Bruno Freire de Carvalho Calabrich

Proteção de Dados Pessoais

na Investigação Criminal e no Processo Penal

garantismo, eficiência e *standards* de validade

2024

EDITORA JusPODIVM

www.editorajuspodivm.com.br

2

TRATAMENTO DE DADOS PESSOAIS, GARANTISMO E PERSECUÇÃO PENAL NO BRASIL

Os conceitos de "dado pessoal" e de "tratamento de dados pessoais" são amplíssimos (LGPD, art. 5º, I e X). Por isso, do início ao fim, todos os atos de uma investigação criminal e todos os atos de um processo penal são atos de tratamento de dados pessoais. E, para cada um desses atos, devem ser respeitados os direitos fundamentais de seus titulares – mas não só estes.

Uma mão decalcada com o sangue de um animal selvagem numa caverna recém-descoberta por arqueólogos pode conter os dados biométricos de um ser humano morto há centenas de anos. Como não será possível associar esses dados a nenhum titular, sua captação nada dirá sobre alguém, menos ainda a um (outrora inconcebível) direito seu à autodeterminação informativa[1]. Mas uma mão decalcada com sangue, hoje, numa parede, pode servir ao esclarecimento de um ilícito penal. O tratamento dos dados que integram aquele decalque – o contorno, a impressão digital, os componentes genéticos do sangue em que foi impresso – pode ajudar a desvendar a autoria e a materialidade de um crime grave.

Da mesma sorte, quando alguém se apresenta numa delegacia de polícia relatando ter sido vítima de um crime, dá-se início a uma atividade de investigação criminal que exige a coleta – e, portanto, o tratamento – de inúmeros dados pessoais. Tais dados, cujo tratamento é elementar para o desempenho dessa atividade do Estado, são titularizados pela vítima, pelo agente criminoso, por testemunhas e por terceiros que talvez nunca sejam

1. Embora possam incidir sobre esse registro variadas normas, como as que regem a proteção do patrimônio histórico e cultural de uma comunidade.

informados de que, um dia, seus nomes foram mencionados numa investigação (como potenciais suspeitos ou testemunhas, por exemplo). A simples colheita das informações da vítima e sua assinatura ao final do termo de depoimento é um tratamento de dados pessoais. A descrição das características físicas do criminoso, idem.

Todo ato de colheita ou produção de elementos de convicção numa investigação criminal é um tratamento de dados pessoais, eis que será invariavelmente associado a uma pessoa "identificada ou identificável" (art. 5º, I, da LGPD). E todos os atos do processo penal devem ser praticados de modo a proteger direitos fundamentais individuais e de toda a coletividade.

O respeito a direitos fundamentais de réus e investigados pode se dar tanto por ações quanto por omissões do Estado. Das mais comezinhas obrigações, como não torturar e não acusar alguém com base em provas ilícitas, até as obrigações menos evidentes ao olhar leigo mas ínsitas a um processo penal de feições democráticas, como a de não pedir a condenação de alguém se não houver prova suficiente para tanto, o Estado promove direitos fundamentais ao *não agir*. Essa forma de proteção de direitos fundamentais no processo penal está associada aos direitos fundamentais de primeira geração ou dimensão, pela qual se impõe ao Estado uma prestação negativa, uma obrigação de não transpor os limites da esfera de liberdades individuais.

Todavia, ao lado de suas obrigações negativas, cabe também ao Estado atuar, positivamente, sob pena de não garantir direitos fundamentais de forma integral. Assim é que o processo penal deve ser conduzido com eficiência e sob um duplo viés[2]: de proteção de direitos de réus e investigados e, ao mesmo tempo, de preservação de direitos da vítima e de toda a sociedade ao justo sancionamento de quem que tenha praticado um crime.

Tratar dados pessoais no processo penal é uma obrigação processual positiva. Tratar dados pessoais com respeito aos direitos fundamentais dos seus titulares é uma faceta dessa obrigação processual positiva; sua outra faceta, que se opera pelo princípio da finalidade, é o sentido do tratamento dos dados pessoais, que há de sempre estar voltado, se e quando necessário tal tratamento, ao esclarecimento dos fatos tão precisamente quanto possível.

Não se mede a eficiência de um processo penal, nem de cada um dos atos neste praticados, com base na sua utilidade apenas para "fundamentar

2. FISCHER, Douglas; PEREIRA, Frederico Valdez. **As obrigações processuais positivas segundo as Cortes Europeia e Interamericana de Direitos Humanos**. 4. ed. Porto Alegre: Livraria do Advogado, 2023, p. 27.

condenações". A condenação ou absolvição de alguém não é a finalidade do processo penal nem do tratamento de dados que porventura o componha, senão como um produto, axiologicamente indiferente, da certificação dos fatos, sem a qual não será possível ao Estado emitir um juízo responsável sobre a incidência da regra geral e abstrata ao caso concreto – seja para absolver, seja para condenar.

No presente capítulo será estudada a compreensão dual do processo penal e da investigação criminal, sua relação com a proteção de dados pessoais no atual quadro constitucional e legal brasileiros e os principais julgados do STF que têm dado conformação própria à matéria.

2.1 INVESTIGAÇÃO CRIMINAL E PROCESSO PENAL

A persecução penal, atividade do Estado na qual se inserem a investigação criminal e o processo penal, inicia-se com o primeiro ato tendente à verificação de um fato potencialmente criminoso e se estende até quando for possível incidir qualquer consequência de natureza penal acerca desses mesmos fatos. Assim, a persecução penal começa com os primeiros atos de investigação de um ilícito penal (não necessariamente documentadas num inquérito policial, que é apenas uma das espécies de investigação), passando pela denúncia, pela instrução do processo e pela sentença condenatória ou absolutória. A persecução penal também abrange todas as vias recursais e o trânsito em julgado de uma eventual condenação – mas não se encerra aí. A execução penal também está inserida no escopo da persecução penal, assim como também estão inseridos todos os efeitos de uma condenação, enquanto persistirem. Assim, desde os primeiros atos praticados pelo Estado acerca da possível prática de um ilícito penal até o último dos atos do Estado sobre esse ilícito penal que possam trazer consequências para o agente, estar-se-á falando de persecução penal. O último marco legal para a atividade de persecução penal que diga respeito a um fato criminoso específico é dado pelo art. 93 do Código Penal, que trata do instituto da reabilitação e assegura ao condenado "o sigilo dos registros sobre o seu processo e condenação" – e mesmo assim, estará condicionada ao que prevê o art. 95 CP (que trata da possibilidade de revogação da reabilitação "se o reabilitado for condenado, como reincidente, por decisão definitiva, a pena que não seja de multa"[3]).

3. "Art. 94 – A reabilitação poderá ser requerida, decorridos 2 (dois) anos do dia em que for extinta, de qualquer modo, a pena ou terminar sua execução, computando-se o período de prova da suspensão e o do livramento condicional, se não sobrevier revogação, desde que o condenado:

A persecução penal também abrange as ações penais privadas, porquanto o que se delega ao particular é a iniciativa para a deflagração da ação penal (pela queixa), mas jamais o exercício do *jus puniendi,* ou poder-dever de aplicar uma sanção penal a quem tiver cometido um crime.

A definição do que seja o processo penal é extraída de um doloroso e não linear processo histórico que permitiu a positivação, nas Constituições e nas leis atuais, de uma série de direitos (do indivíduo) e de deveres (do Estado – correlatos estes, sempre, a direitos individuais ou transindividuais), e que pode ter como resultado a aplicação de uma pena a quem tiver praticado um crime (embora não seja esse exatamente seu *objetivo*).

Do ponto de vista procedimental, o processo penal é uma sequência de atos ordenados no tempo e destinados a um fim (a prolação de uma sentença), iniciada a partir da imputação formal de um crime a alguém. Do ponto de vista instrumental, o processo penal é um complexo de relações jurídicas (ou jurídico-processuais) envolvendo diversos sujeitos (juiz, acusador, réu e seu defensor, dentre outros) e que tem como propósito a proteção de diretos fundamentais, inclusive (mas não necessariamente) pela aplicação, se for o caso, de uma sanção penal.

De acordo com Luigi Ferrajoli:

> O que faz do processo uma operação distinta da justiça com as próprias mãos ou de outros métodos bárbaros de justiça sumária é o fato que ele persegue, em coerência com a dúplice função preventiva do direito penal, duas diferentes finalidades: a punição dos culpados juntamente com a tutela dos inocentes. É essa segunda preocupação que está na base de todas as garantias processuais que circundam o processo e que condicionam de vários modos as instâncias repressivas expressas pela primeira. A história do processo penal pode ser lida como a história do conflito entre essas duas finalidades, logicamente complementares, mas na prática contrastantes[4].

I – tenha tido domicílio no País no prazo acima referido;

II – tenha dado, durante esse tempo, demonstração efetiva e constante de bom comportamento público e privado;

III – tenha ressarcido o dano causado pelo crime ou demonstre a absoluta impossibilidade de o fazer, até o dia do pedido, ou exiba documento que comprove a renúncia da vítima ou novação da dívida.

Parágrafo único – Negada a reabilitação, poderá ser requerida, a qualquer tempo, desde que o pedido seja instruído com novos elementos comprobatórios dos requisitos necessários.

Art. 95 – A reabilitação será revogada, de ofício ou a requerimento do Ministério Público, se o reabilitado for condenado, como reincidente, por decisão definitiva, a pena que não seja de multa."

4. FERRAJOLI, Luigi. **Direito e razão**: teoria do garantismo penal. Trad. Luis Flávio Gomes et al. São Paulo: RT, 2002, p. 483.

O Código de Processo Penal também não define o que é *investigação criminal*. Diversamente, refere-se ao que chama de "fase de investigação" (arts. 3-A e 3-D) e enumera atos a serem praticados pela autoridade policial num inquérito (art. 6º e ss. do CPP) – que é apenas uma das diversas espécies de investigação estatal.

Investigações classificam-se em estatais e privadas. Elementos de convicção que interessam a uma (eventual) acusação criminal podem ser colhidos ou produzidos com esse foco específico – como é o caso das investigações criminais realizadas pela polícia ou pelo Ministério Público – ou por outros entes do Estado que tenham atribuição para apurar os mesmos fatos, embora sob outro enfoque – como nas apurações realizadas por órgãos fazendários e ambientais. Tais apurações prestam-se validamente, quaisquer destas, à persecução penal, desde que conduzidas por autoridades dotadas de atribuição legal para tanto e respeitados os direitos do investigado. As investigações privadas, como as realizadas por particulares ou por profissionais do jornalismo, distinguem-se das investigações estatais por lhes faltarem os atributos da *imperatividade*, da *exigibilidade* e (quando for o caso) da *(auto)executoriedade*, próprios dos atos administrativos[5].

Para investigação criminal, adota-se aqui a definição que já propusemos antes: é a sequência de atos preliminares direta ou indiretamente voltados à produção e à colheita de elementos de convicção e de outras informações relevantes acerca da materialidade e autoria de um fato criminoso[6].

Eventualmente, a investigação poderá exigir a obtenção de informações diversas não diretamente vinculadas ao fato criminoso que se pretenda apurar, mas ainda assim úteis a essa apuração. Quando necessário, por exemplo, a autoridade responsável pode empreender diligências para localizar uma testemunha; é também sua atribuição colher a qualificação completa de todos, sobretudo do investigado. Daí a alusão não só a *elementos de convicção*, mas também a *outras informações relevantes*.

É também preferível a expressão *elementos de convicção* a *provas*: enquanto não submetidos ao contraditório, os elementos informativos não

5. Discorre-se com mais vagar sobre cada uma destas espécies de investigação em CALABRICH, Bruno Freire de Carvalho. **Investigação criminal pelo Ministério Público**: fundamentos e limites constitucionais. São Paulo: RT, 2007, pp. 65-70.

6. CALABRICH, Bruno Freire de Carvalho. **Investigação criminal pelo Ministério Público**: fundamentos e limites constitucionais. São Paulo: RT, 2007, p. 54.

podem ser utilizados validamente num processo e, portanto, não podem ser consideradas provas em sentido estrito.

É importante mencionar que, no processo penal, não existe exatamente um "processo cautelar", com o sentido de "processo preparatório" da ação principal, como existe no processo civil. Não existem, no que se convencionou identificar como "medidas cautelares do processo penal", elementos da tradicional da teoria geral do processo como *demanda, partes legitimadas* e *pedido*[7]. De acordo com o art. 282 do CPP, nos casos de *urgência ou de perigo de ineficácia da medida*, nem mesmo se reconhece ao réu ou investigado o direito ao contraditório prévio a sua decretação; nessa hipótese, devem *ser justificados e fundamentados em decisão que contenha elementos do caso concreto* a urgência ou o risco de ineficácia da medida.

Mesmo que não se as classifiquem como processos de natureza cautelar propriamente dita, uma das características das medidas cautelares do processo penal é precisamente sua *jurisdicionariedade*, *i.e.,* a necessidade de que sejam decretadas pelo Poder Judiciário. Há, contudo, exceções. A lei Maria da Penha (Lei nº 11.340/06) prevê ser possível a decretação de medidas protetivas pela autoridade policial (art. 12-C[8]). Além disso, o art. 342 do CPP prevê o arbitramento da fiança pelo delegado de polícia[9] para crimes com pena máxima igual ou inferior a 4 anos. De qualquer modo, mesmo nessas específicas situações em que a medida pode ser determinada por uma autoridade administrativa (o delegado de polícia), é imprescindível sua submissão para confirmação do Poder Judiciário, sem o que a medida será tornada ilegal e deve perder seus efeitos.

---

7. OLIVEIRA, Eugenio Pacelli de. **Curso de processo penal**. 27. ed. Salvador: Juspodivm, 2023, p. 416.

8. "Art. 12-C. Verificada a existência de risco atual ou iminente à vida ou à integridade física ou psicológica da mulher em situação de violência doméstica e familiar, ou de seus dependentes, o agressor será imediatamente afastado do lar, domicílio ou local de convivência com a ofendida:

   I – pela autoridade judicial;

   II – pelo delegado de polícia, quando o Município não for sede de comarca; ou

   III – pelo policial, quando o Município não for sede de comarca e não houver delegado disponível no momento da denúncia.

   § 1º Nas hipóteses dos incisos II e III do *caput* deste artigo, o juiz será comunicado no prazo máximo de 24 (vinte e quatro) horas e decidirá, em igual prazo, sobre a manutenção ou a revogação da medida aplicada, devendo dar ciência ao Ministério Público concomitantemente."

9. "Art. 322. A autoridade policial somente poderá conceder fiança nos casos de infração cuja pena privativa de liberdade máxima não seja superior a 4 (quatro) anos.

   Parágrafo único. Nos demais casos, a fiança será requerida ao juiz, que decidirá em 48 (quarenta e oito) horas."

Os interesses dos titulares dos dados e o interesse público não são necessariamente contrapostos. Em primeiro lugar, e para muito além do processo penal, porque a proteção de dados pessoais é também de interesse público: uma economia livre e equilibrada e uma democracia hígida pressupõem o respeito à autodeterminação informativa. Quanto ao titular de dados pessoais que ocupa a posição de investigado ou acusado num processo penal, é de seu interesse o respeito a seu direito fundamental à autodeterminação informativa tanto quanto é de interesse público que seja respeitado seu direito à autodeterminação informativa. Não é de interesse público que o processo penal se desenvolva violando direitos.

Por outro lado, é certo que todo réu pode ter interesse em resistir a uma pretensão (como a do Estado-acusação, quando lhe impute a prática de um crime), mas esse interesse só será legítimo – e, portanto, só deverá ser acolhido pelo Estado-juiz – se amparado numa norma jurídica. Nem toda resistência a uma pretensão será legítima.

O Estado poderá tratar dados pessoais no processo penal apenas se houver base legal para fazê-lo. Impedir o tratamento de seus dados ou dos dados pessoais de terceiros num processo penal pode ser de interesse de um réu como estratégia para resistir a uma pretensão, mas esse interesse só será legítimo (*i.e.*, só será tutelado pelo direito) se houver razões que denotem ausência de amparo legal para a atividade do Estado. Obstar o tratamento de dados no processo penal, por si só e sem fundamento legal ou constitucional, não é do interesse público. Muito ao revés: tratar dados pessoais, quando necessário para uma investigação ou um processo, é um interesse público e uma obrigação processual positiva do Estado – como se discorrerá adiante.

2.1.1 Cibercrimes

O crime de fraude eletrônica é uma espécie de estelionato praticado "com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo". Esse tipo penal foi criado pela Lei nº 14.155/21, que acrescentou o parágrafo §2º-A ao art. 171 do Código Penal. Os estelionatos em meio eletrônico, cujos dados disponíveis excluem cinco das mais populosas Unidades da Federação do país (BA, CE, RJ, RS e SP), tiveram registradas pelas polícias brasileiras 200.322 ocorrências em 2022 – um aumento de 65,2%

em relação a 2021[10], quando a conduta passou a ser prevista como crime. A *fraude eletrônica* é apenas um dos exemplos de uma ampla categoria de ilícitos conhecida como cibercrimes[11]. O Brasil é o segundo país da América Latina em que mais são praticados crimes cibernéticos, atrás apenas do México[12].

Existem quase tantos termos para descrever o cibercrime quanto existem cibercrimes: as primeiras descrições incluíam "crime informático" e "crime por computador" e, à medida que a tecnologia digital se tornou mais difundida, termos como "alta tecnologia" ou "era da informação" foram acrescentados ao léxico[13]. Com advento da internet, passou-se a utilizar também expressões como "crime da internet", "crime digital", "e-crime", "crime virtual", "crime eletrônico" ou "de alta tecnologia". O termo "cibercrime", que costuma ser utilizado como sinônimo destas e de outras diversas expressões, descreve, em suma, uma espécie de ilícitos penais cometidos com computadores ou outros dispositivos informáticos[14]. "Cibercrime", assim, é um termo amplo que abrange condutas penalmente ilícitas praticadas com o uso de ferramentas computacionais e de aparelhos eletrônicos, como celulares[15], geralmente (mas não necessariamente) capazes de conexão com a internet.

Como não há homogeneidade entre as diversas espécies de crimes que se convencionou chamar de cibercrimes, ainda hoje é tormentoso encontrar uma nomenclatura suficientemente abrangente e tecnicamente precisa. É sintomático dessa dificuldade a existência de delegacias de polícia especializadas no tema que apresentam variadas denominações Brasil afora, que

10. FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **17º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em 15 ago. 2023.

11. Embora ao longo deste trabalho seja dado seja dado especial enfoque à criminalidade do colarinho branco, que causa imensos danos sociais e invariavelmente demanda o tratamento de dados pessoais para uma investigação e um processo eficientes, não se pode esquecer da extrema vulnerabilidade das multidões de vítimas dos crimes cibernéticos ditos "individuais", cujos danos materiais e morais jamais serão ressarcidos.

12. REVISTA EXAME. **R$ 103 bilhões roubados**: Brasil é o 2º país que mais sofre crimes cibernéticos na América Latina. 11 de junho de 2023. Disponível em: https://exame.com/future-of-money/r-103-bilhoes-roubados-brasil-e-o-2o-pais-que-mais-sofre-crimes-ciberneticos-na-america-latina/. Acesso em 14 mai. 2024.

13. CLOUGH, Jonathan. **Principles of Cybercrime**. Cambridge: Cambridge University Press, 2010, p. 9.

14. McQUADE III, Samuel C. McQuade (editor). **Encyclopedia of cybercrime**. Westport, Connecticut; London: Greenwood Press. 2009, p. 44.

15. McQUADE III, Samuel C. McQuade (editor). **Encyclopedia of cybercrime**. Westport, Connecticut; London: Greenwood Press. 2009, p. 43.

vão de "Delegacia Especial de Repressão a Crimes Cibernéticos" (como nos Estados do Amapá, Amazonas, Ceará, Goiás, Pernambuco, Sergipe, São Paulo, Tocantins e no Distrito Federal), "Delegacia de Repressão aos Crimes de Informática" (como no Rio de Janeiro e em Santa Catarina), até "Delegacia Especializada em Repressão a Crimes de Alta Tecnologia", (como no Piauí e, com pequena variação no nome, em Mato Grosso)[16].

Já na década de 1970 empregava-se a expressão "crime informático" para se referir à utilização indevida de computadores e dados, expressão que designava praticamente todas as atividades criminosas envolvendo equipamentos computacionais até ao final da década de 1990. Com a evolução e popularização da tecnologia e, especialmente, da internet, pesquisadores começaram a utilizar o termo "cibercrime" para se referirem a crimes praticados on-line, enquanto "crime informático" foi usado para se referir à utilização de computadores para atividades ilegais – embora estas expressões tenham sido comumente utilizadas como sinônimos por acadêmicos e pela imprensa no período. Distinguindo essas duas categorias, o cibercrime referir-se-ia a crimes em que o criminoso utiliza conhecimentos especiais "sobre o ciberespaço", enquanto os crimes informáticos são aqueles em que o criminoso utiliza conhecimentos especiais "sobre tecnologia informática"[17].

Apesar de todas as variações de terminologia, é largamente aceito que esses termos englobam ao menos três categorias de cibercrimes (originariamente sintetizadas pelo Departamento de Justiça dos EUA[18]): 1. crimes em que o computador ou a rede informática é o alvo da atividade criminosa (como pirataria informática, *cracking* e ataques do tipo DDoS); 2. crimes já existentes, mas nos quais o computador pode ser um instrumento para cometê-los (como pornografia infantil, *stalking*, violação de direitos de autor e fraudes diversas); 3. crimes em que a utilização do computador é um aspecto meramente incidental para sua prática, mas que pode fornecer provas às autoridades encarregadas da persecução penal (como registros de ligações telefônicas, de aplicativos de geolocalização e históricos de navegação da vítima e de autores de crimes). Susan W. Brenner chama essas três categorias de "*target cybercrimes*" (para destacar a tecnologia como um "alvo" propriamente dito da conduta ilícita), "*tool cybercrimes*" (que

16. BARRETO, Alesandro Gonçalves; KUFA, Carina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. 2. ed. rev. atual. e ampl. São Paulo: Juspodivm, 2021, pp. 48-49.

17. BOSSLER, Adam M.; HOLT, Thomas J. **Cybercrime in progress**: theory and prevention of technology-enabled offenses. New York: Routledge, 2016, p. 06.

18. CLOUGH, Jonathan. **Principles of cybercrime**. Cambridge: Cambridge University Press, 2010, p. 10.

identifica a tecnologia apenas como um instrumento para a prática do crime) e "*computer incidental*" (assinalando o caráter incidental da ferramenta tecnológica na prática do ilícito, sendo o computador, na perspectiva da atividade de persecução penal, majoritariamente uma fonte para a obtenção de evidências)[19].

Não nos parece adequado que, na definição cibercrime, seja exigido que a conduta ilícita se opere através da rede mundial de computadores: crimes praticados com o uso de dispositivos informáticos podem prescindir do uso da internet, a exemplo de determinadas fraudes bancárias ou a invasão de redes ou bancos de dados fechados, não conectados à rede mundial de computadores. Por outro lado, uma conceituação de cibercrime excessivamente abrangente poderia abarcar condutas de naturezas muito distintas, como crimes relacionados a biopirataria, a segredos industriais, a nanotecnologias e a engenharia genética[20].

Dentro de um conceito mais amplo de criminalidade informática, Pedro Dias Venâncio também considera importante distinguir os crimes em que a informática é apenas um novo meio para a prática de um crime não especificamente previsto para o ambiente digital dos crimes em que a informática é um elemento integrador do tipo legal ou do bem juridicamente protegido. Nesse mote, a cibercriminalidade informática em sentido estrito é aquela em que o elemento digital surge como parte integradora do tipo penal ou mesmo como seu objeto de proteção. Essa definição alberga tanto os que têm por bem tutelado o próprio acesso ou funcionalidade da sociedade da informação quanto todos aqueles em que a informática é parte necessária de seus elementos típicos[21].

No plano positivo-normativo, desde sua adesão à Convenção de Budapeste sobre cibercrime e sua promulgação pelo Decreto nº 11.941, de 12 de abril de 2023, pode-se concluir que o Brasil internalizou a definição extraída do preâmbulo do referido tratado. Assim, cibercrimes são ações praticadas contra a confidencialidade, a integridade e a disponibilidade de sistemas informáticos, redes e dados de computador, bem como o abuso de tais sistemas, redes e dados, e tipificadas em lei como ilícitos penais.

19. BRENNER, Susan W. **Cybercrime:** criminal threats from cyberspace. Oxford: Praeger, 2010, pp. 39-47.
20. CLOUGH, Jonathan. **Principles of cybercrime**. Cambridge: Cambridge University Press, 2010, p. 09.
21. VENÂNCIO, Pedro Dias. **Lições de direito do cibercrime e da tutela penal de dados pessoais**. Coimbra: D'Ideias, 2022, p. 22.

Ainda de acordo com a Convenção de Budapeste, há dez espécies de condutas que devem ser tipificadas em sua legislação interna por cada um dos países signatários. Tais condutas estão previstas nos artigos 2 a 11 da convenção e divididos em cinco categorias, correspondentes a seus títulos 1 a 5. No título 1 estão os crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador, que abrangem: acesso ilegal (art. 2), interceptação ilícita (art. 3), violação de dados (art. 4), interferência em sistema (art.5) e uso indevido de aparelhagem (art. 6). No título 2 estão os denominados *crimes informáticos*, que incluem a falsificação informática (art. 7) e a fraude informática (art. 8). O título 3, sobre *crimes relacionados ao conteúdo da informação*, exige a tipificação do crime de pornografia infantil (art. 9). O título 4 e seu art. 10 tratam da violação de direitos autorais e direitos correlatos. Por fim, o título 5, que dispõe sobre outras formas de responsabilidade e sanções, demanda a criminalização da tentativa, do auxílio ou da instigação à prática de quaisquer dos crimes a que alude a convenção.

De acordo com Thiago Misael, os crimes vislumbrados na Convenção de Budapeste podem ser classificados em quatro modalidades: a) crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador (arts. 2º, 3º, 4º, 5º e 6º); b) crimes informáticos propriamente ditos (arts. 7º e 8º); c) crimes relacionados ao conteúdo da informação (art. 9º), aos quais também podem ser acrescidos os crimes do 1º Protocolo Adicional, de racismo e xenofobia (arts. 3º e 6º); e d) violações a direitos autorais (art. 10)[22].

Os crimes elencados na convenção de Budapeste já têm hoje sua correspondente tipificação no direito brasileiro[23], eis que previstos na legislação extravagante ou incluídos no Código Penal (Decreto-lei nº 2848/40) em sucessivas alterações legislativas.

22. MISAEL, Thiago. **Cibercrime:** Convenção de Budapeste e Leis Brasileiras. 14 abr. 2023. Disponível em: https://investigacaofinanceira.com.br/cibercrime-convencao-de-budapeste-e-leis-brasileiras/. Acesso em 05 set. 2023.

23. De acordo com Thiago Misael, as leis nacionais não cobrem em sua integralidade os mandamentos de criminalização da Convenção de Budapeste. Alguns crimes, como os previstos no artigo 154-A e no art. 266, § 1º, do Código Penal, têm escopo menos abrangente – *i.e.*, tipificam menos condutas – que o vislumbrado pelo tratado internacional. (MISAEL, Thiago. **Cibercrime:** Convenção de Budapeste e Leis Brasileiras. 14 abr. 2023. Disponível em: https://investigacaofinanceira.com.br/cibercrime-convencao-de-budapeste-e-leis-brasileiras/. Acesso em 05 set. 2023).

O quadro[24] a seguir mostra o estágio atual da legislação brasileira em relação à obrigação assumida de tipificar, no plano normativo interno, as condutas elencadas na convenção de Budapeste:

Exigências de tipificação penal feitas pela Convenção de Budapeste		**Tipo penal previsto na lei brasileira: Código Penal (CP), Lei de Interceptação de Comunicações Telefônicas (Lei nº 9.296/96) e Estatuto da Criança e do Adolescente (ECA)**	
Artigo 2	Acesso ilegal	Art. 154-A do CP[25]	Invasão de dispositivo informático[26]
Artigo 3	Interceptação ilícita	Art. 10 da Lei nº 9.296/96[27]	Interceptação telefônica sem autorização judicial[28]
Artigo 4	Violação de dados	Art. 154-A e Art. 313-A do CP	O art. 154-A pune a invasão de dispositivo informático "com o fim de obter, adulterar ou destruir dados ou informações", embora não exija tal resultado para sua consumação; o art. 313-A do CP, além da inserção de dados falsos, tipifica também a alteração ou exclusão indevida de dados de sistemas informatizados ou bancos de dados da Administração Pública.

24. A tabela aqui apresentada é uma versão atualizada e com informações adicionais em relação à originalmente publicada em: CALABRICH, Bruno; VERONESE, Alexandre. Cybercrime in Brazil After the Covid-19 Global Crisis: An Assessment of the Policies Concerning International Cooperation for Investigations and Prosecutions. *In.*: LOISEAU, Hugo; VENTRE, Daniel. **Cybercrime During the SARS-CoV-2 Pandemic (2019-2022)**. Londres: ISTE/Wiley, 2023, p. 128.

25. Tipo penal criado pela Lei nº 14.155/2021.

26. "Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:

    Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

    § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*.

    § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

    § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

    Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa."

27. Redação dada pela Lei nº 13.869/2019.

28. "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei:

    Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa."

Exigências de tipificação penal feitas pela Convenção de Budapeste		Tipo penal previsto na lei brasileira: Código Penal (CP), Lei de Interceptação de Comunicações Telefônicas (Lei nº 9.296/96) e Estatuto da Criança e do Adolescente (ECA)	
Artigo 5	Interferência em sistema	Arts. 266[29] e 313-B do CP[30]	Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública[31] e modificação ou alteração não autorizada de sistema de informações[32]
Artigo 6	Uso indevido de aparelhagem	–	Sem tipo penal correspondente, mas é possível aplicar o art. 29 do CP (ao partícipe)
Artigo 7	Falsificação informática	Arts. 297, 298, 298, § único[33] e 313-A do CP[34]	Falsificação de documento público, falsificação de documento particular, falsificação de cartão e inserção de dados falsos em sistema de informações[35]
Artigo 8	Fraude informática	Arts. 155 e 171, *caput* e § 2º-A do CP[36]	Furto mediante fraude, estelionato e fraude eletrônica[37]

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

30. "Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.
Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado."

31. Redação dada pela Lei nº 12.737/2012, com a inclusão do §1º ao art. 266 do CPP, prevendo as mesmas penas para a interrupção de serviço *telemático.*

32. O tipo penal criado pela lei nº 9.983/2000.

33. O tipo penal de *falsificação de cartão de crédito ou débito* foi incluído como um parágrafo único do art. 298 do CP pela Lei nº 12.737/2012.

34. "Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa."

35. Tipo penal criado pela lei nº 9.983/2000.

36. O tipo penal de *fraude eletrônica* foi criado com a introdução do § 2º-A ao art. 171 do CP pela Lei nº 14.155/2021, sem prejuízo das demais formas de estelionato, inclusive quando praticado por vias eletrônicas, mas que não se amoldem à descrição do § 2º-A.

37. "Art. 171 [...]
§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes

Exigências de tipificação penal feitas pela Convenção de Budapeste		**Tipo penal previsto na lei brasileira: Código Penal (CP), Lei de Interceptação de Comunicações Telefônicas (Lei nº 9.296/96) e Estatuto da Criança e do Adolescente (ECA)**	
Artigo 9	Pornografia infantil[38]	Arts. 240, 241, 241-A e 241-B, 241-C, 241-D e 241-E do ECA[39]	Produção, armazenamento e compartilhamento, inclusive por meio de sistema de informática ou telemático[40], dentre diversas outras condutas, de conteúdo de sexo explícito ou pornográfico envolvendo criança ou adolescente.
Artigo 10	Violação de direitos autorais e direitos correlatos	Art. 184 do CP[41]	Violação de direito autoral[42]
Artigo 11	Tentativa, auxílio ou instigação à prática de cibercrimes	Arts. 14[43] e 29 do CP	Tentativa, autoria e participação (concurso de pessoas)

sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional."

38. "Outros aspectos relacionados à sexualidade das crianças e adolescentes, que são preocupações internacionais mas não estão inseridas na Convenção de Budapeste, também são previstas na legislação interna, tais como o cyberstalking, tipificado aqui como perseguição (art. 147-A, CP) (11); cyberbullying (12), cuja forma de atuação pode ser enquadrada em calúnia (art. 138, CP), difamação (art. 139, CP) ou injúria (art. 140, CP); e pornografia de vingança (art. 218-C, CP) (13)." (MISAEL, Thiago. **Cibercrime:** Convenção de Budapeste e Leis Brasileiras. 14 abr. 2023. Disponível em: https://investigacaofinanceira.com.br/cibercrime-convencao-de-budapeste-e-leis-brasileiras/. Acesso em 05 set. 2023.)

39. Os tipos dos arts. 241-A e 241-B, 241-C, 241-D e 241-E foram incluídos no ECA (Lei nº 8.069/90) pela Lei nº 11.829/2008.

40. "Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

§ 1º Nas mesmas penas incorre quem:

I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o *caput* deste artigo;

II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o *caput* deste artigo."

41. "Art. 184. Violar direitos de autor e os que lhe são conexos:

Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa."

42. Redação dada pela Lei nº 10.695/2003.

43. "Art. 14 – Diz-se o crime:

[...]

Em relação à exigência relacionada à criminalização da conduta de *uso indevido de aparelhagem* (artigo 6 da Convenção de Budapeste[44]), é digno de nota que, embora não haja um tipo penal específico, o ordenamento brasileiro, a depender das circunstâncias do caso concreto, permitirá o enquadramento do agente como responsável por quaisquer das condutas ali previstas na qualidade de *partícipe* (do crime principal), nos termos do art. 29 do CP[45].

Também merece registro que o Brasil, ao menos até janeiro de 2024, não era signatário do primeiro protocolo adicional à Convenção de Budapeste, de 2006, sobre a criminalização de atos de racismo e xenofobia cometidos através de sistemas informáticos[46], nem do segundo protocolo adicional, de março de 2022, relativo ao reforço da cooperação e da comunicação de provas eletrônicas[47]. Todavia, quanto ao primeiro protocolo adicional, seus crimes estão já previstos na Lei nº 7.716/89.

O quadro acima apresentado permite notar que, embora haja espaço para aprimoramentos, os tipos penais a que a alude a Convenção de Budapeste foram sendo paulatinamente introduzidos no direito brasileiro por sucessivas alterações no Código Penal e na legislação extravagante desde

---

II – tentado, quando, iniciada a execução, não se consuma por circunstâncias alheias à vontade do agente."

44. "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."

45. "Art. 29 – Quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade."

46. CONSELHO DA EUROPA. **First Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)**. Disponível em: https://www.coe.int/en/web/cybercrime/first-additional-protocol. Acesso em 14 ago. 2023.

47. CONSELHO DA EUROPA. **Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da comunicação de provas eletrônicas**. Disponível em: https://www.coe.int/en/web/cybercrime/second-additional-protocol e https://data.consilium.europa.eu/doc/document/ST-14898-2021-INIT/pt/pdf. Acesso em 14 ago. 2023.

os anos 2000 – muito antes, portanto, da adesão do país ao tratado internacional. A Lei nº 12.737/12, por exemplo, conhecida como "Lei Carolina Dieckmann"[48], é celebrada por alguns como o primeiro instrumento legal prevendo especificamente a criminalização de condutas que se identificava como cibercrimes. A lei incluiu dois artigos ao Código Penal e alterou outros dois, e assim mesmo com falhas e omissões graves de técnica legislativa: a adequação típica é tortuosa, por se valer de conceitos imprecisos, e tem preceitos secundários desproporcionalmente brandos[49].

Dentre as inovações legislativas mais recentes estão os tipos criados pela Lei nº 14.155/21, de *furto mediante fraude eletrônica* (art. 155, §4º-B, do CP) e de *fraude eletrônica* (art. 171, §2º-A, do CP), além do aprimoramento da redação para o tipo de *invasão de dispositivo informático* (art. 154-A do CP), incluindo o incremento das penas abstratamente cominadas. Meses antes, a Lei nº 14.132/2021 já havia incluído no Código Penal crime de *perseguição* (art. 147-A[50]), também chamado de *stalking*, que, por ser de ação livre (*i.e.*, que pode ser praticado por qualquer meio, inclusive pela internet), abrange o *cyberstalking*. Por fim, em 12 de janeiro de 2024 entrou em vigor a lei nº 14.811/2024, que incluiu no Código Penal o art. 146-A, criminalizando as condutas de intimidação sistemática (*bullying*)[51] e intimidação sistemática virtual (*cyberbullying*)[52].

48. A aprovação da Lei nº 12.737/12 foi marcada pela divulgação de fotos íntimas da atriz Carolina Dieckmann, episódio que recebeu farta cobertura da imprensa à época: "O fato acelerou o processo legislativo que há anos se arrastava sem criar um arcabouço normativo para cibercrimes" (BARRETO, Alesandro Gonçalves; KUFA, Carina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. 2. ed. rev. atual. e ampl. ão Paulo: Juspodivm, 2021, pp. 128-129).

49. BARRETO, Alesandro Gonçalves; KUFA, Carina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. 2. ed. rev. atual. e ampl. São Paulo: Juspodivm, 2021, p. 129.

50. "Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade.

Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa."

51. "Art. 146-A. Intimidar sistematicamente, individualmente ou em grupo, mediante violência física ou psicológica, uma ou mais pessoas, de modo intencional e repetitivo, sem motivação evidente, por meio de atos de intimidação, de humilhação ou de discriminação ou de ações verbais, morais, sexuais, sociais, psicológicas, físicas, materiais ou virtuais:

Pena – multa, se a conduta não constituir crime mais grave."

52. "Art. 146-A. Parágrafo único. Se a conduta é realizada por meio da rede de computadores, de rede social, de aplicativos, de jogos on-line ou por qualquer outro meio ou ambiente digital, ou transmitida em tempo real:

Pena – reclusão, de 2 (dois) anos a 4 (quatro) anos, e multa, se a conduta não constituir crime mais grave."