OBSERVATÓRIO DA LGPD
UNIVERSIDADE DE BRASÍLIA

ANÁLISE COMPARADA
LGPD E GDPR

ORGANIZADORES

LAURA SCHERTEL MENDES

GIOVANNA MILANESE

FELIPE ROCHA DA SILVA

TAYNÁ FROTA DE ARAÚJO

ISABELA MARIA ROSAL

PAULO RICARDO SANTANA

EDUARDA COSTA

ELIS BRAYNER

ANUÁRIO DO OBSERVATÓRIO DA LGPD DA UNIVERSIDADE DE BRASÍLIA

VOLUME 1

Universidade de Brasília
Faculdade de Direito

Anuário do Observatório da LGPD da Universidade de Brasília

Análise comparada entre elementos da LGPD e do GDPR

Volume 1
Brasília-DF
2023

Anuário do Observatório da LGPD da Universidade de Brasília: Análise comparada entre elementos da LGPD e do GDPR.

Para esclarecimentos sobre esta obra, entrar em contato com observatorio.lgpd.unb@gmail.com

Volume 1

Organização
Coordenação Geral: prof.ª Laura Schertel Mendes;
Coordenação Adjunta: Giovanna Milanese;
Coordenação de Pesquisa: Felipe Rocha e Tayná Frota de Araújo;
Revisão e Organização: Eduarda Costa Almeida, Elis Bandeira A. Brayner, Isabela Maria Rosal e Paulo Ricardo da Silva Santana.

Informações

Observatório da LGPD/Unb
Faculdade de Direito
Universidade de Brasília
Campus Universitário Darcy Ribeiro, CEP: 70.910-900, Brasília-DF, Brasil

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Central da Universidade de Brasília – BCE/UNB)

A636 Anuário do Observatório da LGPD da Universidade de Brasília [recurso eletrônico] : análise comparada entre elementos da LGPD e do GDPR / organização Laura Schertel Mendes … [et al.]. – Brasília : Universidade de Brasília, Faculdade de Direito, 2024. 2 v.

Inclui bibliografia. Modo de acesso: World Wide Web.

ISBN 978-65-00-92398-8 (v. 1).

ISBN 978-65-00-92399-5 (v. 2).

1. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 2. Universidade de Brasília. 3. Proteção de dados. 4. Direito comparado. I. Mendes, Laura Schertel (org.).

CDU 34

AUTORES

Ana Júlia Prezotti Duarte

Andressa Carvalho Pereira

Angélica Opata Vettorazzi

Gabriel de Araújo Oliveira

Gabriel Cabral Furtado

Eduarda Costa Almeida

Fernanda Passos Oppermann Ilzuka

Isabela de Araújo Santos

Júlia Carvalho Soub

Shana Schlottfeldt

Sofia de Medeiros Vergara

Paulo Ricardo da Silva Santana

Rafael Luís Müller Santos

Wanessa Larissa Silva de Araújo

REVISORES

A realização deste anuário contou com a significativa participação de revisores, que atuaram na avaliação e revisão dos artigos submetidos pelos pesquisadores do Observatório, fornecendo orientações e sugestões de melhoria. Oferecemos nosso mais sincero agradecimento pelas valiosas contribuições de cada um.

Ana Luísa Vogado de Oliveira

Angelo Prata de Carvalho

Davi Ory

Gabriel Fonseca

Isabela Maria Rosal Santos

Maria Cristine Lindoso

Matheus Vinicius Aguiar

Paula Baqueiro

Tainá Aguiar Junquilho

Thiago Guimarães Moraes

SUMÁRIO

SEGURANÇA DA INFORMAÇÃO NO TRATAMENTO DE DADOS PESSOAIS

Paulo Ricardo da Silva Santana [1]

Dispositivo LGPD	Dispositivo RGPD
Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.	**Art. 32.** Segurança do tratamento Levando em consideração o estado da técnica, os custos de implementação e a natureza, escopo, contexto e finalidades do processamento, bem como o risco de probabilidade e severidade variadas para os direitos e liberdades das pessoas físicas, o controlador e o operador devem implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco, incluindo, inter alia, conforme apropriado [...]:

Introdução

É difícil imaginarmos uma esfera da vida humana que não tenha influência da Tecnologia da Informação (TI), tendo em vista a centralidade que os dados exercem na sociedade atual, que é progressivamente sustentada por meios tecnológicos e digitais, orientada pelos dados que produz em volumes e velocidades cada vez maiores.

A segurança da informação, até pouco tempo atrás, estava voltada para a proteção do negócio no âmbito empresarial.[2] Contudo, na sociedade atual, essa disciplina da área de TI tem se direcionado para a proteção de toda e qualquer informação, até mesmo aquelas relativas a informações pessoais.[3] Nesse sentido, conforme as legislações de proteção de dados avançam, a segurança da informação ganha cada vez mais relevância. Se anteriormente as empresas se

[1] Paulo Ricardo da Silva Santana é graduado em Sistemas de Informação pelo Centro Universitário do Distrito Federal (UDF) e em Direito pela Universidade de Brasília (Unb). Coordenador de Pesquisa do Observatório da LGPD/Unb. Membro da comissão de Privacidade e Proteção de Dados da OAB/DF. Advogado e Consultor em Proteção de Dados em FDS Advogados.

[2] A norma internacional ISO 27001:2013, que trata sobre segurança da informação, relaciona incidente de segurança com os riscos às operações de negócio.

[3] A ISO (International Organization for Standardization) acompanhando o cenário internacional com relação à proteção de dados pessoais, atualizou a família de normas ISO 27000 com uma norma específica sobre privacidade, a norma ISO/IEC 27701.

preocupavam apenas em proteger a receita do seu produto comercial, atualmente elas também precisam se atentar para a proteção das informações de seus funcionários, consumidores etc.

No Regulamento Geral sobre a Proteção de Dados (RGPD), a segurança da informação no tratamento de dados pessoais é disciplinada no art. 32, o qual dispõe que os agentes de tratamento devem implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança adequado ao risco. Por sua vez, a Lei Geral de Proteção de Dados (LGPD) trata do tema em seu art. 46, segundo o qual os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Ante a breve exposição supra, pretende-se, neste artigo, realizar um exame comparativo entre casos relacionados à segurança da informação em âmbito europeu e brasileiro. O caso europeu é o Knuddels decidido pela autoridade de proteção de dados do estado alemão de Baden-Württemberg. O caso brasileiro é o recente vazamento de dados da Serasa Experian, ainda em fase investigativa no âmbito administrativo e de conhecimento no âmbito judicial. Por fim, pretende-se ainda realizar alguns breves apontamentos doutrinários sobre o conteúdo da segurança da informação no RGPDe na LGPD.

1. Estudo de caso

1.1. Caso Knuddels GmbH & Co. KG – Armazenamento de senhas em texto simples

Em 28 de novembro de 2018, a *Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*- LfDI Baden-Württemberg, autoridade de proteção de dados do estado alemão de Baden-Württemberg, aplicou penalidade de multa de 20 mil euros à empresa Knudells GmbH & Co. KG, rede social alemã com mais de 1,8 milhão de usuários, por violação da obrigação de garantia da segurança dos dados pessoais com fundamento no art. 32 do GDPR.[4]

Em agosto de 2018, a Knudells sofreu um ataque hacker, ocasionando o vazamento de dados como o apelido dos usuários na rede social (*nickname*), seus verdadeiros nomes, endereço

[4] *LfDI Baden-Württemberg verhängt sein erstes Bußgeld in Deutschland nach der DS-GVO*. *LfDI Baden-Württemberg*. 22 de nov. de 2018. Disponível em: <https://www.baden-wuerttemberg.datenschutz.de/lfdi-baden-wuerttemberg-verhaengt-sein-erstes-bussgeld-in-deutschland-nach-der-ds-gvo> . Acesso em 09 de set. de 2021.

de e-mail e até mesmo seus endereços residenciais.[5] Tão logo soube do ataque, a empresa comunicou seus usuários do incidente ocorrido fornecendo instruções para que realizassem a alteração de suas senhas de acesso.

Em comunicado à imprensa, a Knudells tornou pública a ocorrência do ciberataque e, por meio de várias redes sociais, pediu desculpas aos seus usuários pelo incidente. Além dessas medidas, a própria empresa elaborou um relatório acerca do incidente de segurança ocorrido e apresentou à LfDI Baden-Württemberg.[6] Por fim, prosseguiu com investimentos para atualização da infraestrutura com o fim de melhorar a segurança.

Tanto na investigação conduzida pela LfDI Baden-Württemberg, quanto pelas informações fornecidas pela Knudells, verificou-se que as senhas dos usuários eram armazenadas em arquivos de texto simples e sem criptografia.[7] Este foi o ponto central discutido no caso.

Em sua decisão, a LfDI Baden-Württemberg concluiu que, ao armazenar senhas não criptografadas, a Knudells não protegeu estes dados por meio de medidas técnicas e organizacionais adequadas para impedir o acesso de pessoas não autorizadas e, portanto, violou sua obrigação de garantir a segurança dos dados ao processar dados pessoais, em conformidade com o art. 32, 1 do RGPD.

A Knuddels foi poupada de uma penalidade mais severa em decorrência de uma estratégia eficaz de resposta ao incidente de segurança, notificando seus usuários de forma rápida, procurando a autoridade competente e fornecendo as informações necessárias para a condução da investigação, o que foi levado em consideração para o estabelecimento do valor da multa, seguindo o disposto no art. 83, 2 do RGPD.[8] No caso em tela, a boa-fé do infrator, a vantagem auferida, o grau do dano, a não reincidência e a cooperação com as autoridades foram determinantes na aplicação da sanção.

---

[5] Knuddels von Hackern angegriffen. Der Spiegel. 08 de set. de 2018. Disponível em <https://www.spiegel.de/netzwelt/web/knuddels-de-von-hackern-angegriffen-a-1227170.html>, acesso em 31 de ago. de 2021.

[6] Chat-Plattform muss nach Hackerangriff Bußgeld zahlen. Der Spiegel. 21 de nov. de 2018. <https://www.spiegel.de/netzwelt/web/knuddels-chat-plattform-muss-nach-hackerangriff-bussgeld-zahlen-a-1239776.html>, acesso em 31 de ago. de 2021.

[7] Criptografia é comumente utilizada para aumentar a segurança de dados em geral. Por meio da dela um dado é cifrado, de modo que apenas quem possui uma chave, pode decifrá-lo e acessar o seu c conteúdo.

[8] Este mesmo artigo encontra paralelo com o art. 52, §1º da LGPD.

1.2. *Caso Serasa Experian* - Vazamento de dados

Diferente do caso alemão, o caso do suposto vazamento de dados da Serasa Experian ainda está sendo analisado pela ANPD e vem sendo acompanhado pelo Ministério Público e por órgãos de defesa do consumidor sendo também objeto de Ação Civil Pública (ACP nº 5002936-86.2021.4.03.6100) que tramita na 22ª vara cível federal de São Paulo, ajuizada pelo Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, Compliance e Segurança Da Informação – SIGILO.

Tal como o caso Knudells, o presente caso versa sobre o vazamento de dados, supostamente das bases de dados do Serasa Experian, se diferenciando essencialmente daquele pela sua dimensão e pela natureza dos dados vazados, em que se reporta que 223 milhões de brasileiros tiveram expostos dados pessoais como CPF, foto de rosto, salário e score de crédito.[9] O vazamento foi inicialmente reportado pela startup brasileira PSAFE, logo após o lançamento de um produto contra vazamento de dados de empresas.[10] A denúncia da empresa de cibersegurança provocou a reação de diversas entidades e órgãos de defesa do consumidor. Nesse contexto, o Instituto SIGILO, associação voltada a assuntos relacionados ao direito à privacidade, ajuizou uma Ação Civil Pública.

Na ACP, o Instituto SIGILO argumentou na inicial que, muito embora a Serasa Experian negue ser a origem do vazamento, há indícios suficientes de sua responsabilidade em razão de os dados estarem associados a serviços oferecidos exclusivamente pela ré, além do fato de o nome do arquivo de banco de dados vazado ser "JBR - Serasa Experian - Full Service".

Ainda segundo o Instituto SIGILO, a responsabilidade da Serasa Experian decorre do fato da empresa ter se omitido de tomar todas as medidas razoáveis necessárias para prevenir atividades que pudessem resultar na violação da legislação, qual seja, o dever objetivo de cuidar e de aplicar as melhores práticas de segurança da informação aos dados conforme o disposto art. 46 da LGPD.

---

[9] VENTURA, Felipe. Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava. Tecnoblog. Disponível em: <https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/amp/> . Acesso em 1 set. 2021

[10] O CEO da PSAFE, Marco De Mello informou que em outubro de 2020, a empresa lançou o "*Dfndr Enterprise*", solução contra o vazamento de dados de empresas. Ao varrer a dark web, o sistema de inteligência artificial de monitoramento alertou para o vazamento de 40 milhões de CNPJs. Sem dar muitos detalhes, De Mello informou que o primeiro passo foi validar os vazamentos a partir de uma amostra de dados coletada com o criminoso pela dark web. Ver mais em SAMBRANA, Carlos. Uma catástrofe digital se aproxima. E nem as empresas e as pessoas se ligaram. Neofeed. 05 de fev. de 2021. Disponível em <https://neofeed.com.br/blog/home/uma-catastrofe-digital-se-aproxima-e-nem-as-empresas-e-as-pessoas-se-ligaram>, Acesso em 15 de set. de 2021.

Em sede de contestação, a Serasa Experian alegou que no exame de sua infraestrutura, realizado por uma auditoria especializada, não se verificou indícios de vazamento massivo de dados. Além do mais, foi alegado que a Serasa possui os recursos técnicos adequados para prevenir, detectar e conter incidentes de vazamento de dados. A ré argumentou ainda que prestou os esclarecimentos necessários à ANPD, executou todas as rotinas previstas em seus protocolos internos e intensificou todas as medidas de monitoramento, verificação e identificação, previstas em suas diretrizes internas.

Colocando os casos lado a lado, é importante observar a diferença da condução dos incidentes pela Serasa Experian e a Knudells, especialmente com relação a notificação das pessoas afetadas. Justo mencionar que no caso alemão, a responsabilidade da empresa estava clara em razão dos dados vazados, até mesmo pelo reconhecimento da própria Knudells. Por sua vez, no caso da Serasa Experian há a controvérsia em torno da origem do vazamento, isto porque não só pelo fato de a Serasa ter negado ser a fonte do vazamento como também pelo fato de que, conforme apontado pela ANPD em sua contestação, ao analisar amostra do vazamento, o Gabinete de Segurança Institucional da Presidência da República (GSI) indicou que o vazamento seria uma mescla de diversas bases de dados do setor privado.

Ainda que a origem não tenha sido exclusiva da Serasa Experian, se das amostras analisadas se reconheceu dados exclusivamente tratados por ela, conforme aponta o Instituto SIGILO na inicial, a notificação aos titulares afetados deveria ter sido realizada, devendo a responsabilidade individual ser apurada em momento posterior, observando o devido processo legal, tal como impõe o art. 52, §1º da LGPD. A comunicação ao titular de incidente de segurança referente a seus dados pessoais não deve ser interpretada como uma assunção de culpa, mas sim como respeito e cumprimento às disposições da LGPD, além de demonstrar boa-fé do controlador que, enquanto princípio, deve ser observada em todas as atividades de tratamento de dados pessoais.[11] A ausência de notificação dos titulares por parte da Serasa Experian, ainda que em fase investigativa, diante dos fatos já postos, indica, além de violação diretamente ao art. 48, §1º da LGPD, ofensa aos seus princípios, tal como o da transparência e da prestação de contas.

Contudo, o que se verificou foi que a própria ANPD, em detrimento dos titulares afetados, ratificou a argumentação da Serasa Experian quando, ao ser questionada sobre a notificação dos titulares de dados, afirmou que ainda seria preciso aguardar a correta

[11] Art. 6º, caput da LGPD.

identificação dos controladores responsáveis. Decerto que a ANPD não pode exigir o cumprimento de uma obrigação sem que seja apurada, por meio de processo adequado, a devida responsabilidade do controlador. Contudo, seria importante que em sua atuação junto à Serasa Experian, a ANPD orientasse a empresa no sentido de comunicar aos titulares de dados pessoais afetados sobre o vazamento de dados, o que poderia ser feito deixando claro aos titulares que o caso ainda estaria em fase investigativa com relação à origem. Como se verá adiante, a notificação dos titulares é importante não somente por questões de transparência e prestação de contas, mas também porque possibilita que o próprio titular de dados tome medidas de proteção. Diante do papel da agência, da extensão do vazamento, dos riscos envolvidos aos titulares e dos elementos da atuação da ANPD no caso em tela, enseja preocupação quanto aos próximos incidentes de segurança que possam surgir.

2. Doutrina

A segurança da informação é definida como preservação da confidencialidade, integridade e disponibilidade da informação.[12] Importante destacar que não há distinção entre o formato da informação, de modo que ela pode estar em meio digital ou físico. Em uma sociedade altamente informatizada, quando falamos em medidas técnicas e administrativas, imaginamos medidas aplicáveis aos meios digitais como senhas, criptografia, antivírus, firewall, backups etc. No entanto, é preciso observar que quando falamos em segurança no tratamento de dados, também deve-se incluir as informações em meio físico. A título de exemplo, o acesso identificado em sala de arquivos e a correta eliminação de dados em papel também são exemplos de medidas administrativas que aumentam a segurança da informação e diminuem o risco de acesso não autorizado à informação.

Na União Europeia, a segurança da informação é tratada por meio de normas e regulamentos específicos e de uma agência própria, a ENISA.[13] No Brasil, contudo, conforme observa Laura Schertel, a segurança da informação não compõe uma política pública própria, nem é executada por um órgão centralizado, como na Europa, mas sim faz parte da agenda de diversos órgãos e atores, que realizam iniciativas esparsas e independentes.[14] Algumas normas

[12] HINTZBERGEN, Jules. Fundamentos da Segurança da Informação: com base na ISO 27001 e na ISO 27002/Jule Hintzbergen... [et al]; tradução Alan de Sá - Rio de Janeiro: Brasport, 2018. P. 30.
[13] A ENISA é a Agência da União Europeia para Cybersegurança que tem o papel de contribuir para a elaboração da política e da legislação da UE em matéria de segurança das redes e da informação.
[14] MENDES, Laura Schetel. Segurança da Informação, Proteção de Dados Pessoais e Confiança. Revista de Direito do Consumidor, São Paulo, vol. 90, p245-261, nov.-dez.2013. p. 249.

como o Código de Defesa do Consumidor, o Marco Civil da Internet (MCI) e até mesmo o Código Penal trazem disposições importantes sobre segurança da informação, porém, é na LGPD que o tema ganha notável destaque, muito em razão de sua interdependência[15] com a proteção de dados pessoais.

Além de um capítulo dedicado ao tópico (VII), a segurança também é referenciada nos arts. 12, §3º; 13, caput e §2º; 34; 38 parágrafo único; 40; 44; 50; e 55-J. Ademais, assim como o RGPD, a LGPD também reconheceu a segurança como um princípio,[16] segundo o qual o tratamento de dados pessoais deve observar a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.[17]

2.1. Requisitos mínimos de segurança

Da leitura do art. 46, Fabiano Menke e Guilherme Goulart, apontam para o fato de que o referido artigo traz um conceito jurídico indeterminado ao impor a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais. Segundo os autores, diante de múltiplas situações envolvidas nos sistemas utilizados, não parece simples indicar o que é uma medida apta.[18] Esta lacuna poderá ser suprida por meio de regulamentos futuros expedidos pela própria ANPD, seguindo o disposto no §1º do mesmo artigo.

Inicialmente, embora a indeterminação descrita acima possa parecer problemática, a disposição do art. 46, §1º viabiliza a expedição de regulamentos conforme as especificidades de cada setor. Desse modo, setores que tratam dados pessoais com maior potencial de afetar os titulares, como o da saúde e o financeiro, por exemplo, podem receber orientações mais precisas da ANPD quanto aos requisitos mínimos de segurança a serem observados no tratamento de dados pessoais.

[15] Ibid. p. 247. Sobre interdependência entre segurança e proteção de dados pessoais, Laura Schertel afirma que a proteção da privacidade e a política de segurança da informação formam, duas faces da mesma moeda; a efetividade de uma depende da efetividade da outra.
[16] A segurança também tem status de princípio no Marco Civil da Internet em seu art. 3º, inciso V.
[17] Art. 6º, VII da LGPD.
[18] MENKE, Fabiano. GOULART, Guilherme D. Segurança da Informação e vazamento de dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 347.

Por seu turno, diferente do que faz a LGPD, o RGPD traz, nas alíneas do seu art. 32, os parâmetros mínimos a serem adotados pelos controladores e subcontroladores para assegurar um nível mínimo de segurança adequado ao risco envolvido no tratamento de dados: a) a pseudonimização e a cifragem dos dados pessoais; b) a capacidade de assegurar confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) a capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais em tempo razoável no caso de um incidente físico ou técnico; e d) um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

Paul Voigt e Axel Bussche observam que o RGPD apresenta uma abordagem baseada em risco para determinar quais medidas técnicas e organizacionais são apropriadas em uma determinada situação.[19] O nível necessário de segurança de dados deve ser identificado caso a caso por meio de uma avaliação de risco objetiva. A avaliação do risco é importante na adoção de medidas de segurança, especialmente quando o tratamento abarca dados com potencial de discriminação, como é o caso dos dados pessoais sensíveis.[20] No entanto, o risco não decorre somente do tipo de dados envolvido, como também dos controladores e até mesmo de terceiros. Neste sentido, dispõe o Considerando nº 76 do RGPD que a probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Embora de forma mais tímida, o risco também é mencionado pela LGPD ao se considerar as medidas de segurança a serem adotadas.[21]

Quanto aos requisitos mínimos de segurança, enquanto novos regulamentos não são estabelecidos pela ANPD, o Decreto nº 8.771/2016 que regulamenta o MCI pode ser aplicado de forma subsidiária, ao menos nas situações que envolvem o tratamento de dados pessoais no meio digital. O referido decreto possui uma sessão sobre padrões de segurança e sigilo dos registros, dados pessoais e comunicações privadas, na qual estabelece em seu art. 13 sobre as seguintes diretrizes de segurança: (I) o estabelecimento de controle estrito sobre o acesso aos dados; (II) a previsão de mecanismos de autenticação de acesso aos registros; III - a criação de

[19] VOIGT, Paul. BUSSCHE, Axel. The EU General Data Protecion Regulation (GDPR): A Practical Guide. Berlim. Springer.2017. p. 40.
[20] Art. 5º, II da LGPD.
[21] o art. 50, §1 da LGPD, impõe que ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado; e (IV) o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

2.2. Privacy by Design e Privacy by default

O §2º do art. 46 da LGPD cita que as medidas de que trata o caput deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução. Deste dispositivo se observa a positivação do conceito *privacy by design* (privacidade desde a concepção).[22] Bruno Bioni esclarece que o *privacy by design* é a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles serem embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais.[23] Nessa perspectiva, muitas são as medidas que podem ser adotadas para elevar a proteção de dados pessoais tais como criptografia, anonimização e pseudonimização dos dados.

Em relação ao *privacy by default* (privacidade por padrão), o *European Data Protecion Board* – EDPB [24] elucida que *by default* refere-se a fazer escolhas em relação aos valores de configuração ou opções de processamento que são definidos ou prescritos em um sistema de processamento, como um aplicativo de software, serviço ou dispositivo.[25] Nesse sentido, a título de exemplo, podemos citar as autorizações que são solicitadas ao usuário para permitir acesso à câmera ou ao microfone durante a utilização de algum aplicativo de celular, o que implica que por padrão, os aplicativos instalados não possuem acesso aos dados pessoais, devendo o usuário escolher se permite acesso ou não.

No RGPD, tanto o *privacy by design* quanto *privacy by default* são tratados no art. 25, 1 e 2, respectivamente. O regulamento europeu é mais detalhado sobre ambos e dispõe,

---

[22] CAVOUKIAN, Ann. Privacy by Design: the 7 fundational Principles. Jan. de 2011. p. 1. O *privacy by design* é um conceito criado pela pesquisadora canadense Ann Cavoukian, para quem a garantia de privacidade deve, idealmente, se tornar o padrão de uma organização modo de operação.

[23] BIONI, Bruno Ricardo. Proteção de Dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 234.

[24] O European Data Protection Board (EDPB) é o Comitê Europeu para a Proteção de Dados (CEPD). É um organismo europeu independente que visa contribuir para a aplicação coerente de regras em matéria de proteção de dados na União Europeia e promove a cooperação entre as autoridades de proteção de dados da UE.

[25] EDPB. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. 20 de out. 2020. Disponível em <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en> . Acesso em: 08 de set. de 2021.

inclusive, sobre a forma como o controlador pode comprovar o cumprimento das obrigações impostas pelos referidos dispositivos. Importante observar que o item 2 do art. 25 do regulamento europeu enuncia que o responsável pelo tratamento deve aplicar medidas técnicas e administrativas para assegurar que, por padrão (*by default*), só sejam tratados os dados pessoais que forem **necessários para cada finalidade** (grifei) específica do tratamento. Da leitura do dispositivo, denota-se, portanto, que o princípio da necessidade é um percurso essencial para a aplicação de medidas de segurança por padrão. Daí a afirmação de Bruno Bioni de que, apesar de a LGPD não dispor expressamente sobre o *privacy by default*, é possível extraí-lo do princípio da necessidade.[26]

Tanto o *privacy by design* quanto o *privacy by default* se relacionam com as chamadas *Privacy Enhancing Technologies* (PETs), que são tecnologias que facilitam e aprimoram a privacidade, resultando em medidas que protegem os dados pessoais e dão mais poder ao titular sobre seus dados pessoais. Neste sentido, Bruno Bioni assevera que as PETs são capazes de empoderar os cidadãos desempenhando um papel emancipatório.[27]

2.3. Comunicação de Incidente de Segurança

Conforme a norma internacional de segurança da informação ISO 27001:2013, incidente de segurança é indicado por um único ou uma série de eventos de segurança da informação, indesejados ou inesperados, que tenham uma probabilidade significativa de comprometer a operação dos negócios e ameacem a segurança da informação.[28] É uma definição ampla que engloba dados de qualquer natureza.

Partindo desse conceito é possível extrair o sentido de incidentes de segurança relativos a dados pessoais na LGPD. Neste sentido, Camila Jimene entende que, por meio de uma interpretação harmônica da LGPD, incidente de segurança relativo a dados pessoais pode ser interpretado como um acontecimento indesejado ou inesperado, que seja hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações

[26] BIONI, Bruno R.; MONTEIRO, Renato Leite. Proteção de Dados Pessoais Como Elemento de Inovação e Fomento à Economia: O impacto econômico de uma lei geral de dados pessoais. In: Proteção de dados: contexto, narrativas e elementos fundantes / [organização Bruno Ricardo Bioni]. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021. p.356.
[27] BIONI, Bruno Ricardo. Op. cit. 2019. p. 234.
[28] HINTZBERGEN, Jules. Op. cit. 2018. P. 29

acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.[29]

O art. 48 da LGPD informa que o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Este artigo encontra dois correspondentes no RGPD. Isto porque o regulamento europeu possui um artigo para a comunicação com a autoridade de proteção de dados e outro para a comunicação com os titulares, respectivamente os arts. 33 e 34.

Segundo o RGPD, o controlador deve notificar a autoridade de controle sobre um incidente, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento sobre o mesmo. Essa notificação deve ocorrer apenas quando houver elevado risco para os direitos dos titulares. Segundo o Considerando nº 75 do GPDR, os riscos devem ser aferidos com base em uma avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado. Como abordado no tópico 2.1, esse risco é determinado pela natureza, âmbito, contexto e finalidade do tratamento de dados.

A LGPD, diferente do regulamento europeu, trata do prazo de notificação por meio de um conceito mais aberto, devendo a comunicação ser feita em prazo razoável.[30] Já para o titular, o art. 34 do RGPD informa que a comunicação deve ocorrer sem demora injustificada, o que parece repetir a abertura que ocorre no art. 48 da LGPD. O EDPB, na tentativa de jogar luz sobre a questão, afirma que o termo "sem demora injustificada" quer dizer o mais rapidamente possível.[31]

Já com relação às situações que obrigam a notificação de incidente, a exemplo do que também ocorre no art. 34 do RGPD, a LGPD dispõe que nem todo incidente acarretará a obrigação de comunicação, mas apenas aqueles aptos a acarretar risco ou dano relevante aos titulares de dados. A LGPD não orienta quanto aos critérios para se determinar quando um incidente acarreta risco ou dano relevante de modo que os critérios estabelecidos pelo RGPD

[29] JIMENE. Camilla do Vale. Capítulo VII: Da Segurança e das Boas Práticas. p.387. in: LGPD: Lei Geral de Proteção de Dados comentada/coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

[30] Pela redação do art. 48, §1º depreende se que a ANPD possa emitir regulamento sobre prazo razoável. Segundo a página oficial da ANPD, enquanto pendente a regulamentação, recomenda-se que após a ciência do evento adverso e havendo risco relevante, a ANPD seja comunicada com a maior brevidade possível, sendo tal considerado a título indicativo o **prazo de 2 dias úteis**, contados da data do conhecimento do incidente. Ver mais em "Comunicação de incidentes de segurança". ANPD. 22 de fev. de 2021. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>, acesso em 09 de set. de 2021.

[31] EUROPEAN DATA PROTECTION BOARD. Op. Cit. 2018. p. 21.

podem orientar o intérprete da norma brasileira.[32] Nessa direção, Carlos Affonso de Sousa sugere que para verificar o potencial lesivo de um incidente de segurança aos titulares, alguns fatores devem ser considerados. Em primeiro lugar, o tipo de incidente, a natureza, a sensibilidade e o volume dos dados pessoais comprometidos devem ser sopesados nessa equação.[33] O autor acrescenta ainda que, apesar do §2º do art. 48 da LGPD falar em "ampla divulgação do fato em meios de comunicação", é preciso ressaltar que essa medida não substitui a comunicação individual que deve ser direcionada aos titulares das informações.[34]

A comunicação de ocorrência de incidentes aos titulares é importante, não só por questões de transparência, mas também por dar poder ao titular para que possa tentar se preservar diante de possíveis ameaças. Nessa perspectiva, o EDPB esclarece que o objetivo principal da comunicação de incidentes consiste na prestação de informações específicas acerca das medidas que devem ser tomadas para que os titulares possam se proteger. Como observado acima, dependendo da natureza da violação e do risco que coloca, a comunicação no devido prazo irá ajudar as pessoas a tomarem medidas para se protegerem de quaisquer consequências negativas de uma violação.[35]

Considerações Finais

Diante de todo o exposto supra, é possível concluir que com as novas disposições sobre segurança da informação trazidas pela legislação pátria de proteção de dados, uma política nacional ou regulamento geral de segurança da informação parece ser um caminho coerente a fim de proporcionar aos controladores as diretrizes essenciais para que se garanta o mínimo de segurança exigido ao tratamento de dados que a LGPD preceitua.

É evidente que, em matéria de segurança da informação, muito ainda precisa ser ajustado, especialmente em razão de a LGPD ser menos detalhada em relação ao tema que o RGPD. Além dos requisitos mínimos de segurança, é importante que os regulamentos que

[32] A ANPD já deu início à regulamentação da matéria. Ver mais em "ANPD inicia processo de regulamentação sobre incidentes de segurança com tomada de subsídios." 22 de fev. de 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-inicia-processo-de-regulamentacao-sobre-incidentes-de-seguranca-com-tomada-de-subsidios>. Acesso em 22 de set. de 2021.
[33] SOUSA, Carlos Affonso Pereira de. Capítulo XV. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018 p. 435. In: TEMPEDINO, Gustavo. OLIVA, Milena. Lei Geral de Proteção de Dados e duas repercussões no Direito brasileiro. 2ª Edição. Thomson Reuters, Revista dos Tribunais, 2019.
[34] Ibid. p. 435.
[35] EUROPEAN DATA PROTECTION BOARD. *Guidelines on Personal data breach notification under Regulation* 2016/679. 2018. Disponível em < https://ec.europa.eu/newsroom/article29/items/612052/en >. Acesso em: 09 de set. de 2021. p. 21.

possam ser expedidos pela ANPD estimulem ainda mais a adoção de metodologias que aprimoram a privacidade como o *privacy by design* e *privacy by default*. A comunicação de incidentes de segurança é ponto igualmente importante e tem sua urgência de regulamentação, muito em razão de que se constitui de mecanismo que propicia ao titular de dados pessoais o poder de se auto proteger dos possíveis riscos envolvidos em um incidente, em especial quando se trata de vazamento de dados.

Tendo em vista a sua magnitude e sua extensão, o caso do vazamento de dados do Serasa é simbólico para a proteção de dados brasileira. Espera-se da ANPD uma apuração justa e correta dos fatos privilegiando a cooperação com os controladores envolvidos, mas sempre com enfoque na proteção dos titulares de dados. Nesta mesma linha, o Tribunal de Justiça de São Paulo no julgamento da Ação Civil Pública.

O caso Knudells é um caso interessante e significativo, especialmente quando se observa o nível de cooperação que se estabeleceu entre o controlador e a autoridade de controle. A cooperação é incentivada por vários dispositivos da LGPD, por conseguinte, o que se espera é que os controladores brasileiros ajam conjuntamente com a ANPD, não só para a solução de casos de incidente, mas também no sentido de contribuir para fortalecer a proteção de dados no Brasil.

O Brasil, acompanhando a tendência mundial, avançou na proteção de direitos e liberdades individuais com a LGPD. Todavia, será preciso aguardar para ver quais os contornos aos novos direitos e obrigações serão dados pela ANPD e pelos tribunais por meio de suas decisões.

Referências bibliográficas

ANPD. Comunicação de incidentes de segurança. 22 de fev. de 2021. Disponível em <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>, acesso em 09 de set. de 2021.

BIONI, Bruno Ricardo. Proteção de Dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 234.

BIONI, Bruno R.; MONTEIRO, Renato Leite. Proteção de Dados Pessoais Como Elemento de Inovação e Fomento à Economia: O impacto econômico de uma lei geral de dados pessoais. In: Proteção de dados: contexto, narrativas e elementos fundantes / [organização Bruno Ricardo Bioni]. São Paulo: B. R. Bioni Sociedade Individual de Advocacia, 2021

CAVOUKIAN, Ann. Privacy by Design: the 7 fundational Principles. Jan. de 2011. p. 1.

EUROPEAN DATA PROTECTION BOARD. Guidelines 4/2019 on Article 25 Data Protection by Design and by Default. 20 de out. 2020. Disponível em <https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en>. Acesso em: 08 de set. de 2021.

EUROPEAN DATA PROTECTION BOARD. Guidelines on Personal data breach notification under Regulation 2016/679. Disponível em < https://ec.europa.eu/newsroom/article29/items/612052/en>. Acesso em: 09 de set. de 2021.

HINTZBERGEN, Jules. Fundamentos da Segurança da Informação: com base na ISO 27001 e na ISO 27002/Jule Hintzbergen... [et al]; tradução Alan de Sá - Rio de Janeiro: Brasport, 2018. P. 30.

JIMENE. Camilla do Vale. Capítulo VII: Da Segurança e das Boas Práticas. p.387. in: LGPD: Lei Geral de Proteção de Dados comentada [livro eletrônico] / coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

MENDES, Laura Schetel. Segurança da Informação, Proteção de Dados Pessoais e Confiança. Revista de Direito do Consumidor, São Paulo, vol. 90, pp. 245-261, nov.-dez.2013.

MENKE, Fabiano. GOULART, Guilherme D. Segurança da Informação e vazamento de dados. In: DONEDA, Danilo (coord.); SARLET, Ingo Wolfgang (coord.); MENDES, Laura Schertel (coord.); RODRIGUES JUNIOR, Otavio Luiz (coord.) BIONI, Bruno Ricardo (coord.). Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 347.

VENTURA, Felipe. Exclusivo: vazamento que expôs 220 milhões de brasileiros é pior do que se pensava. Tecnoblog. Disponível em: <https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/amp/>. Acesso em 1 set. 2021

SOUSA, Carlos Affonso Pereira de. Capítulo XV. Segurança e Sigilo dos Dados Pessoais: primeiras impressões à luz da Lei 13.709/2018 p. 435. In: TEMPEDINO, Gustavo, OLIVA, Milena. Lei Geral de Proteção de Dados e suas repercussões no Direito brasileiro. 2ª Edição. Thomson Reuters, Revista dos Tribunais, 2019.

VOIGT, Paul. BUSSCHE, Axel. The EU General Data Protecion Regulation (GDPR): A Practical Guide. Berlim. Springer.2017. p. 40.


OBSERVATÓRIO DA
LGPD
UNIVERSIDADE DE BRASÍLIA