II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS I

T255
Tecnologias Disruptivas, Direito e Proteção de Dados - I [Recurso eletrônico on-line] organização Congresso Internacional de Direito e Inteligência Artificial: Skema Business School – Belo Horizonte;

Coordenadores: Lorena Muniz e Castro Lage; Yuri Nathan da Costa Lannes; Marco Antônio Sousa Alves. – Belo Horizonte:Skema Business School, 2021.

Inclui bibliografia
ISBN: 978-65-5648-272-9
Modo de acesso: www.conpedi.org.br
Tema: Um olhar do Direito sobre a Tecnologia

1. Direito. 2. Inteligência Artificial. 3. Tecnologia. II. Congresso Internacional de Direito e Inteligência Artificial (1:2021 : Belo Horizonte, MG).

CDU: 34

II CONGRESSO INTERNACIONAL DE DIREITO E INTELIGÊNCIA ARTIFICIAL

TECNOLOGIAS DISRUPTIVAS, DIREITO E PROTEÇÃO DE DADOS I

Apresentação

Renovando o compromisso assumido com os pesquisadores de Direito e tecnologia do Brasil, é com grande satisfação que a SKEMA Business School e o CONPEDI – Conselho Nacional de Pesquisa e Pós-graduação em Direito apresentam à comunidade científica os 12 livros produzidos a partir dos Grupos de Trabalho do II Congresso Internacional de Direito e Inteligência Artificial (II CIDIA). As discussões ocorreram em ambiente virtual ao longo dos dias 27 e 28 de maio de 2021, dentro da programação que contou com grandes nomes nacionais e internacionais da área em cinco painéis temáticos e o SKEMA Dialogue, além de 354 inscritos no total. Continuamos a promover aquele que é, pelo segundo ano, o maior evento científico de Direito e Tecnologia do Brasil.

Trata-se de coletânea composta pelos 255 trabalhos aprovados e que atingiram nota mínima de aprovação, sendo que também foram submetidos ao processo denominado double blind peer review (dupla avaliação cega por pares) dentro da plataforma PublicaDireito, que é mantida pelo CONPEDI. Os oito Grupos de Trabalho originais, diante da grande demanda, se transformaram em doze e contaram com a participação de pesquisadores de vinte e um Estados da federação brasileira e do Distrito Federal. São cerca de 1.700 páginas de produção científica relacionadas ao que há de mais novo e relevante em termos de discussão acadêmica sobre a relação da inteligência artificial e da tecnologia com os temas acesso à justiça, Direitos Humanos, proteção de dados, relações de trabalho, Administração Pública, meio ambiente, formas de solução de conflitos, Direito Penal e responsabilidade civil.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de 36 proeminentes professoras e professores ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores. Cada livro desta coletânea foi organizado, preparado e assinado pelos professores que coordenaram cada grupo. Sem dúvida, houve uma troca intensa de saberes e a produção de conhecimento de alto nível foi, mais uma vez, o grande legado do evento.

Neste norte, a coletânea que ora torna-se pública é de inegável valor científico. Pretende-se, com esta publicação, contribuir com a ciência jurídica e fomentar o aprofundamento da relação entre a graduação e a pós-graduação, seguindo as diretrizes oficiais. Fomentou-se, ainda, a formação de novos pesquisadores na seara interdisciplinar entre o Direito e os vários

campos da tecnologia, notadamente o da ciência da informação, haja vista o expressivo número de graduandos que participaram efetivamente, com o devido protagonismo, das atividades.

A SKEMA Business School é entidade francesa sem fins lucrativos, com estrutura multicampi em cinco países de continentes diferentes (França, EUA, China, Brasil e África do Sul) e com três importantes acreditações internacionais (AMBA, EQUIS e AACSB), que demonstram sua vocação para pesquisa de excelência no universo da economia do conhecimento. A SKEMA acredita, mais do que nunca, que um mundo digital necessita de uma abordagem transdisciplinar.

Agradecemos a participação de todos neste grandioso evento e convidamos a comunidade científica a conhecer nossos projetos no campo do Direito e da tecnologia. Já está em funcionamento o projeto Nanodegrees, um conjunto de cursos práticos e avançados, de curta duração, acessíveis aos estudantes tanto de graduação, quanto de pós-graduação. Em breve, será lançada a pioneira pós-graduação lato sensu de Direito e Inteligência Artificial, com destacados professores da área. A SKEMA estrutura, ainda, um grupo de pesquisa em Direito e Inteligência Artificial e planeja o lançamento de um periódico científico sobre o tema.

Agradecemos ainda a todas as pesquisadoras e pesquisadores pela inestimável contribuição e desejamos a todos uma ótima e proveitosa leitura!

Belo Horizonte-MG, 09 de junho de 2021.

Profª. Drª. Geneviève Daniele Lucienne Dutrait Poulingue

Reitora – SKEMA Business School - Campus Belo Horizonte

Prof. Dr. Edgar Gastón Jacobs Flores Filho

Coordenador dos Projetos de Direito da SKEMA Business School

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: A OCORRÊNCIA DE INCIDENTE DE SEGURANÇA E A LACUNA NO PRAZO PARA A COMUNICAÇÃO

GENERAL LAW OF DATA PROTECTION: THE OCCURRENCE OF A SECURITY INCIDENT AND THE DEALINE GAP IN COMMUNICATION

Cássia Tatiane Guimarães da Rocha [1]

Resumo

O estudo analisa a lacuna do prazo razoável de comunicação do incidente de segurança na Lei Geral de Proteção de Dados Pessoais (LGPD). Qual é o prazo de outros países com relação a referida comunicação e poderia ser aplicado na legislação brasileira? Teve por objetivo verificar o prazo em regulamentos estrangeiros e o que poderia ser aplicado à LGPD. Sob uma abordagem dedutiva, procedimento comparativo e pesquisa bibliográfica e documental, conclui-se ser necessária a análise de alteração legislativa para um prazo exato.

Palavras-chave: Lei geral de proteção de dados, Incidente de segurança, Prazo

Abstract/Resumen/Résumé

The study analyzes the reasonable communication deadline of a security incident in the General Law of Personnal Data Protection(LGPD). What is the deadline in other countries in relation to the referred communication and could this be applied to the Brazilian legislation? The objective is to verify the foreign deadline regulations and what could be applied to the LGPD. In a deductive approach, a comparative procedure, a documentary and bibliographic research, it is concluded to be necessary a legislative alteration analysis for an accurate deadline.

Keywords/Palabras-claves/Mots-clés: General law of data protection, Security incident, Deadline

[1] Acadêmica de Direito da Universidade Estácio do Rio Grande do Sul.

1. INTRODUÇÃO

Com a vigência da Lei Geral de Proteção de Dados (LGPD), tornou-se imprescindível a adequação das empresas brasileiras a esta norma que regulamenta o tratamento de dados pessoais, traz diretrizes a serem seguidas e possibilidade de sanções. A sua não observância pode acarretar prejuízos e custo alto às organizações.

No entanto, observa-se que na lei o prazo para o controlador comunicar o incidente de segurança à autoridade nacional e ao titular dos dados aparece como "prazo razoável", o que gera uma lacuna e diferentes possibilidades de interpretação. Sendo assim, questiona-se: qual é o prazo de outros Estados que possuem leis similares? Isso poderia ser aplicado no Brasil?

Busca-se analisar como é delimitado o prazo do controlador comunicar o incidente de segurança em outros países e se o mesmo poderia ser aplicado no Brasil. Para atingir esse objetivo, utilizou-se do método de abordagem dedutivo, o método de procedimento comparativo e as técnicas de pesquisa bibliográfica e documental.

O presente trabalho dividiu-se em dois capítulos: o primeiro abordará a LGPD e o prazo razoável na comunicação da ocorrência de incidente de segurança e o segundo tratará do prazo em outros Estados.

2. LGPD E O PRAZO RAZOÁVEL NA COMUNICAÇÃO DA OCORRÊNCIA DE INCIDENTE DE SEGURANÇA

A Lei Geral de Proteção de Dados (LGPD), nº 13.709/2018 (BRASIL, 2018), entrou em vigor em 2020, iniciando um caminho já traçado em outros países, que possuem regulamento para o tratamento de dados pessoais. Ela traz adequações que as empresas, tanto do setor privado quanto público, como Órgãos e Entidades da Administração Pública, deverão adotar.

Tal norma disciplina alguns tópicos, como as categorias de dados, a abrangência, a coleta, o tratamento, os direitos dos titulares de dados, determina o que são dados sensíveis e como deverão ser abordados, dispõe sobre diretrizes para as empresas com algumas diferenciações ao setor público, sanções aos descumprimentos, além da criação de uma autoridade nacional para a fiscalização e acompanhamento (BRASIL, 2018).

O tratamento é "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento [...]" e segurança é 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" (BRASIL, 2018).

Incidente de segurança com dados pessoais é "qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais" (BRASIL, 2021). Nos termos da lei, o controlador é "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", ou seja, a própria organização, que demanda o tratamento, pode realizá-lo e/ou nomear um operador, que pela lei é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"; e eles, juntos, são intitulados agentes de tratamento (BRASIL, 2018).

O encarregado, por sua vez, aparece na alteração do texto legislativo como "pessoa indicada pelo controlador e operador para atuar como um canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)" (BRASIL, 2019).

Pinheiro (2020) alerta que a adequação à LGPD traz grande mobilização às instituições, o que pode contribuir para o aumento do chamado Custo Brasil, principalmente para as *Startups*, as pequenas empresas e no setor público para aquelas que cuidam de dados pessoais sensíveis relacionados à saúde. Por isso, a capacitação dos agentes de tratamento torna-se tão importante quanto a implementação propriamente dita.

Segundo a Associação Brasileira da Indústria de Máquinas e Equipamentos (ABIMAQ) "na prática, 'Custo Brasil' é o diferencial de custo em se produzir o mesmo produto no Brasil ou no exterior. Ele decorre do conjunto de dificuldades estruturais, burocráticas e econômicas que encarecem a produção e o investimento no Brasil" (ABIMAQ, 2018). O Custo Brasil não afeta somente o setor industrial, mas a economia brasileira como um todo, por isso a importância de uma legislação clara e objetiva, que não deixe lacunas para diferentes interpretações que acarretem erros e suas previstas sanções.

Com isso, atenta-se que o artigo 48 da LGPD deixa uma lacuna visível e precisará ser abordado com maior atenção para futura alteração. Isso porque está previsto que a comunicação do controlador "à autoridade nacional e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares" e no seu § 1º traz: "A comunicação será feita em prazo razoável conforme definido pela autoridade nacional" (BRASIL, 2018).

Surge então a dúvida que paira diante da legislação brasileira, sobre o porquê da indefinição do referido período. Entende-se que a autoridade nacional deverá abordar

posteriormente alguns pontos da legislação basilar, mas a priori a norma não prevê a obrigatoriedade de definição ao assunto.

Bobbio (2001), ao tratar das normas jurídicas, aborda a distinção entre comandos e conselhos e observa que somente o direito contém a obrigação, ou seja, só o direito possui coerção sobre o sujeito. Já a moral limita-se a dar recomendações que deixam o intérprete livre para segui-las ou não. Com isso, infere-se que a LGPD, ao abordar o prazo para o controlador informar à autoridade nacional e aos titulares sobre a ocorrência de incidente de segurança, deixa livre a interpretação, visto que a legislação traz como prazo a palavra "razoável" e não um comando exato ou limitado no qual conteria uma obrigação a ser seguida. Sendo assim, esta é uma norma que, por não ser um comando exato, carece de coercibilidade.

A referida lacuna na LGPD, sobre prazo razoável, é abordada por Pinheiro (2020, p.13-14), que explica que "[...] em alguns aspectos deixou margem para interpretação mais ampla, trazendo alguns pontos de insegurança jurídica por permitir espaço para a subjetividade onde deveria ter sido mais assertiva." A questão levantada pela autora torna-se de suma importância quando avaliada do ponto de vista das sanções, já que algumas são multas diárias e poderiam receber interferência conforme a interpretação do que seria um prazo razoável.

De acordo com Blum e Wajsbrot (2020), a reação das empresas desde o início das discussões sobre a lei de proteção de dados no Brasil, de forma geral, foi de hesitação e receio quanto às sanções expressas, algumas consideradas brandas e outras mais expressivas, como as multas de até 2% sobre o faturamento no último exercício com o limite de R$ 50.000.000,00 (cinquenta milhões de reais) por infração e publicização da infração.

As sanções tratadas nos artigos 52, 53 e 54 da LGPD passarão a vigorar dia 1º de agosto de 2021 (BRASIL, 2020). Isso torna evidente a importância da observação de todas as diretrizes da LGPD pelas organizações, já que a inobservância ou a divergência de interpretações as levariam a prejuízos desagradáveis.

Por isso, observa-se grande valia à atenção dispensada nesse prazo legislativo em pauta, importante para posterior abordagem conforme diretrizes mais elaboradas. Interessa, para o presente estudo, analisar as legislações de proteção de dados em outros Estados. Assim, encaminha-se para o próximo item da pesquisa.

3. PRAZO DE COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA EM OUTROS ESTADOS

Diante de um desafio mundial no controle dos dados, as regulamentações de proteção tornaram-se necessárias. O debate sobre o tema teve início em 1970 na União Europeia (UE),

a pioneira no assunto, que posteriormente com o objetivo de abordar a tutela das pessoas físicas no tratamento de dados pessoais e na livre circulação desses, elaborou o Regulamento Geral sobre a Proteção de Dados, *General Data Protection Regulation* (GDPR) nº 679 de 2016 (PINHEIRO, 2020).

Considerando-se que o "nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros" estabeleceu-se o prazo de dois anos para a adequação, passando-se a exigir que outros países e empresas, que prezem por suas relações comerciais com a UE, possuam uma legislação do nível do GDPR (UNIÃO EUROPEIA, 2016).

Conforme Serafino (2020, p. 234) "A entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia (GPDR), que exige parâmetros mínimos equivalentes de proteção de dados entre os países para que haja transferência de informações internacionais" foi o que motivou a estruturação da legislação brasileira.

O regulamento europeu é bastante detalhado, possuindo 11 capítulos com 99 artigos bem distribuídos e poderia ser considerado a Bíblia normativa da tutela de dados pessoais, já que de fato o mercado europeu nas suas relações e comércio internacionais movimentam boa parte do cenário nos demais países. No que diz respeito a esse detalhamento, nas instruções do GDPR torna-se oportuno observar que no artigo 33 aborda-se a "notificação de uma violação de dados pessoais à autoridade de controle" o responsável pelo tratamento deve notificar o fato no prazo explícito de 72h contadas da ciência do incidente (UNIÃO EUROPEIA, 2016).

Ademais, por efeito da responsabilidade no tratamento dos dados e do detalhamento das ações que devem ser desempenhadas, observa-se no artigo 33 da legislação europeia que "como reflexo da boa-fé, transparência e responsabilização dos atos dos agentes, a comunicação pelo controlador da ocorrência de incidentes de segurança durante o processo de tratamento de dados é essencial" (PINHEIRO, 2020, p.71).

Torna-se mister para este estudo analisar, ainda, o prazo em questão também na regulamentação da Argentina, país latino-americano próximo ao Brasil que, desde o ano 2000, possui regulamentação acerca da proteção dos dados pessoais.

Sobre a Argentina, Raminelli e Rodegheri (2016, p. 97) a apontam como o "[...] primeiro país latino-americano que editou uma lei de proteção de dados, recebeu certificação da União Europeia quanto ao nível de segurança no tratamento das informações, apresentando maior abrangência ao tratar do assunto em sua primeira lei sobre o tema [...]".

A Lei nº 25.326/00, *Ley de Protección de los Datos Personales* (PDPA), Lei de Proteção de Dados Pessoais da Argentina, trata das disposições gerais, princípios gerais

relativos à proteção de dados, dos direitos dos detentores dos dados, dos usuários e gestores de arquivos, registros e bancos de dados, do controle, sanções e ação de proteção de dados pessoais (ARGENTINA, 2000).

Recentemente, em 2020, a regulamentação foi tratada no Projeto de Lei que criou a Comissão Bicameral de Fiscalização da Lei de Proteção de Dados Pessoais colocando algumas modificações à lei original em pauta, principalmente atualizações no artigo 3º que incorporaria o artigo 7º Bis da Lei 25.326, que como proposta tem a seguinte redação: "O responsável pelo tratamento deve informar a autoridade de controle em um prazo razoável, levando em consideração as circunstâncias do caso, as violações de segurança de dados pessoais que ocorreram em qualquer fase do tratamento de dados [...]" (CELE, 2020). No entanto, até o momento, na legislação atualizada, não consta o texto da proposta apresentada.

O texto original prevê sanções administrativas e penais para os responsáveis ou utilizadores de ficheiros, como são chamados os agentes de tratamento na legislação Argentina, caso não atendam especificações como as do artigo 9º da lei, o qual descreve que deverão "[...] adotar as medidas técnicas e organizacionais necessárias para garantir a segurança e confidencialidade dos dados pessoais, de forma a evitar a sua adulteração, perda, consulta ou tratamento não autorizado [..]", mas não determinou um prazo para informar as autoridades e titulares de dados caso ocorra algum incidente de segurança (ARGENTINA, 2000).

Percebe -se, com a análise, o deficit de prazo para a comunicação do incidente de segurança na norma Argentina, levando em consideração o texto atual. Verificou-se ainda que, mesmo na proposta legislativa do ano de 2020 não consta um prazo determinado; portanto, ainda que seja aprovada restará uma lacuna podendo gerar, como visto nesse estudo, diversas interpretações, posteriores sanções e insegurança jurídica.

4. CONCLUSÃO

Perante um desafio mundial no controle dos dados pessoais, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor no Brasil em 2020. A norma disciplina pontos que devem ser observados pelas empresas, como categorias de dados, abrangência, conceitos, atores envolvidos, prazos e a previsão de sanções, pelo não cumprimento, para agosto de 2021 em diante.

O prazo para o controlador comunicar um incidente de segurança à autoridade e ao titular na LGPD aparece implícito na palavra razoável, o que deixa margem a diferentes interpretações, que influenciarão nas sanções e consequentes custos às instituições. Com a

presente pesquisa, verificou-se que o prazo em questão expresso na legislação europeia é de 72h, enquanto na lei Argentina ocorre um déficit no seu estabelecimento.

Depreende-se que o período para a referida comunicação, já empregado na norma da União Europeia, poderia ser aplicado na LGPD, revelando-se a possibilidade de uma revisão legislativa brasileira que traga maior eficiência e segurança jurídica.

Para posterior aprofundamento da presente pesquisa, sugere-se a análise de julgados que possam surgir por influência da lacuna deixada pelo prazo razoável, após agosto de 2021, com a vigência da aplicação de sanções às empresas.

REFERÊNCIAS

ABIMAQ - Associação Brasileira da Indústria de Máquinas e Equipamentos. **Custo Brasil**. São Paulo, 2018. Disponível em: http://abimaq.org.br/Arquivos/Html/DEEE/180723-%20Custo%20Brasil.pdf. Acesso em: 12 abr. 2021.

ARGENTINA. **Ley de Protección de los Datos Personales nº 25.326 de 2000**. Buenos Aires, 2000. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion. Acesso em: 21 abr. 2021.

BLUM, Renato Müller da Silva Opice; WAJSBROT, Shirly. Um novo mindset de negócios – lidar com os desafios com um olhar disruptivo. In: BLUM, Renato Opice (org.). **Proteção de dados**: Desafios e Soluções na Adequação da Lei. Editora Forense Ltda, 2020.

BOBBIO, Norberto. **Teoria da norma jurídica.** 1ed. Bauru- SP: EDIPRO, 2001.

BRASIL. **Comunicação de incidentes de segurança**, incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD. Brasília, 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 27 abr. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 abr. 2021.

BRASIL. **Lei nº 13.853, de 08 de julho de 2019.** Altera a Lei nº 13.709 para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados [...]. Brasília, DF, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 05 abr. 2021.

BRASIL. **Lei nº 14010, de 10 de junho de 2020**. Dispõe sobre o Regime Jurídico Emergencial e Transitório das relações jurídicas de Direito Privado (RJET) no período da pandemia do coronavírus (Covid-19). Brasília, DF, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/L14010.htm. Acesso em: 05 abr. 2021.

CELE - Centro de Estudios en Libertad de Expresión y Acceso a la Información. **Projeto de lei que cria a Comissão bicameral de fiscalização da lei de proteção de dados pessoais.**

Buenos Aires- AR, 2020. Disponível em: https://observatoriolegislativocele.com/pt/argentina-proyecto-de-ley-que-crea-la-comision-bicameral-de-seguimiento-de-la-ley-de-proteccion-de-datos-personales-2020. Acesso em: 22 abr. 2021.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020. [recurso eletrônico].

RAMINELLI, Francieli Puntel; RODEGHERI, Letícia Bodanese Rodegheri. A Proteção de Dados Pessoais na Internet no Brasil: Análise [...]. **Revista Cadernos do Programa de Pós-Graduação em Direito (PPGDir.)** / UFRGS, v. 11, n. 2. Porto Alegre- RS, 2016. Disponível em: https://seer.ufrgs.br/ppgdir/article/view/61960/39936. Acesso em: 24 abr. 2021.

SERAFINO, Danielle Campos Lima. Direito Tributário e Tratamento de Dados pelo Poder Público. In: BLUM, Renato Opice (org.). **Proteção de dados**: Desafios e Soluções na Adequação da Lei. Editora Forense Ltda, 2020.

UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR) nº 679 de 2016**. Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1725&from=EN. Acesso em: 09 abr. 2021.