Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados

Diego Machado
Mestre e Doutorando em Direito Civil pela Universidade do Estado do Rio de Janeiro – UERJ.
Advogado.
diegocmachado@gmail.com

Danilo Doneda
Mestre e Doutor em Direito Civil pela Universidade do Estado do Rio de Janeiro – UERJ.
Advogado. Professor no IDP.
ddoneda@gmail.com

1. Introdução

Em recentes declarações, o ministro da segurança do Reino Unido, Ben Wallace, afirmou que não se deve permitir que alguém "possa se esconder atrás do anonimato", razão pela qual propõe a implementação de uma identidade digital (*digital ID*) – o que, segundo ele, seria uma escolha pela "sociedade civilizada" *on-line*, em vez do "oeste selvagem"[1]. O político ainda chamou atenção para o fato de que as companhias e provedores de aplicação de internet devem contribuir com a sociedade no que se refere ao combate aos efeitos negativos de suas tecnologias, tal como a criptografia ponta a ponta[2].

1. BUCHAN, Lizzy. *Digital IDs needed to end "mob rule" online, says security minister Ben Wallace*. Disponível em: [www.independent.co.uk/news/uk/politics/online-digital-identification-mob-rule-online-security-minister-ben-wallace-a8390841.html]. Acesso em: 18.06.2018.
2. Idem.

Machado, Diego; Doneda, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. *Revista dos Tribunais*. vol. 998. Caderno Especial. p. 99-128. São Paulo: Ed. RT, dezembro 2018.

2503_book.indb 99 23/11/2018 16:37:59

A aproximação entre as noções de anonimato e criptografia não é novidade, é recorrente, especialmente ao se tratar de comunicações e interações mantidas por meio de tecnologias da informação e da comunicação como a internet. Aliás, essa correlação é feita também em sentido diametralmente oposto ao do discurso do ministro britânico, como se vê no relatório de 2016 do Special Rapporteur da ONU sobre a proteção e promoção do direito à liberdade de opinião e de expressão, David Kaye: para ele, ambos (criptografia e anonimato) são importantes veículos para a tutela e realização de direitos humanos na era digital, tais como a privacidade e a liberdade de expressão[3].

O presente trabalho tem por objeto abordar uma interface entre anonimato e criptografia pouco explorada no cenário brasileiro. Trata-se de tema afeto à atividade de tratamento de informações e proteção de dados pessoais, dado que o processo de anonimização de dados e as suas respectivas técnicas têm relevantes repercussões jurídicas quanto à aplicação do regime de proteção de dados. Já, de outro lado, a aderência da criptografia ao que se discute se dá em razão do emprego de técnicas criptográficas como medida de segurança computacional adotada por empresas – ou pelos próprios usuários ou titulares dos dados – a fim de, por exemplo, proteger adequadamente as informações de seus usuários contra riscos de vazamento e outros problemas de segurança da informação em seus sistemas informáticos e bases de dados[4].

3. No relatório se lê que: "Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression" (HUMAN RIGHTS COUNCIL. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, 2016, p. 7. Disponível em: [www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Privatesectorinthedigitalage.aspx]. Acesso em: 20.06.2018).

4. O ano de 2017 foi marcado por numerosos casos de vazamento de dados, como o que envolveu o Pentágono norte-americano e o birô de crédito Equifax. Segundo relatório divulgado pela Identity Theft Resource Center, nesse ano houve aumento de 44,7% de ocorrências de vazamento de dados (nos Estados Unidos) em relação ao ano anterior, um total de 1.579 (IDENTITY THEFT RESOURCE CENTER. *2017 Annual Data Breach Year-end Review*. [S. l.], 2018. Disponível em: [www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf]. Acesso em: 20.06.2018).

2503_book.indb 100 23/11/2018 16:37:59

Em linhas gerais, criptografia "é a ciência da escrita secreta com o objetivo de esconder o significado de uma mensagem"[5]. As diversas técnicas criptográficas modernas que constituem mecanismo de confidencialidade[6] em segurança computacional, quando utilizadas, cifram informações de modo tal que apenas o destinatário da comunicação ou o detentor de chave criptográfica (simétrica ou assimétrica) pode acessar e compreender seu conteúdo informacional (*plaintext*)[7].

Assim, suscita-se a seguinte questão: se a criptografia é apta a tornar informações ininteligíveis, pode a cifragem de dados ser reputada como técnica de anonimização quando o dado tiver caráter pessoal, isentando, por conseguinte, responsáveis pelo tratamento de dados cifrados da observância do regime jurídico da proteção de dados pessoais? Em outras palavras, considerando que a definição de dado pessoal dada pela Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), em seu art. 5º, I, abrange a "informação relacionada a pessoa natural identificada ou identificável", em qual medida os dados pessoais submetidos a procedimento de encriptação serão considerados como tais?

Objetiva-se demonstrar que a resposta a essa questão não pode ser dada de maneira simplista. Dados criptografados não configuram dados anônimos ou anonimizados pelo só fato de ocorrer operação de cifragem. Para tanto, este texto é estruturado em duas partes: (i) primeiramente, serão delimitados alguns parâmetros propedêuticos sobre a conceituação de *dado pessoal*[8], haja

5. PAAR, Christof; PELZL, Jan. *Understanding cryptography:* a textbook for students and practitioners. London: Springer, 2010. p. 3. Tradução livre de: "is the science of secret writing with the goal of hiding the meaning of a message".

6. Dar-se-á destaque neste estudo à tradicional finalidade da criptografia: garantir a *confidencialidade* das comunicações. Não se ignora, entretanto, a existência de outros importantes objetivos que inspiram o desenvolvimento das técnicas criptográficas, a saber, *integridade*, *autenticidade* e *não repúdio*.

7. A cifragem resulta da conjunta operação do algoritmo criptográfico a da chave criptográfica: "The key to an encryption algorithm is the special code that pairs with the known algorithm to encrypt or decrypt data. Any computer data can be encrypted, including text, images, video, or programs" (KERR, Orin S.; SCHNEIER, Bruce. Encryption Workarounds. *The Georgetown Law Journal*, v. 106, p. 993, 2018).

8. No direito norte-americano se utiliza com mais frequência o termo *informação pessoalmente identificável* (*personally identifiable information*), conforme Daniel Solove e Paul Schwartz (SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review*, v. 86, p. 1827, dec. 2011). Neste trabalho, entretanto, utiliza-se o termo

2503_book.indb 101 23/11/2018 16:37:59

vista sua importância hermenêutica na aplicação da legislação de proteção dos dados pessoais, bem como sua colocação diante de dados pseudonimizados e dados anônimos; (ii) em seguida, há de se confrontar as características de técnicas criptográficas implementadas em contemporâneas tecnologias digitais àquelas que configuram efetiva anonimização de dados, para, junto a demais subsídios conceituais e dogmáticos, traçar apontamentos sobre o(s) estatuto(s) jurídico(s) aplicável(is) no Brasil a dados pessoais criptografados.

2. Dado pessoal: contornos conceituais e normativos

A partir da década de 1960, o conceito de informação[9] pessoal passou de algo que era meramente pressuposto (pois a garantia da privacidade deveria

"dado pessoal" ou "informação pessoal" pela pertinência quanto à realidade que pretende significar, bem como em razão do consagrado uso entre *experts* e na comunidade jurídica no Brasil e alhures, associado, ainda, ao seu emprego no direito positivo brasileiro.

9. Os vocábulos "informação" e "dado" comumente se apresentam sobrepostos. Vincenzo Zeno-Zencovich, por exemplo, ao expor a natureza poliédrica da informação, destaca que, numa acepção conteudística, "per informazione si intende qualsiasi dato rappresentativo della realtà che viene conservato da un soggetto oppure comunicato da un soggetto ad un altro" (ZENO-ZENCOVICH, Vincenzo. Informazione (profili civilistici). *Digesto* – Sezione Civile. Torino: UTET, 1993. v. IX. p. 3). Muito embora o tema não seja ora objeto de análise aprofundada, haja vista os limites do presente trabalho, vale pontuar que a equivalência entre *informação* e *dado* é afastada por expressiva parcela dos estudiosos da teoria da informação e suas diversas interfaces. No Brasil, já se afirmou que: "[...] o 'dado' apresenta conotação um pouco mais primitiva e fragmentada, como observamos por exemplo em um autor que o entende como uma informação em estado potencial, antes de ser transmitida; o dado estaria associado a uma espécie de 'pré-informação', anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar para o seu receptor. Sem aludir ao significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido de uma redução de um estado de incerteza. A doutrina não raro trata estes dois termos indistintamente" (DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 152). No campo filosófico, a partir da segunda metade do século XX surgem diversas concepções sobre o que é informação: Cf. ADRIAANS, Pieter. Information. *The Stanford Encyclopedia of Philosophy* – Edward N. Zalta (Ed.). Disponível em: [https://plato.stanford.edu/archives/fall2013/entries/information/]. Acesso em:

2503_book.indb 102 23/11/2018 16:37:59

necessariamente compreender a proteção dos documentos e informações de natureza privada) para gradativamente emergir como conceito central para a tutela jurídica da privacidade[10]. Isso tem direta correspondência com a transformação do *sentido social* de privacidade a que Stefano Rodotà faz alusão: de um sentido negativo, de confidencialidade e reserva sobre a esfera privada – logo, atinente a dados necessariamente vinculados ao indivíduo e suas relações particulares –, para compreender o controle dinâmico sobre as próprias informações[11].

A delimitação do conceito de dado pessoal é hoje imprescindível na interpretação do alcance normativo de leis de proteção de dados[12]. A título de exemplo, o Children's On-line Privacy Protection Act (COPPA) de 1998, estatuto norte-americano de proteção da infância no uso da internet, é aplicável a

27.08.2018; PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 48-53, 2018.

10. Não obstante a ausência de autonomia como conceito jurídico, no fim do século XIX, a noção de informação pessoal permeou as considerações seminais de Warren e Brandeis no consagrado artigo *The Right to Privacy*, como uma ideia pressuposta para os autores: "The early jurisprudence of privacy law lacked any concept of PII as a stand-alone category. In their famous 1890 article, Samuel Warren and Louis Brandeis merely assumed that privacy regulation would always involve information identifiable to a person. They conceived of privacy as a right of 'personality.' Although the two authors did not define this concept in any detail, they drew on continental philosophy to argue that every person deserves protection against certain kinds of harms as a consequence of her status as a human" (SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, v. 86, p. 1819, dec. 2011).

11. RODOTÀ, Stefano. *Il mondo nella rete:* quali i diritti, quali i vincoli. Roma-Bari: Laterza, 2014. p. 29.

12. Na doutrina, duras críticas já foram endereçadas a essa centralidade do conceito de dado pessoal, a exemplo do que faz Paul Ohm, que, considerando problemática a noção sempre em expansão de "informação pessoalmente identificável", sustenta o abandono do conceito como pilar da proteção jurídica da privacidade: "At the very least, we must abandon the pervasively held idea that we can protect privacy by simply removing personally identifiable information (PII). This is now a discredited approach. Even if we continue to follow it in marginal, special cases, we must chart a new course in general" (OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, n. 57, p. 1742, 2010). Porém, ao conceito continua sendo dada destacada relevância e função na aplicação do direito à proteção dos dados pessoais.

2503_book.indb 103 23/11/2018 16:37:59

todos que coletem informação pessoal de menores de 13 anos, estabelecendo critérios para o legítimo tratamento desses dados[13]. Pode-se citar também o Regulamento Geral de Proteção de Dados Pessoais da União Europeia[14], a Convenção 108 do Conselho da Europa[15] e a Lei Federal 13.709/2018, do Brasil (Lei Geral de Proteção de Dados – LGPD). Nesses três recentes textos legislativos percebe-se que o conceito de informação pessoal é chave para entender o âmbito material de aplicação da lei, que, por sua vez, visa nas esferas regional, internacional e nacional, respectivamente, regular a atividade de tratamento de dados pessoais.

Num primeiro enfrentamento a respeito da definição de dado pessoal, pode-se depreender a distinção de abordagens de técnica legislativa utilizadas para a construção dos conceitos *restrito* e *amplo*, ou que observa, correspondentemente, o que Daniel Solove e Paul Schwartz nomeiam de *perspectivas reducionista* e *expansionista* de política regulatória de proteção de dados[16].

13. Conforme previsto na *Section 1303, a, 1,* o COPPA estatui: "(1) In general. – It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed under subsection (b)" (ESTADOS UNIDOS. *Children's Online Privacy Protection Act of 1998*. Disponível em: [www.law.cornell.edu/uscode/text/15/chapter-91]. Acesso em: 05.08.2018).
14. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, que entrou em vigor nos países-membros do bloco europeu em 25 de maio de 2018.
15. A Convenção 108, de 1981, sobre a proteção de indivíduos com relação ao tratamento automatizado de dados pessoais, foi o primeiro instrumento internacional vinculante de proteção dos dados pessoais. Em 18 de maio de 2018, foi adotado pelos membros do Conselho da Europa um protocolo de alteração para modernizar o tratado, tendo em vista a necessidade de lidar adequadamente com os novos desafios e questões que as tecnologias da informação e comunicação impõe à tutela da privacidade. V. COUNCIL OF EUROPE. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108). Disponível em: [https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf]. Acesso em: 24.06.2018.
16. SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review*, v. 86, p. 1871-1877, dec. 2011. A respeito do tema, *vide* também BIONI, Bruno. *Xeque-mate:* o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: GPOPAI, 2015.

2503_book.indb 104 23/11/2018 16:37:59

Na conceitualização restrita, por dado pessoal entende-se a representação de fatos sobre pessoa *identificada*, isto é, representação referente a alguém que se conhece e individualiza em meio a certo grupo ou coletividade. O processo de identificação aí operado é possível a partir de elementos informativos chamados *identificadores*, "os quais mantém relação particularmente privilegiada e próxima com certo indivíduo"[17].

Os identificadores podem, por sua vez, ser *diretos* ou *indiretos*. O típico identificador direto de um indivíduo é o seu nome. Constituído por prenome e sobrenome, o nome da pessoa humana é o primeiro sinal distintivo da individualidade, forma de *identificação social* da pessoa entre os demais membros de dada comunidade[18]. No entanto, nem sempre o identificador direto é bastante, pois pode se configurar, a título de exemplo, a homonímia, de maneira que identificadores indiretos como o número do CPF ou do telefone, a nacionalidade, a filiação, o endereço eletrônico ou o CEP da residência, e mesmo características fenotípicas, podem ser necessários para se distinguir alguém. Essa categoria é conexa ao "fenômeno das 'combinações únicas'"[19].

Uma vez adotada, essa concepção pode ser implementada *por específica tipificação* em lei de quais identificadores (diretos ou indiretos) são reputados informação pessoal. Isto é, se o dado se enquadrar dentro de uma das categorias-tipo elencadas pelo legislador, ele se torna informação pessoal por obra da lei[20]. Fora da moldura legal não haveria, portanto, dado pessoal, nem se

17. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. Bruxelas: [s. n.], 2007. p. 12. Disponível em: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf]. Acesso em: 21.08.2018. Tradução livre de: "[...] which hold a particularly privileged and close relationship with the particular individual".

18. O nome atende aí ao que Lara Trucco denomina etapa de atribuição do processo de "identificação pessoal jurídica" (TRUCCO, Lara. *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*. Torino: Giappichelli, 2004, p. 4-5). *Vide* também ARTICLE 29 DATA PROTECTION WORKING PARTY. Op. cit., p. 13. Ressalta-se, todavia, que o nome da pessoa humana não é aqui tratado tão somente sob o prisma da identificação, não contemplando a profundidade própria da perspectiva da tutela da personalidade.

19. ARTICLE 29 DATA PROTECTION WORKING PARTY. Op. cit., p. 13.

20. "In the context of the specific-types approach, if information falls into an enumerated category, it becomes per se PII by operation of the statute" (SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review*, v. 86, p. 1831-1832, dec. 2011).

2503_book.indb 105 23/11/2018 16:38:00

aplicaria o regime de proteção de dados. No ordenamento jurídico dos Estados Unidos da América, o conceito restrito é tipificado em dois importantes diplomas do *statutory law*: o *Privacy Act*, de 1974, e o já mencionado COPPA[21].

De outro lado, o conceito amplo estende seu alcance para além da pessoa natural meramente identificada: também é informação de caráter pessoal aquela relativa a pessoa *identificável*. Há dado pessoal não apenas quando houver a presença de identificadores diretos ou indiretos que diferem precisamente um indivíduo. Os dados que *potencialmente* conduzem à individuação da pessoa são igualmente tomados como informação pessoal.

Existem dados ou identificadores que, apesar de não individuarem efetivamente alguém, caso tratados com técnicas que são acessíveis e em conjunto com dados suplementares, podem levar à identificação de seu titular. Ainda que o agente responsável pelo tratamento dos dados não possa identificar com precisão a pessoa natural a quem se referem as informações processadas, com algum esforço ele, ou terceiro[22], pode se valer de meios disponíveis para a obtenção dos dados adicionais aptos a fazê-lo.

Por exemplo, se provedor de aplicação de internet, além de processar dados de tráfego, armazenar registros de endereço IP de terminais que acessaram seu sítio eletrônico, não obstante a ausência de identificação imediata, os usuários da internet podem ser identificados mediante requerimento judicial de acesso

21. O U. S. Code, Title 15, Chapter 9, § 6501 (8), determina: "Personal information. The term "personal information" means individually identifiable information about an individual collected online, including — (A) a first and last name; (B) a home or other physical address including street name and name of a city or town; (C) an e-mail address; (D) a telephone number; (E) a Social Security number; (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph".

22. A perspectiva que considera a identificabilidade de pessoa natural não só por esforços do responsável pelo tratamento mas também de *qualquer pessoa*, é chamada de *absoluta*. Foi essa a abordagem adotada pelo Grupo de Trabalho de Proteção de Dados do Artigo 29, no Parecer 04/2007, e pelo Tribunal de Justiça da União Europeia no caso *Breyer*. Cf. SPINDLER, Gerald; SCHMECHEL, Philipp. Personal data and encryption in the European General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, v. 7, p. 165, 2016; PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 46, 2018.

2503_book.indb 106 23/11/2018 16:38:00

a registros de conexão e dados cadastrais armazenados pelos respectivos provedores de conexão. Esse é, a propósito, o entendimento adotado na União Europeia, tanto pelo Grupo de Trabalho de Proteção de Dados do Artigo 29[23] como pelo Tribunal de Justiça da União Europeia (TJUE) nos casos C-70/10, Scarlet Extended SA *v.* Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), e C-582/14, Patrick Breyer *v.* Bundesrepublik Deutschland. No primeiro, a menção à caracterização do endereço IP como dado pessoal é feito em sede de *obiter dictum*, mas no *Breyer case* compõe de fato as razões de decidir (*ratio decidendi*) do julgado a qualificação do endereço IP (dinâmico) como "informação relativa a pessoa natural identificada ou identificável".

A análise do potencial de identificação (ou identificabilidade) de certa informação pelo responsável pelo tratamento ou por outro sujeito não pode ser feita em abstrato apenas, como se bastasse uma possibilidade puramente hipotética[24]. No direito europeu, desde a Diretiva 95/46/EC vigora o critério *dos meios suscetíveis de ser razoavelmente utilizados*, que busca ser balizado por fatores objetivos como custos e tempo de trabalho exigidos para a identificação, o estado da arte da tecnologia existente no período de duração do tratamento, os riscos de falhas técnicas e de descumprimento dos deveres de confidencialidade, por exemplo[25].

Trata-se de critério dependente de aspectos contextuais – *e.g.,* estágio de desenvolvimento das tecnologias da informação e inteligência artificial – que faz

23. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Privacy on the internet* – An integrated EU Approach to On-line Data Protection. Bruxelas: [s. n.], 2000. Disponível em: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp37_en.pdf]. Acesso em: 22.08.2018.

24. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data.* Bruxelas: [s. n.], 2007. p. 15. Disponível em: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf]. Acesso em: 21.08.2018.

25. O Considerando 26 do GDPR estabelece que: "The principles of data protection should apply to any information concerning an identified or identifiable natural person. [...] To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments".

2503_book.indb 107 23/11/2018 16:38:00

da caracterização como dado pessoal um estado *dinâmico*[26]. Esse caráter maleável do conceito, se de um lado contribui para que uma lei de proteção de dados acompanhe as transformações tecnológicas e socioeconômicas, por outro pode dar ensejo a insegurança em alguma medida, uma vez que os avanços das *data-driven technologies* se desenvolvem em passo acelerado e poderiam conferir caráter pessoal a dado antes considerado anônimo, devido à disponibilização de novas técnicas capazes de realizar essa reidentificação[27].

O direito brasileiro seguiu a orientação Europeia e adotou o conceito amplo de dado pessoal, como pode se verificar no artigo 5º, I, da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD): dado pessoal é "informação relacionada a pessoa natural identificada ou identificável". O conceito da LGPD, na verdade, endossa o que já prescreve a Lei 12.527/2011 (Lei de Acesso à Informação), no seu artigo 4º, IV, pelo qual a informação é "aquela relacionada à pessoa natural identificada ou identificável".

Importante se ter em mente, porém, que essa conceituação também estabelece, consequentemente, a linha divisória do que é e *não é* informação pessoal. Se os dados não são relativos a pessoa identificada ou identificável, desde a origem ou após ulterior tratamento, são dados ditos *anônimos* ou que foram *anonimizados*. Nos termos do artigo 5º, III, da LGPD, dado anonimizado é "dado relativo a titular que *não possa ser identificado*, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (grifou-se).

Não se pode apenas reduzir a noção de dado anônimo ou anonimizado a dado não associado ao nome de alguém. Ainda que não haja a certeira identifi-

26. PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 47, 2018. Cf. ARTICLE 29 DATA PROTECTION WORKING PARTY. Op. cit., p. 15; EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS; COUNCIL OF EUROPE. *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2018. p. 88.

27. Sobre esse apontamento crítico, afirma Purtova: "The resulting standard of the reasonable likelihood of identification is quite broad and context-dependent, leading to one major consequence: the status of data as 'personal' is dynamic, ie the same dataset may not obviously be personally identifiable at the start of processing, or from the perspective of the controller, given the tools and data available to him, but become, or appear to have been all along, identifiable from the perspective of another person or once the circumstances change" (PURTOVA, Nadezhda. Op. cit., p. 47).

2503_book.indb 108 23/11/2018 16:38:00

cação do titular das informações pelo nome, a distinção (*singling out*) mediante outros identificadores[28] é possível, inclusive para a formação de perfil de comportamento do indivíduo[29]. Para ser anônimo, o dado não pode ter associação com pessoa identificada ou identificável de forma permanente e irreversível[30] – raciocínio este apenas derivado do conceito amplo de dado pessoal. Se assim caracterizado, o estatuto de proteção dos dados pessoais não se aplica, ou, eventualmente, aplica-se de maneira particularizada à atividade de tratamento das informações em questão[31].

28. Como ocorre com os *cookies*, que, uma vez enviados por *websites* e armazenados nos computadores dos usuários a partir do navegador utilizado, funcionam como identificadores eletrônicos. Esses arquivos são notadamente empregados com o propósito de monitorar hábitos de navegação dos usuários, ou proporcionar-lhes uma experiência personalizada de navegação no sítio eletrônico. Cf. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS; COUNCIL OF EUROPE. *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2018. p. 91.

29. Nesse sentido, discorre Giusella Finocchiaro: "Né può semplicisticamente adottarsi la definizione di anonimo come privo di nome, etimologicamente fondata e propria del linguaggio comune, la quale evoca un'assoluta mancanza di collegamento fra un fatto o un atto e un soggetto. La riconducibilità di un'informazione ad un soggetto, di cui si può ignorare il nome, ma rispetto al quale si hanno numerose altre informazioni, consente comunque di ricostruirne il profilo" (FINOCCHIARO, Giusella. Anonimato. In: *Digesto delle Discipline Privatistiche – Sezione Civile*. Aggiornamento. Torino: UTET, 2010. p. 13).

30. Nesse particular, a LGPD prescreve: "Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido".

31. VIOLA, Mario; DONEDA, Danilo; ANDRADE, Norberto N. G. de. Dados anônimos e tratamento de dados para finalidades distintas: a proteção de dados pessoais sob uma ótica civil-constitucional. In: TEPEDINO, Gustavo; FACHIN, Luiz E. (Org.). *Pensamento crítico do direito civil brasileiro*. Curitiba: Juruá, 2011. p. 200. Sobre esse assunto, dispõe o Considerando 26 do Regulamento (UE) 2016/679: "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes".

2503_book.indb 109 23/11/2018 16:38:00

Nas últimas duas décadas, importantes estudos realizados no campo da ciência da computação, como as pesquisas de Latanya Sweeney[32], Arvind Narayanan e Vitaly Shmatikov[33], revelaram sérias falhas em práticas de anonimização de dados tidas por confiáveis. Isso levou a doutrina especializada a romper com a *suposição da anonimização robusta* (*robust anonymisation assumption*[34]) então em vigor – a ideia de que com simples operações de eliminação ou substituição de atributos dos titulares dos dados, por exemplo, respeitar-se-ia a privacidade ao mesmo tempo que seria reservada a utilidade das informações ao responsável pela base de dados.

Considerados os resultados e as pertinentes análises críticas, hoje há o reconhecimento de que sempre haverá fatores de risco de identificação ou reidentificação de pessoas com o tratamento de dados anonimizados, tendo em vista o enorme volume de dados hoje disponibilizados (via internet) e o desenvolvimento da capacidade de processamento e análise de algoritmos de mineração de dados e de aprendizado de máquina. Todavia, isso não resultou absolutamente na eliminação da diferenciação entre dado pessoal e dado não pessoal. As recentes leis de proteção de dados ainda insistem e estão fundamentadas nessa distinção e na eficácia possível de técnicas de anonimização[35], tais como

32. SWEENEY, Latanya. Simple demographics often identify people uniquely. *Carnegie Mellon University*, Data Privacy Working Paper 3, Pittsburgh, 2000.

33. NARAYANAN, Arvind; SHMATIKOV, Vitaly. *How to break anonymity of the Netflix Prize dataset*. 2007. p. 3. Disponível em: [https://goo.gl/RxggOU]. Acesso em: 30.08.2018.

34. OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, n. 57, p. 1706, 2010.

35. Na análise feita pelo Grupo de Trabalho de Proteção de Dados do Artigo 29, no Parecer 05/2014 sobre a anonimização de dados no contexto do direito da União Europeia, foram destacadas quatro características fundamentais das técnicas de anonimização: (i) a anonimização pode ser um resultado do tratamento de dados pessoais com a finalidade de impedir de forma irreversível a identificação do titular dos dados; (ii) várias são as técnicas de anonimização que podem ser utilizadas, visto que não há prescrição na legislação europeia de técnica específica; (iii) os elementos contextuais são muito importantes, ou seja, na avaliação deve ser tomado o conjunto "dos meios 'suscetíveis de serem razoavelmente' utilizados para identificação pelo responsável pelo tratamento e por terceiros", de acordo com o estado da técnica; e (iv) à anonimização é inerente a existência de um fator de risco (ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 5/2014 on Anonymisation techniques*. Bruxelas: [s. n.],

2503_book.indb 110 23/11/2018 16:38:00

a adição de ruídos, permutação, privacidade diferencial, k-anonimato e l-diversidade.

No exame da robustez e do nível de garantia oferecidos por técnicas e práticas de anonimização de dados, sugere-se que três tipos de riscos principais sejam levados em consideração: distinção (*singling out*), possibilidade de ligação e inferência. O primeiro versa sobre a possibilidade de se isolar alguns ou todos os registros que destaca uma pessoa em uma base de dados; o segundo é a capacidade de se estabelecer uma conexão entre pelo menos dois registros relativos ao mesmo indivíduo ou mesmo grupo de pessoas; e o terceiro, por fim, diz com a possibilidade de deduzir, com uma significativa probabilidade, o valor de um atributo a partir dos valores de um conjunto de outros atributos.[36]

Em meio a essa discussão, com uma abordagem orientada pelo risco, há o surgimento de propostas que visualizam entre o dado pessoal e o dado anônimo um gradiente de cores ou um *continuum* com categorias que superam a lógica binária[37] dado pessoal/dado anônimo, informações a que se aplicam o regime de proteção de dados pessoais/informações a que não se aplicam o regime de proteção de dados pessoais. É nesse contexto que se coloca a ideia de *dado pseudonimizado*.

2014. p. 6-7. Disponível em: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf]. Acesso em: 24.08.2018).

36. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 5/2014 on Anonymisation techniques*. Bruxelas: [s. n.], 2014. p. 11-12. Disponível em: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf]. Acesso em: 24.08.2018.

37. Nessa direção: ESAYAS, Samson Yoseph. The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach. *European Journal of Law and Technology*, v. 6, n. 2, 2015; POLONETSKY, Jules et. al. *The seven states of data: when is pseudonymous data not personal information?* The Future of Privacy Forum, 2013. Disponível em [https://fpf.org/wp-content/uploads/2016/05/states-v19-1.pdf]. Acesso em: 25.08.2018. No modelo de conceptualização pensado por Daniel Solove e Paul Schwartz, os autores sugerem: "Our model places information on a continuum that begins with no risk of identification at one end, and ends with identified individuals at the other. We divide this spectrum into three categories, each with its own regulatory regime: under the PII 2.0 model, information can be about an (1) identified, (2) identifiable, or (3) non-identifiable person. Our three categories divide up this spectrum and provide different regimes of regulation for each. Because these categories do not have hard boundaries, we define them in terms of standards" (SCHWARTZ, Paul M.; SOLOVE, Daniel J. Op. cit., p. 1877).

2503_book.indb 111 23/11/2018 16:38:00

Segundo o Grupo de Trabalho de Proteção de Dados do Artigo 29, o procedimento de "pseudonimização consiste em substituir um atributo (tipicamente um atributo único) em um registro por outro"[38]; seria um processo de mascaramento ou disfarce (*disguising*) de identidade[39], que afeta principalmente identificadores diretos[40]. Conquanto haja na doutrina quem defenda que a pseudonimização seja mais uma técnica de anonimização[41], a distinção entre ambos é feita em sede legal, tanto pela GDPR[42] como pela LGPD[43].

A pseudonimização opera de maneira que as informações não podem ser conectadas a um titular de dados específico sem que se recorra a informações suplementares, desde que estas sejam mantidas separadamente, empregadas medidas organizativas e de segurança. Em pesquisas médicas, desde a década de 2000 já se estuda a implementação dessas técnicas a fim de se alcançar o respeito à privacidade dos sujeitos da pesquisa e o tratamento de dados de modo útil à investigação científica. Para estudos de radiologia clínica, a título de exemplo, a pseudonimização é importante para identificar dados de certo paciente de forma consistente com o passar do tempo – o que a anonimização

38. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 5/2014 on Anonymisation techniques*. Bruxelas: [s. n.], 2014. p. 20. Disponível em: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf]. Acesso em: 24.08.2018.

39. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. Bruxelas: [s. n.], 2007. p. 18. Disponível em: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf]. Acesso em: 21.08.2018.

40. ESAYAS, Samson Yoseph. The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach. *European Journal of Law and Technology*, v. 6, n. 2, p. 4, 2015. Na mesma direção: "Pseudonymization means that a true identifier such as name or patient identification number is replaced by a pseudonym that is unique to the individual but bears no relation to the person "in the real world". Pseudonym cannot therefore be used as a means of identification. This is because in pseudonymization, the information that reveals who the pseudonym relates to will be held securely, and separately, from the data being processed" (NOUMEIR, Rita; LEMAY, Alain; LINA, Jean-Marc. Pseudonymization of Radiology Data for Research Purposes. *Journal of Digital Imaging*, v. 20, n. 3, p. 286, 2007).

41. ESAYAS, Samson Yoseph. Op. cit., p. 4.

42. Ver Considerandos 26 a 29, 75, 78; e artigos 4º e 5º.

43. Ver artigos 5º, III e XI, e 13, § 4º.

2503_book.indb 112 23/11/2018 16:38:00

ainda não faz[44]. O pseudônimo de um paciente específico é associado a todas as informações de-identificadas relativas a ele apesar do momento em que houve a de-identificação dos dados[45]. Como resultado há o acompanhamento do evolver do quadro clínico do sujeito da pesquisa.

Muito embora com certa clareza seja reputado informação pessoal na GDPR[46], o dado pseudonimizado pode se submeter a um regime jurídico modulado ou particularizado, em linha de sintonia com esse mesmo estatuto: abrem-se portas para o tratamento de informações com *finalidade diversa da original* e não lastreada em consentimento expresso do titular dos dados, desde que o propósito ulterior seja *compatível* com o inicialmente consentido (GDPR, artigo 6º, 4, *e*)[47]. Semelhante raciocínio pode ter arrimo no sistema jurídico brasileiro a partir da previsão legal do artigo 9º, § 2º, da LGPDP[48].

3. Cifragem de dados pessoais e anonimização de informações

As palavras do ministro britânico citadas no início retratam o discurso e mentalidade de setores governamentais não apenas do velho continente, mas que também transpõem o Atlântico. A aplicação de sistemas criptográficos em tecnologias da informação e da comunicação é vista por esses agentes como

44. NOUMEIR, Rita; LEMAY, Alain; LINA, Jean-Marc. Op. cit., p. 286-287.

45. Ibidem, p. 287.

46. De acordo com o Considerando 26 do Regulamento europeu, "[p]ersonal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person".

47. "Article 6. *Lawfulness of processing*. [...] 4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: [...] (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation."

48. "Art. 9º. [...] § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações."

2503_book.indb 113 23/11/2018 16:38:00

entrave a certas ações estatais e investigações criminais, ou, como dito por Christopher Wray, Diretor da agência estadunidense de investigação (FBI), uma "urgente questão de segurança pública"[49].

A criptografia ponta a ponta é tecnologia que reiteradamente tem sido ventilada em fóruns sobre regulação e políticas públicas endereçadas a técnicas criptográficas, num debate que foi levado, inclusive, para os tribunais brasileiros. Depois de uma série de bloqueios determinados judicialmente ao acesso e uso do aplicativo de mensagem instantânea WhatsApp[50], foram propostas perante o Supremo Tribunal Federal (STF) as ações de controle de constitucionalidade ADI 5527 e ADPF 403 (ainda não julgadas), nas quais o mecanismo da criptografia ponta a ponta empregado pela referida aplicação de internet é analisado[51].

A técnica consiste em garantir que apenas emissor e destinatário (as "pontas") da comunicação tenham acesso à chave criptográfica necessária para decifrar as informações enviadas. Na linguagem da segurança computacional, a criptografia ponta a ponta é um *protocolo criptográfico*[52] que reduz a superfície

49. VOLZ, Dustin. *FBI chief calls unbreakable encryption 'urgent public safety issue'*, 2018. Disponível em: [www.reuters.com/article/us-usa-cyber-fbi/fbi-chief-calls-unbreakable-encryption-urgent-public-safety-issue-idUSKBN1EY1S7]. Acesso em: 27.06.2018.

50. Sobre todos os bloqueios judiciais de aplicações de internet no Brasil, consulte a plataforma criada pelo *InternetLab:* [http://bloqueios.info/pt/linha-do-tempo/].

51. O tema recebeu destaque na audiência pública realizada pelo Supremo Tribunal Federal nos dias 02 e 05 de junho de 2017. Questões sobre o funcionamento da criptografia ponta a ponta e a possibilidade de interceptação de comunicações mantidas por aplicações que a utilizam, pautaram as intervenções no evento. *Vide* a transcrição das contribuições apresentadas na audiência pública em [www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarcoCivildaInternete-BloqueioJudicialdoWhatsApp.pdf].

52. Sobre a noção técnica de protocolo criptográfico, anotam Hans Delfs e Helmut Knebl: "Encryption and decryption algorithms, cryptographic hash functions or *pseudorandom generators* [...] are the basic building blocks (also called cryptographic primitives) for solving problems involving secrecy, authentication or data integrity".
"In many cases a single building block is not sufficient to solve the given problem: different primitives must be combined. A series of steps must be executed to accomplish a given task. Such a well-defined series of steps is called a cryptographic protocol. As is also common, we add another condition: we require that two or more parties are involved. We only use the term protocol if at least two people are required to complete

2503_book.indb 114 23/11/2018 16:38:00

de ataque ao sistema diminuindo "a ameaça de pontos intermediários ou *atacantes internos* que operam o serviço e desfrutam de acesso privilegiado"[53]. Ou seja, no contexto das comunicações de dados que opera na internet, esse tipo de protocolo é concebido para resguardar a confidencialidade das informações trocadas entre emissor e destinatário não somente de sujeitos externos, como também do próprio intermediário, provedor de serviço de internet – *e.g.*, WhatsApp e Facebook Messenger – que faz parte da arquitetura da rede e das comunicações em meio digital como hoje conhecemos.

A maioria dos protocolos criptográficos modernos pode ser classificada como "ponta a ponta"[54]. Além da conhecida implementação em aplicações de mensagem instantânea como o WhatsApp, Signal e Wire, outro importante exemplo são os protocolos SSL/TLS, que visam oferecer ao usuário uma segura navegação na rede, entre seu terminal e o servidor em que está hospedado certo sítio eletrônico acessado[55]. Pode-se citar também o uso de criptografia ponta a ponta em aplicações de correio eletrônico como o ProtonMail e o Hushmail.

Partindo desse ângulo, todavia, a criptografia parece ser realçada num contexto em que a cifragem de dados se opera quando a mensagem comunicada trafega de um computador a outro[56]. Esse processo de criptografia em trânsito (*encryption in transit*)[57], se não acompanhado da cifragem de dados em repou-

---

the task" (DELFS, Hans; KNEBL, Helmut. *Introduction to cryptography*: principles and applications. 2. ed. Berlin-Heildelberg-New York: Springer, 2007. p. 5).

53. *Vide* texto publicado neste volume: ARANHA, Diego F. O que é criptografia fim-a-fim e o que devemos fazer a respeito.

54. ARANHA, Diego F. O que é criptografia fim-a-fim e o que devemos fazer a respeito.

55. A título de exemplo, pode-se citar o emprego desses protocolos que formam o *Hyper Text Transfer Protocol Secure – HTTPS*, e o carregamento de páginas *web* por meio do navegador *Firefox*: em julho de 2018, mais de 70% dos sítios eletrônicos acessados com este *web browser* se deu com o uso de *HTTPS* (LET'S ENCRYPT. *Let's encrypt stats*. Disponível em: [https://letsencrypt.org/stats/]. Acesso em: 10.09.2018). Tome-se em consideração que, em termos globais, o percentual médio da parcela de mercado, de setembro de 2017 a agosto de 2018, do navegador Firefox é de 5,70%, referente a *desktops* e dispositivos móveis (NETMARKETSHARE. *Browser market share*. Disponível em: [https://bit.ly/2QkSqiW]. Acesso em: 10.09.2018).

56. Cf. GILL, Lex; ISRAEL, Tamir; PARSONS, Christopher. *Shining a Light on the encryption debate*: a Canadian field guide. [s.l]: Citizen Lab/Samuelson-Glushko CIPPIC, 2018. p. 5-6.

57. A criptografia *em trânsito* "refers to the process of using encryption to secure information as it travels from one computer to another. This prevents data – such as web

2503_book.indb 115 23/11/2018 16:38:00

so (*encryption at rest*), sujeita as informações comunicadas a vulnerabilidades passíveis de exploração e consequente violação de direitos.

A "[c]riptografia em repouso refere-se a dados que são protegidos enquanto são persistentemente armazenados em um terminal, como num laptop, um dispositivo móvel ou no servidor de um provedor de serviços"[58]. Nessa perspectiva é que se analisa a cifragem de um arquivo digital, uma pasta, uma partição do disco rígido, ou mesmo do inteiro dispositivo do usuário (*full-disk encryption*[59]). Em outras palavras, sem a chave de decriptação o conteúdo do arquivo encriptado ou de todos os dados armazenados no dispositivo ou terminal (*e.g.*, *smartphone*, *tablet*) são ininteligíveis a terceiros não autorizados.

Esse tipo de cifragem se diferencia entre os prismas do usuário (*client-side encryption*) e do servidor (*server-side encryption*). Enquanto no primeiro a criptografia é aplicada localmente num terminal junto ao usuário, por exemplo, em seu *smartphone* ou computador pessoal; no segundo, os dados são armazenados e encriptados remotamente, em servidores situados em localidade(s) diversa(s)[60]. Este último caso é o que comumente ocorre com serviços de internet que utilizam computação em nuvem (*cloud computing*)[61], abrangendo não só aqueles que são estruturados principalmente no fornecimento de armazenamento remoto de dados (*e.g.*, Spideroak One Backup), mas também outras

traffic, a text message, content entered into a webform, or an e-mail – from being intercepted or modified by an unauthorized third party as it travels to its destination over the network. Encryption in transit protects the confidentiality and integrity of the content while facilitating authentication" (GILL, Lex; ISRAEL, Tamir; PARSONS, Christopher. *Shining a light on the encryption debate*: a Canadian field guide. [s.l]: Citizen Lab/Samuelson-Glushko CIPPIC, 2018. p. 5).

58. GILL, Lex; ISRAEL, Tamir; PARSONS, Christopher. Op. cit., p. 4. Tradução livre de: "Encryption at rest refers to data which is secured while it is persistently stored at an endpoint, such as on a laptop, a mobile device, or on the server of a service provider".

59. WIKIPEDIA. *Disk encryption*. Disponível em: [https://en.wikipedia.org/wiki/Disk_encryption]. Acesso em: 10.09.2018.

60. GILL, Lex; ISRAEL, Tamir; PARSONS, Christopher. *Shining a light on the encryption debate*: a Canadian field guide. [s.l]: Citizen Lab/Samuelson-Glushko CIPPIC, 2018. p. 4.

61. De acordo com Christopher Millard: "In slightly more technical terms, cloud computing is an arrangement whereby computing resources are provided on a flexible, location-independent basis that allows for rapid and seamless allocation of resources on demand" (MILLARD, Christopher (Ed.). *Cloud computing law*. Oxford: Oxford University Press, 2013. *E-book*).

2503_book.indb 116 23/11/2018 16:38:00

aplicações como as de correio eletrônico, mensagens instantâneas[62], monitoramento de saúde etc.

Importante ressaltar que a guarda de dados cifrados em servidores de empresas fornecedoras de computação em nuvem não decorre somente da realização de políticas de privacidade do provedor e da implementação de técnicas criptográficas para segurança informacional. Afinal, o próprio usuário pode individualmente decidir se valer de *softwares* de encriptação de dados para assegurar a confidencialidade destes antes mesmo de carregá-los aos servidores de *cloud computing*, em aplicações como *Google Drive* e *Dropbox*, por exemplo.

Nesse sentido, pode-se delinear as seguintes situações-tipo[63]: (i) comunicação intermediada por provedor de aplicação de internet, em que o teor das mensagens e dados só pode ser acessado pelo(s) usuário(s) que possui(em) a chave criptográfica pertinente; (ii) dados de usuários armazenados e processados em servidores ou bases de dados de ente responsável, ou terceiro a ele interligado, encriptados por iniciativa ou determinação do próprio provedor de serviço, que pode acessar a chave de decriptação; e (iii) informações cifradas por ato do usuário e armazenadas e processadas em servidores ou bases de dados de provedor de serviço de computação em nuvem, o qual não tem acesso à correspondente chave criptográfica.

Tendo em vista o que até então se afirmou a respeito da criptografia ponta a ponta e das duas perspectivas de análise da cifragem de dados, há que se retomar o problema aventado inicialmente: pode a encriptação de dados ser reputada como técnica de anonimização quando o dado tiver caráter pessoal? A partir dessa questão, poderemos responder se se aplica aos dados criptografados o regime jurídico de proteção de dados pessoais.

62. O aplicativo Signal, a título exemplificativo, deixa o histórico de mensagens criptografados e armazenados nos dispositivos dos próprios usuários (SIGNAL. *Signal terms & Privacy policy*. Disponível em: [https://signal.org/legal/#terms-of-service]. Acesso em: 11.08.2018). O propósito desse provedor de aplicação de internet é armazenar o mínimo possível de dados dos usuários, mas se lê nos termos do serviço: "For the purpose of operating our Services, you agree to our data practices as described in our Privacy Policy, as well as the transfer of your encrypted information and metadata to the United States and other countries where we have or use facilities, service providers or partners. Examples would be Third Party Providers sending you a verification code and processing your support tickets".

63. Não se trata de uma tentativa de exaurir os possíveis casos que na prática podem ocorrer. Assim, para uma finalidade didática assume-se o risco de incorrer numa criticável simplificação da realidade.

2503_book.indb 117 23/11/2018 16:38:00

Para tentar responder à questão, antes, deve-se ter em mente, com base nas situações-tipo anteriormente traçadas, as hipóteses básicas em que está em jogo o tratamento de dados pessoais aos quais se aplicam técnicas criptográficas.

Na primeira situação, a cifragem do conteúdo das mensagens comunicadas não diz respeito propriamente ao tratamento de dados pessoais; o fluxo informacional em questão pode, por exemplo, estar no âmbito do sigilo das comunicações privadas, tal como ocorre com o uso de aplicações de mensagens instantâneas ou de correio eletrônico. De informações pessoais se pode cogitar, porém, no que tange a dados do perfil ou conta criada pelo usuário ou sobre as comunicações travadas (metadados), que normalmente não são criptografados.

Já na situação descrita no item *ii,* a cifragem em repouso dos dados como medida de segurança pode ser adotada tanto (a) pelo *controlador*[64] como (b) pelo *operador*[65], ambos os agentes de tratamento de informações pessoais. Na hipótese levantada no item *iii*, por sua vez, dados pessoais podem ser encriptados pelo usuário antes de tratados pelo provedor do serviço de armazenamento por computação em nuvem.

Sustentar que a criptografia aplicada a dados pessoais os anonimiza somente é admissível se os dados cifrados não mais se associarem a pessoa natural identificada ou identificável, por meios suscetíveis de ser razoavelmente utilizados, de forma permanente e irreversível. Não atendendo aos elementos caracterizadores dos dados anonimizados, a informação é reputada pessoal e o regime da proteção de dados é aplicável.

Nessa matéria há uma premissa por todos adotada, inclusive pela doutrina, que defende ser a cifragem de dados um modo de anonimização, observados certos critérios: dado pessoal criptografado permanece com o mesmo predicado para o agente que detém a chave criptográfica (privada)[66]. Como afirmado por Spindler e Schmechel, "[a] questão relevante é se dado cifrado deve tam-

64. A LGPD define esse agente no artigo 5º, VI, como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

65. Nos termos da LGPD, operador é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (artigo 5º, VII).

66. SPINDLER, Gerald; SCHMECHEL, Philipp. Personal data and encryption in the European General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, v. 7, p. 171, 2016.

2503_book.indb 118 23/11/2018 16:38:00

bém ser dado pessoal para o controlador ou operador que não tem acesso à chave de decriptação"[67].

Para estes autores, dados pessoais cifrados podem ser tomados por dados anonimizados. Na construção do raciocínio, entretanto, elegeu-se a perspectiva *relativa* da identificabilidade da pessoa, é dizer, "apenas o conhecimento e as possibilidades do *controlador* para identificar o titular dos dados devem ser levados em consideração"[68] (grifou-se). Afasta-se, portanto, os esforços possíveis de *qualquer pessoa* em decriptar a informação ou obter por outra via lícita o *plaintext*.

A esse ponto de partida acrescenta-se proposta que inclui três critérios para avaliar se os mecanismos para decifrar os dados e identificar o titular das informações pessoais são suscetíveis de ser razoavelmente utilizados: (i) a força do algoritmo de cifragem utilizado; (ii) a extensão da chave de encriptação (*e. g.*, 128 ou 256 bits); e (iii) a segurança do gerenciamento de chaves[69]. Por fim, deve-se também lançar no esquema interpretativo os aspectos contextuais do estado da arte das tecnologias criptográficas.

Importantes ressalvas devem ser feitas a essa orientação.

Primeiramente, este trabalho não observa a perspectiva relativa sobre a noção de identificabilidade da pessoa humana, como se vê das linhas propedêuticas sobre o conceito de dado pessoal escritas no item n. 2. Leva-se em consideração, portanto, os esforços e meios razoáveis empregados por outros sujeitos que não o controlador na apreciação da potencial identificação do titular dos dados e superação das técnicas criptográficas utilizadas.

Além disso, há certa incompatibilidade da proposição com o *princípio da segurança,* ou *da integridade e confidencialidade*, consagrado nos mais recentes quadros normativos da proteção dos dados pessoais[70]. Considerando a LGPD

67. SPINDLER, Gerald; SCHMECHEL, Philipp. Personal data and encryption in the European General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, v. 7, p. 171, 2016. Tradução livre de: "The relevant question is whether encrypted data shall also be personal data for a controller or processor who does not have access to the decryption key [...]".

68. Ibidem, p. 172. Tradução livre de: "[...] only the knowledge and possibilities of the controller to identify the data subject shall be taken into account".

69. Ibidem, p. 172.

70. Prevê a LGPD: "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...] VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autori-

2503_book.indb 119 23/11/2018 16:38:00

no Brasil e a GDPR na União Europeia, nota-se que controladores e operadores têm o dever de adotar práticas e medidas de segurança aptas, de acordo com o estado da técnica, a resguardar as informações de natureza pessoal contra acessos não autorizados, destruição, ou outros riscos e tratamentos ilícitos[71]. O Regulamento europeu prescreve, em seu artigo 32, o dever dos agentes de tratamento de dados implementarem adequadas medidas técnicas e organizacionais de segurança informacional, tendo em vista a gradação ou nível de risco causado pela atividade de tratamento de informações pessoais a direitos e liberdades fundamentais dos titulares dos dados. A encriptação é expressamente mencionada pelo legislador europeu como *modo de cumprimento de tal dever*, segundo as disposições legais inscritas nos artigos 32, 1, e 25, 1.

Deve-se atentar, ainda, para o fato de que os três sugeridos critérios são, como os próprios autores citados afirmam, alguns parâmetros para avaliar a robustez da segurança computacional de um sistema criptográfico[72]. Não parece ter pertinência temática aí incidente com a ideia de identificabilidade de um indivíduo. A bem da verdade, verifica-se uma incoerência, ao servir-se dos critérios mencionados, com a própria razão de ser da criptografia: se o sistema não oferecer segurança aos dados cifrados, seja por falha intencional (*backdoor*) ou por falha encontrada ulteriormente, os dados em questão podem ser considerados pessoais. A Criptografia moderna, como um ramo da área de Segurança Computacional, tem a particularidade de ser uma *ciência autofágica*, é dizer, "o progresso é promovido pela demonstração da vulnerabilidade das técnicas, com posterior substituição por técnicas mais seguras que resistem a adversários mais poderosos"[73].

---

zados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". A GDPR, por seu turno, estabelece: "Article 5. *Principles relating to processing of personal data*. 1. Personal data shall be: [...] (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')".

71. Ver artigo 46 da LGPD.

72. Cf. GILL, Lex; ISRAEL, Tamir; PARSONS, Christopher. *Shining a light on the encryption debate*: a Canadian field guide. [s.l]: Citizen Lab/Samuelson-Glushko CIPPIC, 2018. p. 3.

73. ARANHA, Diego F. O que é criptografia fim-a-fim e o que devemos fazer a respeito. Acrescenta o autor: "A evolução da Criptografia segue então o observado em outras ciências, com a distinção de que técnicas obsoletas tornam-se também perigosas, por

2503_book.indb 120 23/11/2018 16:38:00

Afigura-se, portanto, mais adequado pensar o dado cifrado como informação pessoal *prima facie*. O Grupo de Trabalho de Proteção de Dados do artigo 29 tratou a utilização das técnicas criptográficas como forma de pseudonimização de dados, constituindo a encriptação em medida de segurança para proteção de dados pessoais a ser adotada pelo controlador e pelo operador. É o que se vê nos seus Pareceres 04/2007[74] e 05/2014[75]. A cifragem de informações se dá de forma que os dados deixam de poder se conectar a um titular de dados específico sem recorrer a informações suplementares, isto é, à chave de decriptação.

Sendo, portanto, o dado pessoal encriptado um dado que pode ser caracterizado como dado pseudonimizado, pode-se aplicar um regime modulado ou particularizado aos dados de caráter pessoal criptografados. Tomando uma vez mais a GDPR, por exemplo, conforme disposto no artigo 34, 3, *a*, não haverá o dever de notificação de incidente de segurança que resulte em altos riscos a direitos e liberdades fundamentais do titular dos dados, se o controlador tiver implementado apropriadas técnicas de segurança, tal como a encriptação dos dados[76].

4. Considerações finais

Análises jurídicas sobre a criptografia costumam apresentar como pano de fundo um cenário de colisão de interesses juridicamente relevantes, representados, de um lado, pela tutela da privacidade, e de outro, pela defesa do inte-

fornecer falsa sensação de segurança aos que contam com sua segurança para depositar segredos. O esforço de atacar técnicas criptográficas para antecipar e prevenir eventuais ataques reais com interesses diversos é estudado pela Criptoanálise e representa etapa crucial na forma como essa ciência progride".

74. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 4/2007 on the concept of personal data*. Bruxelas: [s. n.], 2007. p. 18-20. Disponível em: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf]. Acesso em: 21.08.2018.

75. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 5/2014 on Anonymisation techniques*. Bruxelas: [s. n.], 2014. p. 20-22. Disponível em: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf]. Acesso em: 24.08.2018.

76. "3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; [...]".

2503_book.indb 121 23/11/2018 16:38:00

resse da segurança pública e dos poderes de polícia do Estado. A declaração de Christopher Wray, anteriormente citada, observa essa abordagem com precisão. Contudo, uma tal formulação possui frágil sustento: além de as próprias autoridades de segurança pública necessitarem de tecnologias criptográficas para o bom desempenho de suas atividades[77], é já crítica a demanda por segurança nos fluxos informacionais mediados pelas atuais infraestruturas de informação e comunicação[78] – tamanha é a exigência, que a própria integridade psicofísica de pessoas pode estar em jogo[79].

Deve-se superar de todo a o falso antagonismo entre privacidade *v.* segurança coletiva, tal como se procura fazer neste trabalho. As implementações de tecnologias criptográficas são medidas que promovem igualmente o princípio da segurança e a privacidade e proteção de dados, de sorte que a cifragem de dados pessoais não pode se reputada, por si só, técnica de anonimização de informações que afaste a aplicação do regime de proteção de dados pessoais.

Nos casos concretos, deve ser analisado se os dados criptografados, a partir da execução do protocolo criptográfico desenhado, não mais se vinculam a pessoa natural identificada ou identificável, por meios suscetíveis de ser razoavelmente utilizados, de forma permanente e irreversível. Ainda que cifrados, *prima facie* os dados são de caráter pessoal, pseudonimizados, porém; aplicável, então, o estatuto de proteção de dados pessoais, mesmo que de forma modulada.

77. As tecnologias criptográficas são essenciais também para as autoridades estatais na condução de atividades sigilosas e investigações, e para segurança de suas próprias comunicações. No direito brasileiro, a Lei de Acesso à Informação – LAI (Lei 12.527/2011) e seu decreto regulamentador (Decreto 7.845, de 14 de novembro de 2012) dispõe sobre medidas e procedimentos de segurança para o tratamento de informações sigilosas (artigos 25 e 26 da LAI). O decreto determina que nos sistemas informáticos em houver tratamento de informação considerada *classificada*, deverão ser utilizados *recursos criptográficos* adequados ao nível de sigilo (artigo 38), sendo que as operações de cifração e decifração de tais dados requer o uso de algoritmos de Estado. Conforme o artigo 2º, I, do mesmo decreto, algoritmo de Estado é a "função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo federal".

78. Sobre as infraestruturas de informação e comunicação ver HILDEBRANDT, Mireille. A Vision of Ambient Law. In: BROWNSWORD, R.; YEUNG, K. (Ed.). *Regulating technology*: legal futures, regulatory frames and technological fixes. Portland: Bloomsbury, 2008. p. 175-191.

79. São vários os casos denunciados de assédio sofrido por mulheres de aplicações de *smart home*: BOWLES, Nellie. Thermostats, locks and lights: digital tools of domestic abuse. *New York Times*, 2018. Disponível em: [www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html]. Acesso em: 30.09.2018.

2503_book.indb 122 23/11/2018 16:38:00

Referências

ADRIAANS, Pieter. Information. *The Stanford Encyclopedia of Philosophy* – Edward N. Zalta (Ed.). Disponível em: [https://plato.stanford.edu/archives/fall2013/entries/information/]. Acesso em: 27.08.2018.

ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 5/2014 on Anonymisation techniques*. Bruxelas: [s. n.], 2014. p. 6-7. Disponível em: [http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf]. Acesso em: 24.08.2018.

BIONI, Bruno. *Xeque-mate:* o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: GPOPAI, 2015.

BOWLES, Nellie. Thermostats, locks and lights: digital tools of domestic abuse. *New York Times*, 2018. Disponível em: [https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html]. Acesso em: 30.09.2018

BUCHAN, Lizzy. *Digital IDs needed to end 'mob rule' online, says security minister Ben Wallace*. Disponível em: [www.independent.co.uk/news/uk/politics/online-digital-identification-mob-rule-online-security-minister-ben-wallace-a8390841.html]. Acesso em: 18.06.2018.

DELFS, Hans; KNEBL, Helmut. *Introduction to cryptography:* principles and applications. 2. ed. Berlin-Heildelberg-New York: Springer, 2007.

DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. Rio de Janeiro: Renovar, 2006.

ESAYAS, Samson Yoseph. The role of anonymisation and pseudonymisation under the EU data privacy rules: beyond the 'all or nothing' approach. *European Journal of Law and Technology*, v. 6, n. 2, 2015.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS; COUNCIL OF EUROPE. *Handbook on European Data Protection Law*. Luxembourg: Publications Office of the European Union, 2018.

FINOCCHIARO, Giusella. Anonimato. *Digesto delle discipline privatistiche* – Sezione civile. Aggiornamento. Torino: UTET, 2010.

GILL, Lex; ISRAEL, Tamir; PARSONS, Christopher. *Shining a light on the encryption debate*: a Canadian field guide. [s.l]: Citizen Lab/Samuelson-Glushko CIPPIC, 2018.

HILDEBRANDT, Mireille. A vision of ambient law. In: BROWNSWORD, R.; YEUNG, K. (Ed.). *Regulating technology*: legal futures, regulatory frames and technological fixes. Portland: Bloomsbury, 2008.

HUMAN RIGHTS COUNCIL. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*,

2503_book.indb 123 23/11/2018 16:38:00

2016. Disponível em: [www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Privatesectorinthedigitalage.aspx]. Acesso em: 20.06.2018.

IDENTITY THEFT RESOURCE CENTER. *2017 Annual Data Breach Year-end Review*. [S. l.], 2018. Disponível em: [www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf]. Acesso em: 20.06.2018.

KERR, Orin S.; SCHNEIER, Bruce. Encryption Workarounds. *The Georgetown Law Journal*, v. 106, p. 989-1019, 2018.

MILLARD, Christopher (Ed.). *Cloud computing law*. Oxford: Oxford University Press, 2013. *E-book*.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. *How to break anonymity of the Netflix Prize dataset*. 2007. p. 3. Disponível em: [https://goo.gl/RxggOU]. Acesso em: 30.08.2018.

NOUMEIR, Rita; LEMAY, Alain; LINA, Jean-Marc. Pseudonymization of radiology data for research purposes. *Journal of Digital Imaging*, v. 20, n. 3, p. 284-295, 2007.

OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *UCLA Law Review*, n. 57, p. 1701-1777, 2010.

PAAR, Christof; PELZL, Jan. *Understanding cryptography:* a textbook for students and practitioners. London: Springer, 2010.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 40-81, 2018.

RODOTÀ, Stefano. *Il mondo nella rete:* quali i diritti, quali i vincoli. Roma-Bari: Laterza, 2014.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII problem: privacy and a new concept of personally identifiable information. *New York University Law Review*, v. 86, p. 1814-1894, dec. 2011.

SIGNAL. *Signal terms & Privacy policy*. Disponível em: [https://signal.org/legal/#terms-of-service]. Acesso em: 11.08.2018.

SPINDLER, Gerald; SCHMECHEL, Philipp. Personal data and encryption in the European General Data Protection Regulation. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, v. 7, p. 163-177, 2016.

SWEENEY, Latanya. Simple demographics often identify people uniquely. *Carnegie Mellon University*, Data Privacy Working Paper 3, Pittsburgh, 2000.

TRUCCO, Lara. *Introduzione allo studio dell'identità individuale nell'ordinamento costituzionale italiano*. Torino: Giappichelli, 2004.

VIOLA, Mario; DONEDA, Danilo; ANDRADE, Norberto N. G. de. Dados anônimos e tratamento de dados para finalidades distintas: a proteção de dados pessoais sob uma ótica civil-constitucional. In: TEPEDINO, Gustavo; FA-

2503_book.indb 124 23/11/2018 16:38:00

CHIN, Luiz E. (Org.). *Pensamento crítico do direito civil brasileiro*. Curitiba: Juruá, 2011.

VOLZ, Dustin. *FBI chief calls unbreakable encryption 'urgent public safety issue'*, 2018. Disponível em: [www.reuters.com/article/us-usa-cyber-fbi/fbi-chief-calls-unbreakable-encryption-urgent-public-safety-issue-idUSKBN1EY1S7]. Acesso em: 27.06.2018.

WIKIPEDIA. *Disk encryption*. Disponível em: [https://en.wikipedia.org/wiki/Disk_encryption]. Acesso em: 10.09.2018.

ZENO-ZENCOVICH, Vincenzo. Informazione (profili civilistici). *Digesto* – Sezione Civile. Torino: UTET, 1993. v. IX.

2503_book.indb 125 23/11/2018 16:38:00