UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I – CAMPINA GRANDE
CENTRO DE CIÊNCIAS JURÍDICAS - CCJ
DEPARTAMENTO DE DIREITO PRIVADO
CURSO DE GRADUAÇÃO EM DIREITO

ANA LUISA BANDEIRA PINHEIRO

PRIVACY BY DESIGN COMO OBRIGAÇÃO DE SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS

CAMPINA GRANDE
2021

ANA LUISA BANDEIRA PINHEIRO

PRIVACY BY DESIGN COMO OBRIGAÇÃO DE SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS

Trabalho de Conclusão de Curso (Artigo) apresentado ao Centro de Ciências Jurídicas, da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de bacharelado em Direito.

Orientador: Prof. Me. Claudio Simão de Lucena Neto.

CAMPINA GRANDE
2021

P654p Pinheiro, Ana Luisa Bandeira.

Privacy by design como obrigação de segurança no tratamento de dados pessoais [manuscrito] / Ana Luisa Bandeira Pinheiro. - 2021.

22 p.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2022.

"Orientação : Prof. Me. Claudio Simão de Lucena Neto , Departamento de Direito Privado - CCJ."

1. Obrigações de segurança. 2. Dados pessoais. 3. Lei Geral de Proteção de Dados. 4. Privacy by design. I. Título

21. ed. CDD 343.071

Elaborada por Kênia O. de Araújo - CRB - 15/649 BSCCJ/UEPB

ANA LUISA BANDEIRA PINHEIRO

PRIVACY BY DESIGN COMO OBRIGAÇÃO DE SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS

Trabalho de Conclusão de Curso (Artigo) apresentado ao Centro de Ciências Jurídicas, da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de bacharelado em Direito.

Aprovada em: 19/10/2021.

BANCA EXAMINADORA

Prof. Me. Claudio Simão de Lucena Neto (Orientador)
Universidade Estadual da Paraíba (UEPB)

Profa. Dra. Ana Alice Ramos Tejo Salgado
Universidade Estadual da Paraíba (UEPB)

Profa. Dra. Ludmila Albuquerque Duoettes Araújo
Universidade Estadual da Paraíba (UEPB)

A Maria Flor, luz da minha vida, e a mainha, pelo cuidado, dedicação e amizade, DEDICO.

“A habilidade humana não pode inventar uma cifra que a habilidade humana não possa solucionar.”

(Edgar Allan Poe)

SUMÁRIO

PRIVACY BY DESIGN COMO OBRIGAÇÃO DE SEGURANÇA NO TRATAMENTO DE DADOS PESSOAIS

Ana Luisa Bandeira Pinheiro*

A necessidade de garantir segurança no tratamento dos dados pessoais legitimou a criação de uma lei específica exigindo regras substanciais para o ambiente digital. Nesse sentido, o presente artigo pretende analisar as obrigações de segurança no tocante ao tratamento de dados pessoais à luz da Lei Geral de Proteção de Dados (LGPD), especialmente no que concerne à metodologia *privacy by design* e o uso de meios técnicos para a proteção dos dados, tais como anonimização e pseudonimização. Ainda, objetiva-se pontuar como dar-se-á a responsabilidade dos agentes de tratamento frente a situações de irregularidades no tratamento de dados. Por fim, pretende-se analisar de forma prática um caso real de vazamento de dados pessoais e como a empresa se posicionou frente ao incidente.

Palavras-chave: Obrigações de segurança. Dados pessoais. Lei Geral de Proteção de Dados. Privacy by design.

The need to ensure data treatment safety has legitimized the creation of a specific law demanding substantial ruling for digital environment. For that matter, the presented article intends to analyze the security obligations towards the treatment of personal data according to the General Law of Data Protection (GLDP), specially concerning the privacy by design methodology and the use of technical assets to data protection, such as anonymization and pseudonymization. Still, it is aimed to disclosure how the responsibility of treatment agents is given when faced with situations of irregularity on data treatment. Finally, It purposes to analyze on a practical way a real case of personal data leaking and how the related company took a stand when facing the incident.

Keywords: Security obligations. Personal data. General law of Data Protection. Privacy by design.

* Ana Luisa Bandeira Pinheiro – Graduanda em Direito pela Universidade Estadual da Paraíba - analuisabandeira@gmail.com.

1 INTRODUÇÃO

É notório que as Tecnologias da Informação se difundiram de modo exponencial, moldando-se ao contexto social de tal forma que se tornaram essenciais para a realização desde as tarefas mais corriqueiras até as mais sofisticadas.

O alto fluxo de dados e informações circulando são pontos característicos da nova realidade social, também marcada pelas interações realizadas constantemente, impulsionando, assim, o desenvolvimento das Tecnologias da Informação e da Comunicação e solidificando novas técnicas de manejo de dados. Esse fenômeno é conhecido como “big data”, ou seja, dados variados, em grande volume e circulando em grande velocidade.

Agora, há uma nova forma de captar, analisar, armazenar e, extrair valor de uma grande quantidade de informações, possibilitando, dentre outros, a tomada de decisões automatizadas, o aumento na eficiência empresarial e governamental, criando novos modelos de negócios e gerando substancial riqueza, além da resultante economia de recursos (GOMES, 2017).

Assim, constata-se que a coleta de dados cresce em níveis exorbitantes pelos mais variados agentes de tratamento, que gozam de fontes e formas de armazenamento distintas. Considerando o alto fluxo de dados circulando e sendo utilizados para manipular informações como, por exemplo, preferências de consumo das pessoas e perfis psicológicos, fez-se necessária a criação de normas que freassem o uso indiscriminado dessas informações, de modo a garantir o direito à privacidade do titular dos dados.

Em meio a esse cenário, a Lei Geral de Proteção de Dados (LGPD) surge com a pretensão de assegurar a proteção do recurso mais visado da atualidade: os dados pessoais. A norma visa conferir maior autonomia ao titular no controle de seus dados, aspirando adaptações das empresas quanto ao tratamento destes.

Ante o exposto, questiona-se: como os agentes de tratamento de dados pessoais devem agir afim de garantir a segurança da informação? Nesse sentido, o objetivo geral do presente artigo consiste em analisar as obrigações de segurança no tratamento de dados prevista na Lei Geral de Proteção de Dados, afim de garantir a tutela do direito à privacidade. Já como objetivos específicos, pretende-se analisar a influência da metodologia *privacy by design* e sua importância no tratamento de dados pessoais, trazer as obrigações dos agentes de tratamento de dados frente a incidentes de vazamento, bem como observar na prática como a empresa Prudential do Brasil respondeu ao vazamento de dados ocorrido em novembro de 2021.

Buscando responder as questões levantadas anteriormente, foi realizada uma pesquisa bibliográfica e documental, através da qual buscou-se informações em livros, portais de notícias online, revistas, artigos científicos e sites de conteúdo jurídico.

A escolha do tema justifica-se pelo interesse pessoal da autora em estudar direito e tecnologia, ocupando-se em conhecer as mais variadas normas que versam sobre privacidade de dados. A relevância social e científica do estudo reside na constante busca pela tutela do direito à privacidade, considerando que os dados são extensões da personalidade do titular e toda violação a esse bem jurídico traz prejuízos diretos ao seu portador. Quanto ao público para o qual a produção é destinada, o presente estudo se estende a sociedade como um todo.

Quanto aos fins, adotou-se a metodologia descritiva e, quanto aos meios, utilizou-se da pesquisa bibliográfica e documental, conforme exposto anteriormente. A linha de pesquisa iniciou-se no início do mês de setembro de 2021, com a escolha e delimitação do tema, ocasião em que começou a ser desenvolvida a pesquisa bibliográfica e documental, e finalizou-se por completo ao início do mês de outubro, concluindo-se as etapas finais propostas no Projeto de Pesquisa.

O que se espera com a presente produção é que se fomente uma rica discussão frente à temática posta, de forma que analisemos criticamente como estamos dispondo dos nossos dados pessoais e com qual finalidade estes estão sendo manipulados.

2 DIREITO A PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO

No início deste século, a expressão “sociedade da informação” passou a ser utilizada como substituto para o conceito complexo de “sociedade pós-industrial”, remetendo à essência da acelerada transformação tecnológica nas relações da sociedade.

Segundo Manuel Castells, a sociedade contemporânea se depara com uma revolução tecnológica, cuja essência está pautada nos sistemas de informação, de processamento e de comunicação (CASTELLS, 1999). Para ele, a informação é a matéria-prima da transformação tecnológica, visto que as tecnologias se desenvolvem para permitir ao homem atuar sobre a informação propriamente dita (CASTELLS, 1999).

Nesse sentido, percebe-se que com o passar dos anos as informações pessoais passaram a se tornar fonte de vantagens para quem as detém, sejam tais vantagens pessoais ou econômicas. O armazenamento e uso adequado dessas informações conferem maior poder de uns sobre os outros (COSTA; GOMES,2017, p. 220).

Nesse contexto, é notório que o crescimento do fluxo de informações aumentou o dinamismo da sociedade e, rapidamente, a captação de informações e de dados pessoais tornou-se uma estratégia interessante para os entes privados com o objetivo de conhecer de forma mais aprofundada seus indivíduos e consumidores, bem como os seus funcionários.

Pode-se dizer que o interesse das empresas em adquirir informações está diretamente relacionado ao princípio da eficiência e do controle social, utilizando-se de pesquisas e censos para obtenção de maior conhecimento sobre a população resultando no aumento do poder de controle sobre os indivíduos. Já a importância da coleta de dados para os entes privados se evidencia a partir do desenvolvimento de tecnologias que diminuem o custo da coleta e tratamento de dados, transformando tais informações em utilidade para as empresas das mais diversas áreas de atuação, em especial às com fins comerciais e, na atualidade, com importante enfoque nas relações de trabalho (DONEDA, 2006, p. 8).

Mediante o grande fluxo de informações pessoais que circulam na rede, fez-se necessário outorgar legislações específicas para frear o uso inadequado desses dados. É o que será exposto nos próximos tópicos.

2.1 Privacidade: direito fundamental

A Declaração Universal dos Direitos Humanos de 1948, assegura em seu artigo 12 o direito a todos de terem sua vida privada resguardada sem interferências ou ataques. Senão vejamos:

> “Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques. ” (UNIC, 2009).

No Brasil, o Pacto Internacional dos Direitos Civis e Políticos, ratificado mediante o Decreto 592 de 06 de julho de 1992, em seu artigo 172, garante o direito à privacidade.

Ainda, temos o direito à privacidade como espécie do gênero dos direitos da personalidade, regulados pelo Código Civil Brasileiro, especificamente em seu artigo 213 que trata da vida privada, e resguardados pela Constituição da República Federativa do Brasil de 1988 em seu artigo 5°, inciso X, que prevê o direito à vida privada como sendo fundamental.

Imperioso trazer à esta discussão que no dia 31 de agosto de 2021, a câmara dos deputados aprovou a Proposta de Emenda à Constituição (PEC) 17/19, que objetiva acrescentar o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, ambos da Constituição Federal. A PEC assegura o direito à proteção de dados pessoais, inclusive nos meios digitais e inclui, entre as competências da União, legislar sobre proteção e tratamento de dados pessoais.

Nesse sentido, resguardar a privacidade é um dever pacificado nos regramentos sociais ao longo das décadas, sendo indefensável ainda haver Estados que não possuem legislações específicas que versem sobre privacidade na internet, considerando o contexto em que vivemos.

O desenvolvimento tecnológico facilitou o acesso às informações pessoais, inclusive a dados sensíveis, tanto pelo poder público quanto por entes privados, justificando a necessidade da implantação de novas formas de proteção das informações privadas. No Brasil, a falta de legislação específica para proteção de dados foi suprida pela promulgação da Lei Geral de Proteção de Dados Pessoais – Lei n° 13.709 - em 14 de agosto de 2018.

A LGPD, ao regulamentar a proteção de dados pessoais, garante o exercício dos direitos da personalidade, estabelecendo limites ao direito de acesso às informações e o uso destas para fins distintos da finalidade de uso a que se propôs. Nesse sentido, o inciso I do artigo 6º da referida norma, traz que finalidade é a “realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades” (BRASIL, 2018).

2.2 Segurança da informação como garantia da proteção de dados

Segurança da informação é a proteção de dados de propriedade das organizações contra ameaças diversas. Trata-se de um esforço pautado por ações que objetivam mitigar riscos e garantir a continuidade das operações.

De acordo com a ISO/ IEC 27002/13, segurança da informação é “a proteção da informação contra os mais diversos tipos de ameaças para garantir a continuidade dos negócios, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócios” (ABNT, 2013).

Nesta seara, cabe aos agentes de tratamento garantir que os dados pessoais coletados sejam manipulados e armazenados de forma segura, certificando-se do uso 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), conforme previsão do inciso VII, do artigo 6º da LGPD.

A segurança da informação está pautada em três princípios, quais sejam: confidencialidade, integridade e disponibilidade. O princípio da confidencialidade preconiza que o conteúdo protegido deve estar disponível somente a pessoas autorizadas, ou seja, deve-se limitar quem pode e como pode acessar determinada informação.

Em sequência, o princípio da integridade aduz que a informação protegida deve ser íntegra, ou seja, não pode sofrer qualquer alteração indevida, não importa por quem e nem em qual etapa, se no processamento ou no envio.

Por fim, o princípio da disponibilidade institui que é preciso garantir que os dados estejam acessíveis para uso estrito de pessoas previamente determinadas, ou seja, de modo permanente a elas.

A segurança da informação é parte da privacidade de dados, no entanto, é válido pontuar que esta não se resume àquela. Em se tratando de segurança de dados, resta límpido que as ações são capazes de ampliar a proteção ao conteúdo, no entanto, não é possível garantir a segurança absoluta dos dados, levando em conta que ao passo que as tecnologias de criptografia são melhoradas, as formas de decodificá-las também evoluem.

Isso significa dizer que, mesmo se a informação estiver armazenada para uso restrito, sempre haverá um risco. Dessa forma, cabe aos profissionais da área trabalharem para que este seja o menor possível, empregando técnicas, táticas e ferramentas constantemente atualizadas – o que funciona como uma resposta proporcional aos avanços existentes também nas ações promovidas pelos *cibercriminosos*.

A Autoridade Nacional de Proteção de Dados (ANPD) lançou em outubro de 2021 o primeiro “Guia Orientativo Sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte”, sendo um grande marco desde que a LGPD entrou em vigor. O guia faz uso de uma linguagem simples e clara afim de instruir os agentes quanto às suas obrigações no tratamento de dados pessoais, bem como apresenta boas práticas para evitar incidentes de vazamento de dados.

3 DO TRATAMENTO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados, nos termos do inciso X, do artigo 5º, define tratamento, como:

> “toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (BRASIL, 2018).

Com a rápida evolução das tecnologias da informação, especialmente o crescimento massivo da Internet, ilimitado no tempo e no espaço, foi observado um crescimento do volume e da variedade de dados que podem ser captados, analisados, armazenados e manipulados a fim de extrair valor do maior número possível de informações, possibilitando, dentre outros, a tomada de decisões

automatizadas, o aumento na eficiência empresarial e governamental, criando novos modelos de negócios e gerando substancial riqueza, além da resultante economia de recursos.

É válido ressaltar que esses dados também podem ser combinados, aumentando o risco de re-identificação mesmo após a anonimização ou desidentificação de bases isoladas (MOONEY SJ, PEJAVER V, 2018).

O reconhecimento da pouca efetividade de procedimentos de anonimização, desidentificação e do consentimento informado na proteção da privacidade têm aumentado a necessidade da implantação de mecanismos que permitam um maior controle sobre uso dos dados (MCGRAIL KM, GUTTERIDGE K, MEAGHER NL, 2015).

Desta forma, torna-se necessária a utilização de mecanismos que possibilitem ao indivíduo obter conhecimento e controle sobre seus próprios dados que, no fundo, são expressão direta de sua própria personalidade (DONEDA, 2006).

Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a dignidade da pessoa humana e como direito fundamental.

3.1 Dados pessoais: produto de riqueza da sociedade atual

Em consonância com o regramento de proteção de dados em vigência na Europa (GDPR), a Lei Geral de Proteção de Dados conceitua dados pessoais como sendo toda informação relacionada a pessoa natural identificada ou identificável, abrangendo dados referentes à vida privada, pública e profissional (BRASIL, 2018).

Temos por “identificável” as situações em que não é possível conhecer explicitamente o titular dos dados, embora seja viável chegar a sua identidade a partir do cruzamento das informações contidas em outros bancos de dados.

A LGPD instrui que os dados pessoais passem por um tratamento especial para garantir a privacidade do titular. Um desses mecanismos é a anonimização, processo através do qual se utiliza de meios técnicos razoáveis e disponíveis na ocasião de tratamento dos dados para garantir que o dado relativo ao titular não mais possa ser usado para identificá-lo, seja de forma direta ou indireta.

Nesse sentido, é relevante pontuar que dados anonimizados não são considerados dados pessoais para os fins da referida norma. É o que prevê o artigo 12, senão vejamos:

> 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. (BRASIL,2018)

Assim, dados pessoais são qualquer informação de cunho pessoal que identifique de forma direta ou indireta alguma pessoa. Os dados pessoais sensíveis, por definição, são aqueles que dizem respeito à origem étnica ou racial, opiniões políticas, crenças filosóficas ou religiosas, associação a sindicatos, dados biométricos e genéticos e informações sobre saúde e sexualidade.

Para Drucker, a informação é um dos maiores produtores de riqueza da sociedade atual, e considerando a alta demanda para comercialização de dados, faz-se necessário investir em meios a fim de evitar incidentes de vazamento, um deles é a anonimização de dados (DRUCKER, 1993).

3.2 Dados anonimizadados e pseudonimizados

Os dados anonimizados são dados pessoais convertidos em dados não identificáveis, exigindo-se para tanto que o processo de anonimização não seja reversível. Dessa forma, o esperado é que uma vez que ocorra a dissociação dos dados, estes não possam ser reagrupados entre si para identificar a quem pertencem.

Esse processo pode se valer de diferentes técnicas que buscam eliminar tais elementos identificadores de uma base de dados, variando entre: supressão; generalização; randomização e pseudoanonimização.

Considerando a vasta gama de dados que circulam na rede, não é viável que haja um único método ou uma combinação perfeita para parametrizar o processo de anonimização, devendo-se analisar contextualmente como este deve ser empreendido para que os titulares dos dados anonimizados não sejam reidentificados, nem mesmo por quem procedeu à sua anonimização.

No entanto, é conhecido que o processo de anonimização é algo falível. A representação simbólica de que os vínculos de identificação de uma base de dados poderiam ser completamente eliminados, garantindo-se, com 100% (cem por cento) de eficiência, o anonimato das pessoas, é um mito (NARAYANAN; SHMATIKOV, 2010).

O regulamento de proteção de dados vigente na Europa e a norma brasileira de proteção de dados, valeram-se do critério da razoabilidade para delimitar o espectro do conceito expansionista de dados pessoais. Agora, não basta a mera possibilidade de que um dado seja atrelado a uma pessoa para atrair o termo identificável, essa vinculação deve ser objeto de um “esforço razoável”, sendo esse o limiar do conceito de dado pessoal como aquele relacionado a uma pessoa identificável.

De outra forma, se para correlacionar um dado a uma pessoa é necessário um esforço fora do razoável, não há que se falar em dados pessoais. Nessa situação, o dado é considerado como anônimo, uma vez que o “filtro da razoabilidade” descarta o seu enquadramento como aquele relacionado a uma pessoa identificável.

Considerando que o processo de anonimização é falível em virtude dos cada vez mais potentes algoritmos de *machine learnin*g e mineração de dados, criou-se a ideia de pseudonimização.

O Grupo de Trabalho de Proteção de Dados do Artigo 29, da União Europeia, conceitua o processo de pseudonimização como o ato de substituir um atributo (tipicamente um atributo único) em um registro por outro, em uma ação de mascaramento ou disfarce de identidade.

Essa distinção está colocada na própria LGPD. No artigo 13, § 4º, é possível verificar a definição anteriormente traçada a respeito da pseudonimização, além do fato de que as informações adicionais devem ser mantidas separadas pelo controlador em ambiente controlado e seguro. Assim, impõe-se uma camada a mais de dificuldade e, consequentemente, segurança, na junção das duas bases de dados (BRASIL, 2018).

4 PRIVACY BY DESIGN: PREVENÇÃO A INCIDENTES DE SEGURANÇA

O parágrafo segundo do artigo 46 da Lei Geral de Proteção de Dados traz a instrução de que as medidas de segurança deverão ser observadas desde a fase de

concepção do produto ou do serviço até a sua execução. Esta metodologia é conhecida como *privacy by design* ou privacidade desde a concepção e, como decorrência da primeira, temos a *privacy by default* (privacidade por padrão). Tais conceitos foram instituídos na década de 1990, pela Comissária de Informação e Privacidade de Ontário - Canadá, a Dra. Ann Cavoukian, e atualmente podem ser observados tanto no regimento europeu de proteção de dados, quanto na legislação brasileira, como inicialmente exposto.

A privacidade desde a concepção, como o próprio nome sugere, deve ser observada desde o projeto inicial do serviço a ser prestado ou do aplicativo a ser desenvolvido. Nessa ótica, a autora Cavoukian subdivide a metodologia *privacy by design* em sete princípios básicos.

O primeiro dos princípios diz respeito à proatividade, no sentido de que é necessário que as empresas priorizem uma postura proativa e não reativa (CAVOUKIAN, 2011). Na legislação pátria, este princípio coaduna-se com o princípio da boa-fé objetiva.

Dessa forma, objetiva-se a antecipação aos eventos invasivos à privacidade, afim de compreender o que poderia afetar a privacidade dos usuários durante a utilização da aplicação ou plataforma.

Em síntese, a autora menciona que o *privacy by design* vem antes do fato, por meio da adoção de uma política de privacidade forte, objetivando:

> A clear commitment, at the highest levels, to set and enforce high standards of privacy − generally higher than the standards set out by global laws and regulation. A privacy commitment that is demonstrably shared throughout by user communities and stakeholders, in a culture of continuous improvement. Established methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive, systematic, and innovative ways (CAVOUKIAN, 2011).

Outro conceito relevante é a privacidade por padrão (*privacy by default)*. Nesse contexto, a configuração referente à privacidade deve, em linhas gerais, garantir o máximo de proteção à privacidade do usuário. Por isso, não se exige do titular qualquer posicionamento no sentido de alterar a configuração para maximizar sua privacidade. As especificações prestadas devem ser claras, limitadas e relevantes para os fins necessários (CAVOUKIAN, 2011). A metodologia *privacy by default* pode ser observada no princípio da finalidade trazido no inciso I, do artigo 6º, da LGPD.

Assim, deve-se respeitar a privacidade sem prejudicar as funcionalidades e objetivos da plataforma, o que exige maior criatividade e dedicação dos desenvolvedores do aplicativo (CAVOUKIAN, 2011). Este é um compromisso que deve percorrer desde a parte inicial até os níveis mais altos de produção, objetivando atingir os mais altos padrões de privacidade, geralmente, ainda em um patamar maior do que aqueles estabelecidos pelas leis e regulamentos globais.

Ainda, há o compromisso de privacidade comprovadamente compartilhado pelas comunidades de usuários e partes interessadas, em uma cultura de melhoria contínua. Por fim, um compromisso com a elaboração de métodos para reconhecer projetos inadequados, antecipar práticas e resultados de privacidade inadequados e corrigir quaisquer impactos negativos, muito antes de ocorrerem de maneira proativa, sistemática e inovadora.

Outrossim, o princípio da segurança de ponta-a-ponta (*lifecycle protection*) se refere à proteção dos dados desde a sua coleta até a sua eliminação. Portanto,

preza-se por uma proteção em sentido amplo, durante todo o ciclo da vida dos dados:

> Applied security standards must assure the confidentiality, integrity and availability of personal data throughout its lifecycle including, inter alia, methods of secure destruction, appropriate encryption, and strong access control and logging methods (CAVOUKIAN, 2011).

A partir do exposto, temos que a segurança da informação é pautada em três princípios, quais sejam: confidencialidade, integridade e disponibilidade, também conhecidos como triângulo CIA (em inglês - *confidentiality*, *integrity*, *and availability*). Todos os princípios devem ser respeitados e devidamente aplicados para garantir uma boa política de segurança da informação.

Nesse sentido, os princípios da privacidade desde a concepção podem servir como parâmetro para as empresas na execução de um programa de governança em privacidade e, consequentemente, para colocar em prática a segurança que a legislação brasileira constantemente menciona.

Dessa forma, os padrões de segurança aplicados devem garantir a confidencialidade, a integridade e a disponibilidade dos dados pessoais durante todo o seu ciclo de vida, incluindo, entre outros métodos, uma destruição segura, criptografia apropriada e métodos fortes de controle de acesso e registro em todas as etapas que compreendem o desenvolvimento do produto ou serviço.

A LGPD, portanto, procura nivelar o tratamento de dados pessoais, agregando proteções às já existentes no ordenamento jurídico brasileiro. As medidas de segurança, além de servir a uma maior proteção dos titulares, partem da premissa de que os benefícios do tratamento de dados pessoais devem vir acompanhados de obrigações para as empresas, para os Estados e para as próprias pessoas, garantindo a efetiva proteção à privacidade dos titulares.

Nesse sentido,

5 COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

A Lei Geral de Proteção de Dados determina em seu artigo 48 que os incidentes de segurança devem ser comunicados à Autoridade Nacional de Proteção de Dados e aos titulares e, no §1º do mesmo artigo, determina os requisitos mínimos que devem estar presentes na referida comunicação.

O dispositivo legal também faz referência à possibilidade de o incidente causar “risco ou dano relevante” ao titular dos dados, embora não haja uma definição do que se entende por “risco ou dano relevante”.

Assim, é importante destacar que o risco ou dano devem ser presumidos como risco da operação, neste caso, deve-se considerar o disposto no Código de Defesa do Consumidor sobre a responsabilidade civil objetiva do prestador de serviço.

Além disso, a avaliação de risco e dano deve observar a amplitude de direitos fundamentais relativos à proteção de dados pessoais, avaliando a possibilidade de danos imateriais, tais como: danos morais e/ou psicológicos e emocionais, tais como: discriminação, difamação, prejuízos à reputação; materiais, como perda ou dano à propriedade; ou à integridade física, como danos à saúde, agressão física ao risco de morte.

Quaisquer camadas de danos aos direitos dos titulares são igualmente relevantes para o pronto envolvimento da ANPD na questão.

Quanto às comunicações sobre os incidentes de segurança, além das informações dispostas no art. 48, § 1º, o controlador deve informar a natureza do vazamento, ou seja, se são violações de confidencialidade - quando a divulgação de dados sigilosos não for autorizada ou foi violada acidentalmente; violações de integridade - quando há alteração não autorizada ou acidental de dados pessoais - ou se são violações de disponibilidade - quando há uma perda acidental ou maliciosa de acesso ou destruição de dados pessoais.

Da mesma forma, deve ser informada a razão do vazamento, se foi, por exemplo, originado por culpa ou por dolo, por má-fé de funcionário interno ou acesso por terceiro não autorizado. Essas informações ajudarão a Agência Nacional de Proteção de Dados a determinar a melhor conduta na solução do incidente.

Da parte dos titulares dos dados, é necessária uma comunicação direta e individual, sempre que possível, como regra geral. A comunicação em veículos de mídia deve ser tratada como exceção ou complemento à comunicação individualizada, para os casos em que não é possível contatar os titulares de dados ou quando eles forem em grande número.

Importante frisar a importância de considerar que os titulares possivelmente não são especialistas no tema, e que podem não compreender mensagens técnicas, razão pela qual a comunicação deve ser feita em linguagem clara e acessível, evitando termos técnicos sempre que possível.

Também, deve-se prezar pela transparência, informando todos os termos da ocorrência, como ela se deu e o que foi ou vai ser feito para mitigar o problema, além das possíveis consequências que os titulares dos dados poderão enfrentar. Por fim, entende-se que deve haver uma forma de contato entre o titular e o controlador dos dados, para o caso de restarem dúvidas a serem sanadas.

Em linhas gerais, os incidentes de segurança devem ser comunicados, tanto à ANPD quanto aos titulares, com o máximo de transparência possível. Além disso, a Autoridade deve sempre prezar pela proteção dos direitos dos titulares de dados em sua atuação, de forma a resguardar a parte mais vulnerável e, assim, estabelecer, tanto quanto possível, uma relação equilibrada entre as partes.

6 CASO PRUDENTIAL DO BRASIL

Em novembro de 2020, a seguradora Prudential do Brasil publicou um comunicado a respeito de um incidente de segurança que havia sofrido. Segundo relato da empresa, uma pessoa não autorizada conseguiu copiar informações relativas a propostas da contratação de seguro de vida, resultando no vazamento de dados pessoais de alguns clientes.

No comunicado (anexo), a empresa informou que com o vazamento podem ter sido obtidos dados pessoais tais como: nome, CPF, endereço, informações de saúde, bens, beneficiários e, em casos limitados, os números de conta corrente e agência. No entanto, segundo a seguradora, nenhum dado de cartão de crédito foi acessado.

A postura da empresa em comunicar publicamente o vazamento de dados sofrido está alinhada à obrigação prevista no artigo 48 da Lei Geral de Proteção de Dados, qual seja informar ao titular dos dados sobre incidente de segurança que possa acarretar risco ou dano relevante aos titulares (BRASIL, 2018).

No entanto, na nota, a Prudential do Brasil não informou quantas pessoas foram impactadas pelo vazamento, nem quais medidas de segurança foram adotadas, posição contrária àquela prevista no inciso VI, parágrafo primeiro, do

artigo 48 da LGPD, qual seja informar as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (BRASIL,2018). Além disso, um fato intrigante é que a empresa não entrou em detalhes a respeito da forma como se deu o ataque, se por ação de hacker, ransomware ou até mesmo por falha humana.

Ainda, a seguradora disse acreditar que o canal "Life Planner" foi o único atingido e depreende-se do comunicado que a segurança foi reestabelecida em seu sistema de propostas, tendo em vista que a empresa garantiu que foi realizada uma investigação em conjunto com a equipe global de segurança de informação da empresa e em estreita colaboração com as autoridades competentes.

A medida tomada para amenizar o dano causado, foi oferecer às pessoas expostas pelo vazamento uma assinatura de 24 meses na plataforma Serasa Premium, serviço que monitora movimentações no número do Cadastro de Pessoa Física (CPF). O oferecimento de serviços de monitoramento de identidade tem se tornado habitual em outros países que já adotaram leis de proteção de dados pessoais.

A partir do caso exposto, reitera-se a importância da adoção, por parte dos entes que realizam tratamento de dados pessoais, de medidas técnicas robustas para garantir a segurança da informação. O mais indicado, é seguir a previsão do artigo 42 da LGPD, e tratar a segurança como um padrão desde a concepção dos projetos, afim de prever o maior número de chances de vazamento de segurança, e preparar-se para evita-las ou lidar com elas.

Em casos de incidentes de segurança, cumpre aos agentes de tratamento adotar medidas condizentes com o previsto na LGPD afim de comedir a exposição de dados pessoais e reverter os danos causados.

7 CONSIDERAÇÕES FINAIS

A instantaneidade trazida pelas novas tecnologias gerou na sociedade o anseio de estar, cada vez mais, conectada às mais diversas pessoas, nas mais diversas plataformas. Esse anseio tem reflexo na quantidade massiva de dados pessoais que têm circulado, sem contar na variedade e na velocidade com que estes se propagam.

Considerando que os dados pessoais se tornaram o recurso mais valioso dos dias atuais, o fenômeno do *big data* encontrou o cenário adequado para se difundir, aumentando, por sua vez, os riscos de incidentes de vazamento de dados pessoais e da utilização inadequada destes.

A Lei Geral de Proteção de Dados, portanto, tem como escopo a salvaguarda dos dados pessoais, impondo parâmetros para as relações comerciais virtuais. Nesse sentido, a norma estabelece novos protagonistas no tratamento desses dados, os quais deverão constar no quadro de funcionários da empresa, além de nortear a atividade empresarial através de princípios destinados à proteção de dados pessoais, e definindo a responsabilidade especifica em cada caso.

Com a vigência da lei, os contratos digitais, aplicativos e sites devem ser desenvolvidos com maior cautela, desde sua prototipagem, isto é, a privacidade deve ser observada desde a concepção – *privacy by design*. O ideal é que o agente de tratamento mantenha uma postura preventiva e não reativa, visando a mitigação dos riscos ao titular dos dados.

Nesse cenário, o controlador, o operador e o encarregado, irão atuar para que o tratamento de dados seja realizado de forma segura e transparente, a fim de que o

titular de dados, vulnerável nessa relação, possua seus direitos fundamentais resguardados.

Assim, a Lei Geral de Proteção de Dados prevê como obrigação das empresas que realizam tratamento de dados pessoais a adoção de medidas mitigadoras neste processo. No entanto, o rol de medidas de segurança não se limita à restrição de acesso de pessoas não autorizadas. Há outras providências que podem ser adotadas pelos agentes de tratamento de dados que são capazes de cumprir com os requisitos legais. Uma dessas providências é a anonimização dos dados.

É imperioso mencionar que a LGPD optou pelo conceito mais amplo de dado pessoal, ou seja, aquele que alcança tanto as informações que identificam ou que podem identificar uma pessoa natural.

Considerando que são falíveis as tecnologias que executam os processos de anonimização, a LGPD indica como as empresas devem se comportar frente a eventuais vazamentos de dados de modo que, tanto a ANPD, quanto o titular dos dados sejam cientificados do ocorrido, além de que todo eventual dano seja reparado. Foi o que observamos no caso de vazamento dos dados dos clientes da seguradora Prudential do Brasil, onde, frente ao incidente de segurança, a empresa emitiu uma nota pública divulgando o ocorrido, indicando, por sua vez, a natureza dos dados vazados, garantindo que medidas técnicas foram tomadas para reverter a situação e oferecendo aos clientes a assinatura no serviço de monitoramento de identidade do Seresa como forma de reparação ao dano causado. A postura da seguradora foi no sentido de cumprir o previsto no artigo 48 da Lei Geral de Proteção de Dados.

Portanto, conclui-se que a segurança da informação deve ser observada desde o projeto do aplicativo ou plataforma a serem desenvolvidos, objetivando adiantar e mitigar toda possível situação de vazamento de dados. No entanto, em acontecendo incidentes de dados, espera-se dos agentes de tratamento a adoção de medidas condizentes com o previsto na LGPD afim de comedir a exposição de dados pessoais e reverter os danos causados.

REFERÊNCIAS

AGÊNCIA CÂMARA DE NOTÍCIAS, **Câmara aprova em 2º turno PEC que inclui a proteção de dados pessoais na Constituição**. Disponível em: https://www.camara.leg.br/noticias/801696-camara-aprova-em-2o-turno-pec-que-inclui-a-protecao-de-dados-pessoais-na-constituicao/. Acesso em 08 de outubro de 2021.

BRASIL. PRESIDÊNCIA DA REPÚBLICA. Lei n. 13.709, de 14 de agosto de 2018. **Diário Oficial da União**. Brasília, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 14 de setembro de 2021.

CASTELLS**,** Manuel. **A era da informação: economia, sociedade e cultura**. In: A Sociedade em rede. São Paulo: Paz e Terra, 2000. v. 1.

CAVOUKIAN, Ann. **Information & Privacy: 7 foundational principles. Internet Architecture Board**. 2011. Disponível em: https://www.iab.org/wpcontent/IABuploads/2011/03/fred_carter.pdf. Acesso em: 19 de setembro de 2021.

COMISSÃO EUROPEIA. Opinion 05/2014 on Anonymization Techniques. Article 29 Data Protection Working Party – 0829/EN – WP216. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em 19 de setembro de 2021.

COSTA, Andréa Dourado; GOMES, Ana Virginia Moreira. **Discriminação nas relações de trabalho em virtude da coleta de dados sensíveis**. Londrina, 2017. Disponível em: https://www.uel.br/revistas/uel/index.php/iuris/article/view/28096 Acesso em: 19 de setembro de 2021.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Rio de Janeiro: UNIC, 2009 [1948]. Disponível em: http://www.dudh.org.br/wpcontent/uploads/2014/12/dudh.pdf Acesso em: 19 de setembro de 2021.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico, Joaçaba, p. 91-108, Dez 2011.

Gregory S. Nelson, **"Practical Implications of Sharing Data: A Primer on Data Privacy, Anonymization, and De-Identification,"** ThotWave Technologies, 2015. Article 29 Data Protection Working Party, "Opinion 05/2014 on Anonymisation Techniques," 2014.

MCGRAIL, km; GUTTERIDGE, k; MEAGHER, nl. **Building on principles: the case for comprehensive, proportionate governance of data access**. Medical data privacy handbook, p. 737-64, 2015.

MOONEY SJ, Pejaver v. **Big data in public health: terminology, machine learning, and privacy**. Annu Rev Public Health 2018; 39:95-112.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. **Myths and fallacies of “personally identifiable information”**. Communications of the ACM, Nova York, v. 53, n. 6, p. 24-26, 2010. Disponível em: http://bit.ly/30G9CVq. Acesso em: 20 de setembro de 2021.

REDAÇÃO G1. **Após 'incidente de segurança', seguradora avisa clientes sobre vazamentos de dados.** Disponível em: https://g1.globo.com/economia/tecnologia/blog/altieres-rohr/post/2020/11/12/apos-incidente-de-seguranca-seguradora-avisa-clientes-sobre-vazamentos-de-dados.ghtml. Acesso em: 04 de outubro de 2021.

Simson, L. Garfinkel, "**NIST.IR.8053 - De-Identification of Personal Information**," 2015.

ANEXO A – COMUNICAÇÃO PRUDENTIAL DO BRASIL

Prudential

COMUNICADO IMPORTANTE

Prezando pela ética, responsabilidade e transparência que permeiam todas as suas relações, a Prudential do Brasil comunica que identificou um incidente de cibersegurança em seu sistema de propostas para contratação de seguro de vida individual. Pelo conteúdo da investigação em andamento, não há indicação de que outros sistemas da companhia tenham sido acessados.

Após confirmar a situação, a companhia reestabeleceu a segurança de seu sistema de propostas.

As informações que foram copiadas são referentes a uma parcela limitada da base de dados das propostas de seguro de vida individual. Essas propostas podem conter dados pessoais como nome, CPF, endereço, informações de saúde, bens, beneficiários e, em casos limitados, os números de conta corrente e agência. Informações relacionadas a cartões de crédito não foram comprometidas.

A Prudential do Brasil repudia veementemente essa ação e trabalha com especialistas para melhorar continuamente as medidas de segurança e garantir a preservação dos dados de seus atuais e futuros clientes. Estamos realizando uma investigação em conjunto com a equipe global de segurança de informação da Prudential, em estreita colaboração com as autoridades competentes. Para nós, a proteção das informações de nossos clientes, funcionários e da própria empresa é primordial.

Estamos contatando as pessoas impactadas desde 28/10/2020 para informá-las da situação. Seguindo as boas práticas globais, disponibilizaremos para todos os envolvidos 24 meses de acesso gratuito ao sistema de monitoramento Serasa Premium, que acompanha o uso indevido de informações.

Pedimos sinceras desculpas pelo ocorrido e nos colocamos à disposição para responder eventuais perguntas por meio dos nossos canais exclusivos de atendimento.

Informamos que não houve um novo incidente de cibersegurança na Prudential do Brasil.