Proteção Jurídica Fundamental da Confidencialidade e da Integridade dos Sistemas Técnicos de Informação de Uso Próprio. *Revista Direito Público*, Dossiê: Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Penal, v. 18, n. 100, p. 457-499, 2021. p. 462. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6212. Acesso em: 15 jul. 2023.

20 *Ibidem,* p. 462-463

21 *Ibidem,* p. 476-477

22 *Ibidem,* p. 477

nica, contenham informações pessoais do indivíduo em uma amplitude e diversidade que o acesso a esse sistema permita contemplar as várias dimensões da sua vida pessoal ou até mesmo uma representação abrangente da sua personalidade.[23]Assim, é necessário adotar medidas adicionais e aprimorar as estratégias de proteção para garantir a segurança e a privacidade dos indivíduos em um cenário cada vez mais complexo e tecnologicamente avançado.

Outro fator de risco é que a violação supera de forma fundamental e não apenas em casos individuais, os obstáculos técnicos que normalmente serviriam como impedimentos à espionagem ou vigilância. Quando esses obstáculos são superados, a barreira de proteção relacionada ao sistema, que de outra forma precisaria ser repetidamente superada em caso de intervenções no direito à proteção de dados pessoais e contra a qual poderiam ser aplicadas opções de proteção legal, deixa de estar disponível[24].

Essa situação de risco requer consideráveis extensões para abordar efetivamente as novas ameaças apresentadas por essa violação. É necessário enfrentar esse desafio com abordagens inovadoras para garantir a proteção adequada à personalidade em meio a avanços tecnológicos que superam as barreiras tradicionais de proteção.

Por meio de uma violação, é possível a obtenção de um grande banco de dados, desde aqueles que estão na memória permanente, como aquelas que estão distribuídas em outras camadas dos dispositivos e que podem possuir informações sobre vários traços da personalidade. Através dessa violação, é possível obter percepções sobre partes essenciais do estilo de vida de indivíduos, assim como criar perfis sociais, de consumo, de interesses e comportamentais[25].

A possibilidade de violação no sistema também traz consigo o risco de falsificação dos dados individuais registrados e sua combinação com outros dados, o que pode resultar

23 MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *Revista Jurídica Luso-Brasileira*, ano, v. 5, p. 781-809, 2019. p 800.

24 HOFFMAN-RIEM, 2021, *op cit,* p. 479.

25 *Ibidem,* p. 479

na manipulação do cidadão para a criação de uma falsa concepção sobre as informações que são extraídas do sistema, além de induzir possíveis ações prejudiciais.

Possíveis violações da confidencialidade e integridade podem ocorrer em diversos sistemas, seja em ambientes permanentes das residências, como também em dispositivos móveis, como laptops e celulares. Essas violações não se restringem apenas a uma extensão da interferência que o direito fundamental à proteção de dados pessoais garante em seu âmbito, mas constituem uma ameaça independente com características próprias[26]. As medidas essenciais de proteção devem ter início com a salvaguarda do sistema de tecnologia da informação em si, e essa proteção deve se estender aos dados coletados em decorrência da violação, com o objetivo de garantir a sua efetividade.

Assim sendo, torna-se imperativo a implementação de medidas que evitem tais situações e protejam tanto a segurança, quanto a privacidade dos indivíduos afetados. Essa ameaça requer a adoção de medidas preventivas, garantindo a salvaguarda do sistema contra possíveis abusos, bem como a preservação da integridade dos dados e privacidade de todos os usuários.

## 3. OS DIREITOS FUNDAMENTAIS DO ORDENAMENTO BRASILEIRO

A Constituição do Brasil possui as seguintes previsões no art. 5° que podem ser analisadas no contexto da proteção de sistemas informacionais:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial;

26 MENKE, Fabiano, 2019, *op cit,* p. 796-799.

> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Os conceitos do inciso X já foram estudados por Danilo Doneda, que apontou a "falta de uma definição 'âncora'"[27] para a definição exata do conteúdo semântico de cada um. Ele conclui que, apesar de duas terminologias distintas, elas não devem ser valoradas de formas variadas, com base em duas premissas[28]: (i) ausência de determinação da terminologia por parte da doutrina e da jurisprudência, podendo haver o legislador constitucional optar por excesso para garantir o alcance da norma e, (ii) a discussão dogmática sobre os limites dos termos acaba por desviar o foco da norma, que é a proteção do direito fundamental em si.

Certo é que ambos dizem respeito à direitos que condizem com a ideia de exclusão, ou obrigação de não ação, por parte de terceiros, reforçando uma noção individualista da privacidade[29].

Essa mesma tônica de um direito que determina a exclusão de terceiros sobre esferas individuais acompanha os incisos XI, sobre a inviolabilidade da casa, e XII sobre a inviolabilidade das correspondências e conteúdo das comunicações telefônicas.

Ocorre que os sistemas informacionais, se entendidos como meios que amplificam direitos fundamentais, já contam com a atuação de vários atores: desde os fabricantes, que conseguem realizar modificações em tempo real na estrutura (via atualizações ou acesso a logs de uso) até os provedores de aplicações que podem estar incorporados, como no caso de vários aplicativos que utilizam em tempo real o acesso à geo-

27 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Reuthers, 2019. p. 98.

28 *Ibidem*, p. 105.

29 *Ibidem*, p. 104.

localização para seu funcionamento ou como mecanismo de segurança.

Ademais, um direito baseado na exclusão impõe ao seu titular o ônus de análise sobre riscos no caso da concessão de acesso à terceiros, o que, no caso de sistemas informacionais interconectados, é de extrema complexidade que o usuário comum pode não compreender os riscos envolvidos[30].

Já o direito fundamental à proteção de dados pessoais, recém consagrado na Constituição em 2022, tem como seu grande objeto todos os tratamentos[31] que podem ser realizados nos dados pessoais em si[32], o que pode estar dentro do contexto de quebra de confidencialidade e integridade dos sistemas informacionais.

Analisando a decisão do Tribunal Constitucional Alemão, Hofmann-Riem indica as seguintes diferenças entre essas duas proteções[33]:

> As proteções que são possíveis, ou mesmo requeridas, não se limitam, no entanto, a medidas diretamente relacionadas ao processo de coleta de dados e subsequente armazenagem, uso, processamento ou divulgação, mas também se estendem aos pressupostos (organizacionais, procedimentais, sistêmicos, dentre outros) para garantir que tal coleta e subsequentes medidas atendam às exigências ou, conforme o caso, para que sejam encerradas. Aqui se torna claro que a proteção da autodeterminação informativa já começa no nível da ameaça aos direitos fundamentais e pode, portanto, ser alcançada por meio de medidas para reduzir tais amea-

30 A imposição de ônus que demandam conhecimentos especializados e específicos para a compreensão total dos possíveis danos foi consagrada na decisão do Tribunal Constitucional Alemão: "Individuals will not always be able to detect such third-party access; in any case, they have only limited powers to prevent it. Information technology systems have now evolved to such complexity that taking effective social or technical measures of self-protection presents a considerable challenge and may not be feasible at least for the average user." 1 BvR 370/07, 1 BvR 595/07, p.8

31 O Art. 5°, inciso X da Lei n° 13.709/18 define tratamento como: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

32 Segundo o Art. 5°, inciso I da mesma legislação: dado pessoal é toda informação relacionada a pessoa natural identificada ou identificável;

33 HOFFMAN-RIEM, 2021, *op cit,* p. 475.

> ças. Mesmo quando as medidas de proteção – tais como medidas de proteção de dados do sistema75 – estão previstas na coleta de dados, elas são medidas para evitar prejuízos aos dados – elas ocorrem especialmente na forma de controle e design do contexto, mas não na proteção da confiança no funcionamento do sistema de tecnologia da informação em si. **Em outras palavras: a proteção de dados por meio do design do sistema não é idêntica à proteção do sistema de tecnologia da informação (independentemente de as disposições jurídicas para design do sistema serem implementadas nele) contra o acesso ao próprio sistema e o acesso subsequente aos dados. (grifo nosso)**

Ainda que no Brasil não existam decisões suficientes em nível constitucional acerca do alcance da proteção de dados no nível de infraestrutura, se comparado com o repertório de julgamentos na Alemanha, é possível tomarmos como pressuposto essa diferença quando o objetivo do agente que está manipulando o dispositivo acaba por divergir das expectativas esperadas pelo usuário, essencialmente no correto funcionamento do sistema de maneira à garantir a confidencialidade do uso e a confiança na integridade das informações ali armazenadas. Isso garante ameaças à direitos fundamentais que não se colocam no contexto do uso de dados pessoais, mas como consequências da quebra da confiança como cidadão nos usos sistema informacional.

Outro elemento de diferenciação está na capacidade do titular em conhecer os tratamentos realizados e os tipos de dados utilizados. Os sistemas atuais armazenam dados permanentes e temporários em diversas camadas e que permitem danos à personalidade em níveis que os titulares sequer possuem a possibilidade de tomar conhecimento, impedindo a sua autodeterminação[34] através dos seus direitos. A proteção dos sistemas, nesse caso, permite precauções para a perda desse elemento individual.

34 HOFFMAN-RIEM, 2021, *op cit,* p. 467.

## 4. OS SISTEMAS TÉCNICOS DA INFORMAÇÃO COMO CONCEITOS CONSTITUCIONAIS: A PROTEÇÃO DA PERSONALIDADE ATRAVÉS DA PROTEÇÃO DE SISTEMAS INFORMACIONAIS

Foi demonstrado até aqui a visão de que o arcabouço de direitos fundamentais brasileiros, tal como os da Alemanha, talvez não sejam suficientes para uma categoria de danos contra a personalidade que surgem da quebra dos atributos da confidencialidade e integridade de sistemas de uso pessoal.

A Constituição Federal do Brasil, nas disposições do art. 1°, inciso I e III; art. 3º, III e art. 5° caput e §2º, abre uma possibilidade geral de proteção da dignidade humana através de um direito ao "livre desenvolvimento da personalidade"[35], que pode ser utilizado contra qualquer tipo de ameaça ao desenvolvimento dos cidadãos brasileiros. Segundo Ingo Sarlet:

> É possível afirmar que o direito geral de personalidade (ou direito ao livre desenvolvimento da personalidade) implica uma proteção abrangente em relação a toda e qualquer forma de violação dos bens da personalidade, estejam eles, ou não, expressa e diretamente reconhecidos ao nível da constituição[36]

A quebra da confidencialidade e integridade dos sistemas informacionais pode gerar danos ao desenvolvimento individual que vão além de proteções à privacidade e intimidade baseadas em obrigações de ordem negativos, e da proteção de dados, como dimensão da proteção da personalidade que garante mecanismos de ordem positiva, uma vez que os próprios sistemas são mecanismos de formação da personalidade pelo seu papel no exercício de outros direitos fundamentais na atualidade. Assim, o livre desenvolvimento da personalidade se coloca como um direito com função de proteger os "vazios" deixados por dimensões protetivas específicas e autônomas[37].

35 TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. *Temas de direito civil*, v. 3, p. 25, 1999. p. 25.

36 SARLET, Ingo Wolfgang. Direitos Fundamentais em Espécie. *In:* SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*, 10. ed. São Paulo: Saraiva, 2021. p. 196

37 O Tribunal Constitucional Alemão define como "loophole-filling function over

Esse vazio está justamente em um nível anterior à proteção do titular contra a coleta ilegítima de dados pessoais: a personalidade do titular é ameaçada quando o sistema utilizado pode estar sendo alvo de infiltrações por agentes desconhecidos. Nesse sentido:

> Caso o usuário não queira impedir a geração e a coleta de dados, exige-se uma proteção efetiva da personalidade, de modo que o usuário tenha a confiança de que os dados assim obtidos não possam ser utilizados em contextos diferentes e, em particular, por terceiros não autorizados. Porém, por meio da infiltração dos sistemas técnicos de informática, eles podem ser utilizados por quem não está envolvido no processo de comunicação, sem que o interessado possa reconhecer e se proteger[38].

Assim, esse direito protege a personalidade naqueles casos em que qualquer possibilidade de conhecimento do cidadão sobre acessos de terceiros a seus dados armazenados por um sistema complexo é removida completamente pelo fator que as atividades dos terceiros são realizadas com base no sigilo dos acessos aos sistemas e das manipulações que podem realizar.

Há um elemento quantitativo que também retira o âmbito de proteção do direito à proteção de dados pessoais: essas infiltrações não permitem o acesso à dados envolvidos em processos específicos de tratamentos de dados, mas também todo o conjunto de dados armazenados, permanentes ou voláteis, do sistema informacional para além de somente um dispositivo, envolvendo, também, um conjunto complexo de sistemas. Esse caráter quantitativo cria uma situação de danos que estariam além das capacidades protetivas do direito fundamental à proteção de dados pessoais[39].

Essa nova concretização da proteção da dignidade humana para garantir o desenvolvimento da personalidade quando tais riscos são verificados coexiste com o direito à

---

and above its manifestations recognized thus far by virtue of the fact that it guarantees the integrity and confidentiality of information technology systems". 1 BvR 370/07, 1 BvR 595/07, p.32

38 HOFFMAN-RIEM, 2021, *op. cit*, p. 478

39 *Ibidem,* p. 477

proteção de dados pessoais e as outras manifestações do direito à privacidade, garantindo um amplo escopo de proteção com vistas a garantir a segurança no uso de dispositivos interconectados.

## 5. CONCLUSAO

Em uma sociedade cada vez mais dependente de novas tecnologias que permitem a troca de dados gerados pelo uso dos titulares, ainda que sem conhecimento, uma proteção ampla pode ser essencial para impedir não só danos decorrentes de atividades criminosas, mas também para evitar que o Estado abuse dos seus poderes de vigilância social[40].

Uma proteção constitucional à confidencialidade e integridade dos sistemas informacionais como elementos do desenvolvimento da personalidade e concretização da dignidade humana moderniza a autodeterminação informacional da proteção de dados pessoais, alcançando não só agentes públicos, mas também os privados[41].

O artigo demonstrou em um primeiro momento os riscos que a manipulação de sistemas informacionais, através da manipulação ou quebra de protocolos que buscam garantir a confidencialidade e a integridade do seu uso, por agentes estatais e por criminosos, geram aos cidadãos.

Em seguida, foram analisados os direitos fundamentais existentes no ordenamento jurídico brasileiro e seus escopos de proteção: de um lado, aqueles tradicionais que protegem a vida privada com contornos individuais e baseados em mandamentos de ordem negativa e, por outro, a proteção de dados pessoais como uma salvaguarda da personalidade garantida através de estruturas normativas de ordem positiva aos agen-

40 Sempre cabe relembrar as denúncias do programa PRISM pelo ex-agente da Agência Nacional de Segurança dos Estados Unidos, Edward Snowden, demonstram como poderes estatais estão constantemente buscando novos meios de coletar informações de cidadãos conforme os avanços tecnológicos permitem cada vez mais a geração de novos tipos de dados e inferências de comportamentos. Ver GREENWALD, Gleen; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, 7 jul. 2013.

41 MENKE, Fabiano, 2019, *op cit,* p. 807.

tes de tratamentos de dados pessoais. Valendo-se da dogmática do Tribunal Constitucional Alemão e da leitura da doutrina de Wolfgang Hoffman-Riem, chegou-se à uma possível lacuna dessas proteções perante os riscos apresentados.

Por fim, foram traçados contornos do conteúdo de uma proteção da personalidade que identifica como conceito constitucional a confiança nos sistemas informacionais que os usuários depositam na utilização deles para o exercício e desenvolvimento de elementos da sua personalidade.

## REFERÊNCIAS

1 BvR 370/07, 1 BvR 595/07. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/EN/2008/02/rs20080227_1bvr037007en.pdf;jsessionid=296CC715891419CC52FBA909CB7218C6.internet961?__blob=publicationFile&v=6 . Acesso em: 15 ago. 2023.

BITENCOURT, Cezar Roberto. *Código Penal comentado*. 8. ed. São Paulo: Saraiva, 2014.

CELESTE, Edoardo; SANTARÉM, Paulo Rená da Silva. Constitucionalismo digital: mapeando a resposta constitucional aos desafios da tecnologia digital. *Revista Brasileira de Direitos Fundamentais & Justiça*, v. 15, n. 45, p. 63-91, 2021.

CISCO TALOS. Talos Year in Review 2022. *Cisco Talos*, 14 dez. 2022. p. 32-35. Disponível em: https://blog.talosintelligence.com/talos-year-in-review-2022/. Acesso em: 15 jul. 2023.

DEMARTINI, Felipe. Brasil foi o segundo país mais atingido por ransomware em 2022. Canaltech, 2 maio 2023. Disponível em: https://canaltech.com.br/seguranca/brasil-foi-o-segundo-pais-mais-atingido-por-ransomware-em-2022-248304/. Acesso em: 1 out. 2023.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. 2. ed. São Paulo: Reuters, 2019.

FANTINATO, Giovanna. Cellebrite: conheça o software usado na investigação do caso Henry. *TecMundo*, 12 abr. 2021. Disponível em: https://www.tecmundo.com.br/software/215422-cellebrite-conheca-software-usado-investigacao-caso-henry.htm. Acesso em: 1 out. 2023.

GREENWALD, Gleen; MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*, 7 jul. 2013. Disponível em: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. Acesso em: 2 ago. 2023.

HOFFMAN-RIEM, Wolfgang. A Proteção Jurídica Fundamental da Confidencialidade e da Integridade dos Sistemas Técnicos de Informação de Uso Próprio. *Revista Direito Público*, Dossiê: Privacidade e Proteção de Dados Pessoais na Segurança Pública e no Processo Penal, v. 18, n. 100, p. 457-499, 2021. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/6212. Acesso em: 15 jul. 2023.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. International Standard. ISO/IEC 27000:2014: Information technology — Security techniques — Information security management systems — Overview and vocabulary. 2014, p. 5. Disponível em: https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/c063411_ISO_IEC_27000_2014.pdf. Acesso em: 15 jul. 2023.

KASPERSKY. Ransomware: definição, prevenção e remoção. *Kaspery*, [2023?]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/ransomware. Acesso em: 14 jul. 2023.

MENKE, Fabiano. A proteção de dados e o direito fundamental à garantia da confidencialidade e da integridade dos sistemas técnico-informacionais no direito alemão. *Revista Jurídica Luso-Brasileira*, ano, v. 5, p. 781-809, 2019.

MIGALHAS. Financeira é proibida de usar app que bloqueia celular de inadimplente, Migalhas Quentes. 18 jul. 2023. Disponível em: https://www.migalhas.com.br/quentes/390177/financeira-e-proibida-de-usar-app-que-bloqueia-celular-de-inadimplente. Acesso em: 1 out. 2023.

RIBEIRO, Felipe. Locadoras podem bloquear carros alugados remotamente? *Canatech*, 8 mar. 2022. Disponível em: https://canaltech.com.br/carros/locadoras-podem-bloquear-carros-alugados-remotamente-210783/. Acesso em: 1 out. 2023.

RIBEIRO, Gabriel F. Perícia em Celular: Como é feita, quais as ferramentas e mais. *Tilt Uol*, 8 fev. 2021. Disponível em: https://www.uol.com.br/tilt/reportagens-especiais/pericia-em-celular-como-e-feita-quais-as-ferramentas-e-mais-/. Acesso em: 1 out. 2023.

RICHARDS, Neil M. The Dangers of Surveillance. *Harvard Law Review*, p. 1955-1956, 2013.

SARLET, Ingo Wolfgang. Direitos Fundamentais em Espécie. *In:* SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. *Curso de direito constitucional*, 10. ed. São Paulo: Saraiva, 2021.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil-constitucional brasileiro. *Temas de direito civil*, v. 3, p. 25, 1999.

UNIÃO EUROPEIA. European Data Protection Board. Guidelines 9/2022 on personal data breach notification under GDPR. *The European Data Protection Board*, 18 out. 2022. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-92022-personal-data-breach_en. Acesso em: 14 jul. 2023.

VALENÇA, Lucas. Empresa de software espião Pegasus abandona licitação do governo. *UOL*, 25 maio 2021. Disponível em: https://noticias.uol.com.br/politica/ultimas-noticias/2021/05/25/empresa-de-software-espiaopegasus-deixa-edital-que-e-rodeado-de-incertezas.htm. Acesso em: 1 out. 2023.

WICKI-BIRCHLER, David. The Budapest Convention and the General Data Protection Regulation: acting in concern to curb cybercrime? *International Cybersecurity Law Review*, n. 1, p. 63-72, 2020. Disponível em: https://doi.org/10.1365/s43439-020-00012-5 . Acesso em: 13 jul. 2023.