RISCOS E PROTEÇÃO DE DADOS PESSOAIS

Risks and protection of personal data

Cinthia Obladen de Almendra Freitas[1]

RESUMO:

O artigo aborda riscos de conformidade sob a perspectiva da proteção de dados pessoais, privacidade e segurança da informação. Inicia-se definindo risco e seus elementos constitutivos para adentrar aspectos como ameaças, vulnerabilidades, probabilidade e consequências. O objetivo é esclarecer se há dicotomia entre conformidade e risco, estabelecendo um olhar crítico e atencioso voltado à tomada de decisão frente, especialmente, aos riscos tecnológicos que podem violar direitos e liberdades dos titulares dos dados pessoais no ciberespaço. O trabalho adotou método dedutivo de pesquisa para entender risco, suas definições e algumas reflexões, passando à análise de riscos como ferramental jurídico e, também, tecnológico. O estudo possibilitou uma contribuição sobre riscos no contexto da proteção de dados pessoais, apontando que as questões de conformidade e risco estão profundamente interligadas quando analisadas do ponto de vista dos direitos e liberdades dos titulares dos dados pessoais. Para tal, discute-se sobre *Privacy Impact Assessment*, *Data Protection Impact Assessment*, no contexto do Regulamento Geral de Proteção de Dados na União Europeia, e sobre Relatório de Impacto à Proteção de Dados Pessoais,

ABSTRACT:

The article addresses compliance risks from the perspective of personal data protection, privacy and information security. The discussion begins by defining risk and its constituent elements to delve into aspects such as threats, vulnerabilities, probability and consequences. The main goal is to clarify whether there is a dichotomy between compliance and risk, establishing a critical and attentive look at decision-making in the face, especially, of technological risks that may violate the rights and freedoms of the holders of personal data in cyberspace. The study applied a deductive research method to understand risk, its definitions and some reflections, moving on to risk analysis as a legal and also technological tool. The study enabled a contribution on risks in the context of personal data protection, pointing out that compliance and risk issues are deeply intertwined when analyzed from the point of view of the rights and freedoms of the holders of personal data. To this end, it discusses the Privacy Impact Assessment, Data Protection Impact Assessment, in the context of the General Data Protection Regulation in the European Union, and the Impact Report on Personal Data Protection, in the context of the General Law for the Protection of Personal Data in Brazil. It is concluded that the lower the compliance, or the greater the event of non-compliance, the greater the risk in the vernacular sense, that is, in terms

[1] Professora Permanente e Coordenadora do Programa de Pós-Graduação em Direito (PPGD) da PUCPR. Doutora em Informática Aplicada pela PUCPR. Membro da Comissão de Direito Digital e Proteção de Dados da OAB/PR. Membro da Diretoria do Instituto Nacional de Proteção de Dados (INPD). E-mail: cinthia.freitas@pucpr.br

no contexto da Lei Geral de Proteção de Dados Pessoais no Brasil. Conclui-se que quanto menor a conformidade, ou maior o evento de não conformidade, maior será o risco no sentido vernáculo, ou seja, em termos de consequências ou danos aos direitos fundamentais, para os titulares de dados pessoais.

Palavras-chaves: Proteção de Dados Pessoais; Riscos; Segurança da Informação.

of consequences or damage to fundamental rights, for the holders of personal data.

Keywords: *Personal Data Protection; Risks; Information Security.*

SUMÁRIO

INTRODUÇÃO

Discutir a análise de riscos, sejam esses jurídicos ou tecnológicos, passam pelo entendimento do que vem se denominando como risco de conformidade, ainda pouco explorado e estudado do ponto de vista acadêmico. De um modo geral, sabe-se que quanto maior o risco, maiores são os problemas a enfrentar e, por consequência, a tomada de decisão envolverá recursos (humanos, financeiros, infraestrutura tecnológica, entre outros). Do ponto de vista da conformidade, seja a partir do *General Data Protection Regulation* (GDPR) na União Europeia ou da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, quanto menor a conformidade maior o risco. Tem-se uma relação inversamente proporcional e, portanto, necessita-se de um olhar crítico e atencioso voltado à tomada de decisão. Isso ocorre, devido ao fato de que maiores são as consequências sobre os titulares de dados, sendo assim uma relação aparentemente óbvia, mas de difícil compreensão. Isso devido ao fato de que se faz necessário compreender a conformidade e os riscos sob o prisma dos direitos e liberdades dos titulares dos dados pessoais. Pergunta-se: Há dicotomia entre conformidade e risco?

O objetivo desta contribuição é compreender a noção de risco frente à proteção de dados pessoais, no que tange a necessidade de realizar avaliações de impacto da proteção de dados (DPIA - *Data Protection Impact Assessment* - no GDPR ou RIPD – Relatório de Impacto à Proteção de Dados Pessoais - na LGPD), estabelecendo-se assim um instrumento de gestão de risco em matéria de proteção de dados pessoais.

O estudo recai sobre o significado de se considerar uma ferramenta baseada em risco quando se objetiva proteger dados pessoais. Nesse sentido o trabalho adotou método dedutivo de pesquisa para iniciar pelo estudo do risco, suas definições e algumas reflexões, para chegar à análise de riscos como ferramental jurídico e, também, tecnológico. Possibilitando, finalmente, uma contribuição sobre riscos no contexto da proteção de dados pessoais, evidenciando o risco de conformidade de acordo com o trabalho de Raphaël Gellert, o qual entende que as questões de conformidade e risco estão profundamente interligadas quando analisadas do ponto de vista dos direitos e liberdades dos titulares dos dados pessoais. O autor analisou o GDPR que prevê a obrigação de realizar avaliações de impacto da proteção de dados (DPIA), apresentando as diferenças entre PIA (*Privacy Impact Assessment*) e DPIA (*Data Protection Impact Assessment*) e ressaltando que a metodologia de análise de riscos se torna mais importante diante dos tipos de riscos que ameaçam os direitos e liberdades dos titulares dos dados pessoais.

1 RISCOS E ALGUMAS REFLEXÕES

O estudo inicia-se com o entendimento do que é risco e, cabe destacar que risco não é sinônimo de perigo. O trabalho de Raphaël Gellert (2017, p. 02) explica que existem 02 (dois) significados para risco: um vernáculo e outro técnico. Gellert se apoia em outro autor, Godard et al. (2002, p. 12) e assim explicam: (i) no sentido vernáculo, o risco é geralmente referido como futuro, possível perigo, ou seja, como "um eventual perigo que só pode ser previsto até certo ponto"[2] e (ii) no sentido técnico, risco é usado para a tomada de decisões com base em avaliação de even-

[2] Texto original: "an eventual danger that can be foreseen only to some extent".

tos futuros, sendo que seus elementos constitutivos são compostos por duas operações distintas, mas unidas e dependentes entre si, quais sejam: a) prever eventos futuros (tanto negativos quanto positivos) e tomar decisões com base nesses eventos.

Cabem aqui alguns contrapontos. O primeiro aponta que há que se nos riscos decorrentes da inter-relação e interdependência do homem contemporâneo com o meio ambiente digital, conceito estabelecido pelos autores Cavedon et al. (2015). O segundo contraponto é que deve-se ter por base que o tratamento de dados pessoais está (ou pode estar) vinculado ao surgimento de riscos capazes de comprometer a qualidade de vida do homem (titulares de dados), considerando-se o titular de dados como parte indissociável do meio em que vive e com o qual, necessariamente, interage. Especialmente, se o meio for o meio ambiente digital.

Assim, Cavedon et al. (2015, p. 197) explicam a partir de Pardo (1999, p 25-26) que, "enquanto os perigos têm causas essencialmente naturais, os riscos surgem a partir do momento em que os seres humanos passam a interferir no curso da natureza". E no meio ambiente digital não é diferente. O tratamento de dados pessoais gera interferências na privacidade dos indivíduos e, portanto, na personalidade, ou seja, no conjunto de características que definem uma pessoa, seu padrão de individualidade pessoal e social. Corresponde a dizer que, segundo os autores, os perigos advêm a partir das variações próprias do ambiente, enquanto os riscos surgem da intervenção do homem no intuito de eliminar esses perigos, ou seja, o homem passa a interferir no meio em que vive e, como consequência, os riscos se manifestam. Nesse contexto, pode-se afirmar que a origem dos riscos se vincula diretamente aos processos de tomada de decisão, refletindo claramente o anseio humano de subjugar a natureza, sendo que tratar dados pessoais sem consentimento, como definido em diversos regramentos e legislações nacional ou internacionalmente, é subjugar os direitos dos titulares, por exemplo a partir de violações, usos indevidos, cookies, entre outros.

Pode-se, portanto, argumentar que qualquer decisão relativa ao risco envolve 02 (dois) elementos distintos e inseparáveis: "os fatos obje-

tivos e uma visão subjetiva sobre a conveniência do que se ganha ou se perde com a decisão"[3] (BERNSTEIN, 1996, p. 100). E a tomada de decisão sobre o tratamento de dados pessoais não pode ser uma relação de perda para os titulares de dados.

Do ponto de vista técnico do significado de risco, deve-se ter em mente que risco é "combinação da probabilidade de um evento e de suas consequências", de acordo com ABNT ISO/IEC Guia 73 (2005). Tecnicamente, o risco é igual ao resultado da multiplicação da Consequência (C_i) pela Probabilidade (P_i); sendo que Consequência é o impacto ambiental caso ocorra um evento e Probabilidade é a probabilidade de ocorrência de um impacto que afete o meio ambiente, seja esse natural ou artificial no caso do meio ambiente digital. Outra definição de risco considera que "é um cenário que descreve um evento e suas consequências, estimado em termos de gravidade e probabilidade"[4] (DATA PROTECTION WORKING PARTY, 2017, p. 06). E, ainda, de acordo com a ISO/IEC 27001 (2022) risco é "o efeito da incerteza sobre os resultados desejados"[5], ou seja, há consequência(s) decorrente(s) do risco que estão sob um regime de incerteza (probabilidade de ocorrência).

A partir de Ulrich Beck (1998, p. 64) tem-se o entendimento de uma sociedade de risco, a qual tem sua origem quando as ameaças oriundas de ações e decisões humanas rompem os pilares de certeza estabelecidos pela sociedade industrial, minando, como consequência, os seus padrões de segurança. Sendo esse entendimento cabível na sociedade informacional em que se vive. No que tange aos dados pessoais, seja desde a coleta até seu descarte, passando por inúmeras operações de tratamento de dados, há que se considerar que os riscos abstratos, "além de imprevisíveis e incontroláveis, são também transfronteiriços e transtemporais" (CAVEDON et al., 2015, p. 200).

---

[3] Texto original: "the objective facts and a subjective view about the desirability of what is to be gained, or lose, by the decision".

[4] Texto original: "a scenario describing an event and its consequences, estimated in terms of severity and likelihood".

[5] Texto original: "the effect of uncertainty upon desired results".

Transfronteiriços porque ultrapassam os limites do local originalmente impactado, por exemplo onde ocorre a coleta de dados pessoais. Isto posto, porque na visão de Beck (2004, p. 109-110) confronta-se o conceito de fronteira, entendido como parte limítrofe de um espaço em relação a outro. No meio ambiente digital, delimitar fronteiras é por vezes impossível. Dados fluem.

E, são transtemporais porque não necessariamente se materializarão no momento em que se constituem, ou seja, a criação de um risco não implica, necessariamente, um dano imediato. Esse cenário é bem cabível em tratamento de dados pessoais, visto que dados coletados podem ser desviados para outra finalidade, sem que o titular consinta ou tenha conhecimento.

Diante dessas características, entende-se que Gellert (2017, p. 02) considera que o risco continua sendo uma noção abstrata que necessita de metodologias, modelos e processos que o implementem concretamente. E, a conjunção de aspectos técnicos e jurídicos é que irão permitir que se evite, previna, avalie, quantifique e, finalmente, se mitigue riscos, de modo a proteger dados pessoais.

Portanto, ao se ter por premissa que é impossível reduzir riscos à zero, independentemente da área de aplicação, há que se mitigar os riscos jurídicos e tecnológicos decorrentes do meio ambiente digital para se alcançar a proteção de dados pessoais e garantir direitos e liberdades dos titulares de dados.

Essa é a função da análise de risco, também chamada às vezes de gerenciamento de risco. Espelhando a dimensão dupla do risco, a análise de risco é composta de duas etapas (GELLERT, 2017, p. 02): (i) avaliação de risco: medir o nível de risco em termos de probabilidade e gravidade; (b) gerenciamento de risco: decidir se deve ou não assumir o risco. E, a decisão no nível de gerenciamento de risco é geralmente acompanhada de medidas que visam reduzir o nível de risco (GELLERT, 2017, p. 02). E existem muitos riscos jurídicos e tecnológicos relacionados ao tratamento de dados pessoais. Gellert (2017, p. 02) alerta que as medidas aplicadas na redução de riscos podem ser referidas por vezes como: redução de ris-

co, controle de risco, resposta a risco ou, mais genericamente, como medidas de mitigação de risco, termo comumente utilizado na área jurídica.

E estar em conformidade com o GDPR (UNIÃO EUROPEIA, 2016) ou a LGPD (BRASIL, 2018) é mitigar riscos. Mas há um ponto crucial nessa discussão que é determinar se o nível de risco é suficientemente baixo para que possa ser tomado. Por isso, no próximo item adentra-se a avaliação de risco, uma vez que alguns questionamentos precisam ser evidenciados, tais como: O que deve ser avaliado? O provável alto risco para os direitos e liberdades do titular dos dados ou o impacto sobre a proteção de dados pessoais? E como é que ambos precisam estar relacionados em uma avaliação de impacto?

O que muitas pessoas ainda não perceberam é que, ao mesmo tempo que tanto o GDPR quanto a LGPD são regramentos de proteção de dados pessoais, eles contêm em seu bojo um forte componente tecnológico. O lado tecnológico é tão importante quanto o jurídico, de modo que se pode considerar, no meio ambiente digital, que o GDPR a LGPD são instrumentos jurídicos de implementação tecnológica, portanto avaliar riscos tecnológicos a partir de uma sociedade informacional é mais do que necessário.

2 AVALIANDO RISCOS

Inicialmente cabe exemplificar alguns riscos de privacidade no ciberespaço, incluindo-se o meio ambiente digital, considerando-se que o ciberespaço é "constituído por comunicações eletrónicas de dados em um de três estados possíveis (ou por transmitir, ou em transmissão, ou já transmitidos) que fluem entre, e estão alicerçados em três camadas distintas (a física, a lógica e a cognitiva)" (BRAVO, 2021, p. 19). A Tabela 01 apresenta 03 (três) diferentes riscos à privacidade de usuários de Internet. Os cenários de ameaça à privacidade colocam em risco a proteção de dados pessoais e necessitam compor uma análise de riscos que em um panorama geral afetam direitos e liberdades dos titulares de dados. Os exemplos permitem compreender como um cenário de ameaça está relacionado com vulnerabilidades e riscos.

TABELA 01: Exemplos de riscos à privacidade no ciberespaço

Cenário de ameaça	Vulnerabilidades	Riscos
Uso de dispositivos computacionais móveis (smartphones, tablets e laptops): fácil coleta de dados pessoais, agregação e disseminação de informações.	Número crescente de pessoas realizando atividades no ciberespaço; Número crescente de fontes primárias de coleta de dados pessoais (câmeras, sensores biométricos, geolocalização).	Coleta de dados pessoais não necessários para fins primários; Armazenamento dos dados além do tempo de uso de direito; Divulgação de dados sensíveis sobre a vida ou os negócios de alguém.
Profissionalização dos crackers.	Uso de credenciais (login e senha) comuns para acessar vários sistemas.	Aplicativos ou sistemas sem funcionalidades ou controles de proteção de privacidade adequados.

Esses exemplos deixam claro que os dados pessoais, objeto o originário da proteção, estão sujeitos a riscos por meio de vulnerabilidades, sendo que "as vulnerabilidades de cariz tecnológico e a exposição a ações malévolas ou mesmo de menores cuidados de utilização, tornam o ciberespaço muito exposto a novas vulnerabilidades e ameaças, algumas de natureza disruptiva" (CALDAS; FREIRE, 2013, p. 02). Nota-se, portanto, que a análise de riscos tecnológicos não é trivial, havendo a necessidade de se distinguir entre análise de riscos e gestão de riscos.

Gellert (2017, p. 03) explica que a análise de risco é composta por etapas, a saber: (i) critérios de risco, (ii) identificação dos riscos e (iii) a avaliação de risco propriamente dita (ISO, 2009), sumarizadas a seguir:

- critérios de risco: compreende a definição de critérios para determinar se um evento pode ser considerado um risco, "os termos de referência contra os quais a significância de um risco

é avaliada"[6] (ISO, 2009, p. 5). Parte importante dessa definição está nos procedimentos para identificar o que se apresenta como risco e como medir o nível de risco;

- identificação de risco: definida como o "processo de localização, reconhecimento e descrição de riscos"[7] (ISO, 2009, p. 5). Será necessário estabelecer uma comparação entre o evento em questão e os critérios estabelecidos no item anterior. O objetivo é determinar se o evento é suficientemente arriscado para ser considerado um risco;
- avaliação de risco: aplicação de metodologia para obtenção, por exemplo, de uma matriz de riscos. Após essa etapa é que os riscos poderão ser gerenciados em termos de custos e benefícios. Eis aqui a etapa de tomada de decisão para estabelecer os riscos que necessitam de ação mais urgente ou podem ser deixados em segundo plano.

A necessidade de realizar a análise e a gestão dos riscos leva a compreensão de que a conformidade por si só, seja com o GDPR ou a LGPD, não garante a capacidade de uma organização proteger dados pessoais. É necessário criar um vínculo robusto entre requisitos, políticas, objetivos, desempenho e ações voltadas à mitigação dos riscos.

A criação desse vínculo exige estabelecer os elementos constitutivos do risco, a saber (GELLERT, 2017, p. 03):

- 1º elemento: é o evento, o qual é definido pela ISO (2009, p. 4) como uma "ocorrência ou mudança de um determinado conjunto de circunstâncias"[8]. O evento pode ou não acontecer e terá uma série de consequências positivas e negativas na proteção de dados pessoais;

---

[6] Texto original: "terms of reference against which the significance of a risk is evaluated".

[7] Texto original: "process of finding, recognizing and describing risks".

[8] Texto original: "occurrence or change of a particular set of circumstances".

- 2º elemento: são as consequências, que são precisamente o "resultado de um evento"[9] (ISO, 2009, p. 5), quando tais impactos são negativos podem ser referidos como danos, e quando são positivos podem ser referidos como benefícios;
- 3º. terceiro: são os fatores de risco. Eles determinam se e como o risco se materializará, ou seja, é a probabilidade de ocorrência, bem como a sua gravidade. Sendo "elementos que, isoladamente ou em combinação, têm potencial intrínseco para gerar risco"[10] (ISO, 2009, p. 4).

Há, portanto, que se conhecer a probabilidade e a gravidade de um evento, definidos pelo French Data Protection Authority (CNIL, 2015) e explicado por Gellert (2017, p. 02-03;06-08): a) gravidade: representa a magnitude de um risco, dependendo principalmente da natureza prejudicial dos impactos potenciais e b) probabilidade: representa a possibilidade de ocorrência ou não de um risco, dependendo essencialmente do nível de vulnerabilidades dos ativos que enfrentam ameaças e, ainda, do nível de recursos das fontes de risco para explorá-los.

Probabilidade é um conceito da Estatística e pode ser assim descrito (KAZMIER, 1982, p. 65):

> Se existem *a* resultados possíveis favoráveis à ocorrência de um evento *E* e *b* resultados possíveis não favoráveis à ocorrência de *E*, e sendo todos os resultados igualmente verossímeis e mutuamente exclusivos, então a probabilidade de *E* ocorrer é P(*E*) =

Spiegel (1978, p. 08) aponta que "há sempre uma incerteza quanto à ocorrência ou não de um determinado evento", definindo probabilidade de um evento P(*E*) como a ocorrência de *h* maneiras diferentes desse evento, em um total de *n* maneiras possíveis, todas igualmente possíveis, portanto, a probabilidade P(*E*) = *h*/*n*.

---

9 Texto original: "outcome of an event".

10 Texto original: "elements, which, alone or in combination has the intrinsic potential to give rise to risk".

Nesse caminho, de análise de riscos, deve-se estar também atento às normas técnicas, especialmente à família de normas 27000, como descrito na Tabela 02.

TABELA 02: Especificação das Normas ISO 27000.

Norma ISO	Conteúdo
ISO 27000	Generalidades, definições e diretrizes
ISO 27001	Técnicas de segurança para Sistemas de Gestão da Segurança da Informação (SGSI)
ISO 27002	Boas práticas para SGSI
ISO 27003	Diretrizes para implantação de um SGSI
ISO 27004	Indicadores de desempenho do SGSI
ISO 27005	Gestão de riscos de segurança da informação
ISO 27006	Requisitos e normas para organizações de auditoria e certificação pela ISO 27001/2
ISO 27007	Diretrizes para auditoria ISO 27001/2
ISO 27008	Diretrizes para auditoria de controles de SGSI
ISO 27010	Guia para a comunicação em gestão da segurança da informação
ISO 27014	Técnicas para governança da segurança da informação
ISO 27017	Controles específicos para computação em nuvem
ISO 27701 (antiga 27552)	Requisitos e exigências para estabelecer um Sistema de Gerenciamento de Informações de Privacidade

Fonte: adaptado de (FREITAS et al., 2020).

A norma ISO/IEC 27001 (2013) fornece orientação e direção de como uma organização, independentemente de seu porte e setor, deve gerenciar a segurança das informações e abordar os riscos de segurança das informações, possibilitando muitos benefícios não apenas para a organização, mas também para clientes, fornecedores e outras partes interessadas. Essa norma enfatiza a importância de: (i) entendimento dos requisitos de Segurança da Informação (SI) de uma organização e da necessidade de estabelecer uma política e objetivos para a SI; (ii) implementação e operação de controles para gerenciar os riscos de SI de uma organização no contexto dos riscos de negócio globais da organização; (iii) monitoramento e análise crítica do desempenho e eficácia do SGSI; e (iv) melhoria contínua baseada em medições objetivas. De uma maneira sumarizada, pode-se considerar que a norma aponta que a análise de riscos precisa: (i) definir a metodologia de avaliação de risco; (ii) realizar a avaliação de risco e tratamento de risco e (iii) elaborar um Plano de Tratamento de Risco.

Cabe salientar que a norma ISO/IEC 27001 (2013), bem como ISO/IEC 27001 (2022), não trata de proteção de dados, mas de Segurança da Informação. E é por isso que uma abordagem baseada em processos é tão útil para implementar um Sistema de Gestão de Segurança da Informação (SGCI), o qual deverá "assegurar a seleção de controles de segurança adequados e proporcionados para proteger os ativos de informação e propiciar confiança às partes interessadas" (ISO/IEC 27001, 2013, p. 01). E em uma sociedade informacional, preocupar-se com riscos cibernéticos é mandatório, de modo que não se pode deixar de lado a segurança cibernética e, consequentemente, a segurança das informações.

E qualquer que seja a metodologia adotada para a análise de riscos, a composição de um PIA (*Privacy Impact Assessment*) ou DPIA (*Data Protection Impact Assessment*) exigirá documentação técnica, conforme ISO/IEC 27001 (2013). Essa documentação deverá incluir: a) declarações documentadas da política e objetivos do SGSI (Sistemas de Gestão da Segurança da Informação); b) escopo do SGSI; c) procedimentos e controles que apoiam o SGSI; d) uma descrição da metodologia de análise/avaliação de riscos; e) relatório de análise/avaliação de riscos; f) plano de

tratamento de riscos; g) procedimentos documentados requeridos pela organização para assegurar o planejamento efetivo, a operação e o controle de seus processos de segurança de informação e para descrever como medir a eficácia dos controles; h) registros requeridos pela Norma ISO/IEC 27001 e i) declaração de aplicabilidade.

Caberá, portando, de acordo com ISO/IEC 27001 (2013), adotar um ciclo PDCA – *Plan-Do-Check-Act*, composto por 4 etapas, a saber: (i) *Plan*: compreende a definição de políticas, objetivos, metas, controles, processos e procedimentos, bem como realização do gerenciamento de riscos, que suportam a entrega de segurança da informação alinhada ao *core business* da organização; (ii) *Do*: implementação e operação dos processos planejados na etapa anterior; (iii) *Check*: monitoramento, medição, avaliação e revisão dos resultados em relação à política e objetivos de segurança da informação, para que ações corretivas e/ou de melhoria possam ser determinadas e autorizadas; (iv) *Act*: execução de ações autorizadas para garantir que a segurança da informação entregue seus resultados e possa ser melhorada.

Todos esses elementos confirmam que uma análise de riscos não é trivial, especialmente no contexto de riscos relacionados à proteção de dados pessoais, envolvendo especialmente riscos tecnológicos.

3 RISCOS E PROTEÇÃO DE DADOS PESSOAIS

Em uma leitura mais atenta da LGPD encontra-se um arsenal de termos técnicos da área de Segurança da Informação associados aos termos básicos da área de Ciência da Computação como um todo. Os termos: coleta de dados, tratamento de dados, anonimização, bloqueio, prevenção, riscos, medidas, salvaguardas e mecanismos de mitigação de riscos e relatórios de impacto à proteção de dados pessoais; são alguns exemplos de aspectos tecnológicos que permeiam o texto legislativo.

Cabe lembrar que a unidade básica de proteção, seja no GDPR ou na LGPD, são os dados e sobre eles recaem todas as preocupações e modificações que precisam ser desenvolvidas e implantadas seja nos

sistemas, nos processos ou na organização como um todo, pública ou privada (FREITAS et al., 2016).

3.1 Definindo Dados, Dados Pessoais e Tratamento de Dados Pessoais

A classificação de dados é extensa e envolve conceitos teóricos e técnicos, antes mesmo de conceitos e aplicações jurídicas do termo "dados" (BOFF et al., 2018, p. 201-214). O termo 'dados' é tão amplo que permite até mesmo ser utilizado conceitualmente como política e fenômeno social, podendo-se até mesmo considerar a existência de ecossistema de dados (*data ecosystems*), envolvendo organizações complexas de relações sociais dinâmicas por meio das quais dados e informações se movem e se transformam (DATA-POP ALLIANCE, 2015, p. ii).

De acordo com Laudon e Laudon (1999, p. 10) dado é diferente de informação, ou melhor, dado não é informação, portanto, não são sinônimos (Freitas, 2016). Para os autores "dado são os fatos brutos, o fluxo contínuo de coisas que estão acontecendo agora e que aconteceram no passado". São também "*An object, variable, or piece of information that has the perceived capacity to be collected, stored, and identifiable.*" (DATA-POP ALLIANCE, 2015, p. ii). E, informação é "o conjunto de dados aos quais seres humanos deram forma para torná-los significativos e úteis". Simon (1999, p. 1) explica que "um dado é uma sequência de símbolos, é um ente totalmente sintático, não envolve semântica como na informação".

Para tal, conceitua-se dado, informação e conhecimento como Castro e Ferrari (2016, p. 04):

> Os dados são símbolos ou signos não estruturados, sem significado, como valores em uma tabela, e a informação está contida nas descrições, agregando significado e utilidade aos dados, como o valor da temperatura do ar. Por fim, o conhecimento é algo que permite uma tomada de decisão para a agregação de valor, então, por exemplo, saber, que vai chover no fim de semana pode influenciar sua decisão de viajar ou não para a praia.

Cabe destacar que dados, em especial dados pessoais, constituem um fator de grande interesse às organizações, possibilitando agilidade nos processos de busca e de recuperação de informações, caracterização de perfil de consumidores (*profiling*) (FREITAS; PAMPLONA, 2017, p. 119-144), categorização de gostos e preferências. Assim, a transformação de grandes volumes de dados textuais ou não (imagens, áudio, vídeo), estruturados ou não em informação útil fornece elementos para a reorganização, avaliação, utilização, compartilhamento e armazenamento, enfim, tratamento de dados e, consequentemente, de modo geral, de obtenção de conhecimento a partir do conjunto bruto de dados transformado em informação. Deve-se ter em mente que dados geram informações sobre pessoas, que por sua vez geram mais e mais dados.

Para a LGPD, dado pessoal é "dado pessoal: informação relacionada a pessoa natural identificada ou identificável;" (LGPD, art. 5º, inciso I). E, os dados, pessoais ou não, possuem um ciclo de vida, ou seja, desde seu nascimento até sua morte, descarte. Para tal, tem-se o nascimento como a operação de coleta e a morte como as operações de eliminação ou descarte. São muitas as operações que compõem o ciclo de vida dos dados, o qual, por sua vez, está diretamente ligado com a definição de "tratamento de dados" (LGPD, art. 5º, inciso X):

> tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

As operações listadas de modo exemplificativo e não restritivo. Essas operações não compreendem o conjunto completo de possibilidades de tratamento de dados pessoais ou sensíveis. Deve-se ter em mente que o texto legislativo não se prende às técnicas ou aos métodos computacionais ou operacionais, uma vez que a partir de determinadas operações exemplificadas no art. 5º, inciso X, pode-se realizar desde a captura do

dado até a aplicação de técnicas de Mineração de Dados (*Data Mining*) ou Aprendizagem de Máquina (*Machine Learning*).

3.2 DADOS PESSOAIS, PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO

E, por sua vez, a proteção de dados une-se à Segurança da Informação que tem por base algumas propriedades, a saber: "preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas"[11].

A Segurança da Informação nunca esteve tão em evidência como a partir da promulgação do GDPR e da LGPD. E, entre a proteção de dados e a Segurança da Informação, há que se entender que a proteção é sobre os dados (unidade originária), mas a segurança considera uma abrangência maior, ou seja, os dados, os sistemas, os processos e a organização. A proteção de dados age sobre o objeto, sem semântica. A Segurança da Informação atua sobre a semântica, visto que a informação já constitui resultado a partir de processamento. Já foi estabelecida uma forma para a informação, portanto, a proteção é base para a segurança.

Por isso, o art. 6º, incisos VII e VIII, da LGPD estabelecem que o tratamento de dados deve observar a boa-fé e, ainda, a segurança e a prevenção. Ambos englobando 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" e a "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais".

[11] A partir de 2007, a norma ISO/IEC 17799 foi incorporada ao novo sistema de numeração de normas, passando a constar como ISO/IEC 27002. ABNT NBR ISO/IEC 17799. Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. 2005. p. 01.

Neste sentido, as normas ISO/IEC da família 27000 foram preparadas para "prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)."[12] Assim, as normas relacionadas à Segurança da Informação não mencionam dados ou informações, mas ativos que representam "qualquer coisa que tenha valor para a organização".

Do ponto de vista tecnológico, a LGPD indica como aspecto formal a manutenção de registro das operações de tratamento de dados por parte tanto do controlador quanto do operador, ou seja, pelos agentes de tratamento de dados, especialmente quando o tratamento tiver por base o legítimo interesse (artigo 37, LGPD).

Entender o ciclo de vida dos dados nas organizações é vital para a proteção de dados pessoais, uma vez que cada vez mais dados são ativos, tal qual tratados nas normas ISO/IEC da família 27000 (2013) que foram preparadas para "prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)". Assim, as normas relacionadas à Segurança da Informação não mencionam dados ou informações, mas ativos que representam "qualquer coisa que tenha valor para a organização" (ISO/IEC, 2013, p. 2).

O lado tecnológico da LGPD fica ainda mais evidente em razão da recente publicação da norma ISO 27701 (ABNT NBR ISO/IEC, 2019), que estabelece um novo padrão internacional específico para tratar da extensão de privacidade da norma ISO 27001. Tal norma tem por objetivo aprimorar o Sistema de Gestão de Segurança da Informação (SGSI) sob a ótica da privacidade de dados. Isto no intuito de estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Informações de Privacidade – SGIP.

Um SGIP é diferente de um SGSI, mas eles estão intimamente relacionados. A norma ISO/IEC 27701 reconhece que a Segurança da

[12] ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. 2013. p. v.

Informação e a preservação das suas propriedades: confidencialidade, integridade e disponibilidade; é um aspecto fundamental para que o gerenciamento de privacidade seja eficaz, e que os requisitos de um SGSI estabelecidos na norma ISO/IEC 27001 podem subsidiar com requisitos adicionais a gestão da privacidade. A norma ISO/IEC 27701 possibilita definir os requisitos extras para que um SGSI possa englobar a privacidade e o processamento de dados pessoais. A relação entre proteção de dados e privacidade torna-se ainda mais evidente. Como um todo novo, isso cria o que o Padrão chama de sistema de gerenciamento de informações de privacidade (PIMS).

3.3 PIA, DPIA E RIPD NA PROTEÇÃO DE DADOS PESSOAIS

O *French Data Protection Authority* (CNIL, 2015, p. 01) explica que o acrônimo PIA é usado de forma intercambiável para se referir à Avaliação de Impacto de Privacidade (*Privacy Impact Assessment*) e Avaliação de Impacto de Proteção de Dados (DPIA - *Data Protection Impact Assessment*). O PIA é um processo contínuo de melhoria e pode requerer inúmeras iterações para que se estabeleça um sistema de proteção de privacidade aceitável em termos de riscos e demais elementos de conformidade. Requer também acompanhamento das mudanças ao longo do tempo, no que concerne ao contexto, controles e riscos. O PIA pode ser entendido como uma ferramenta voltada a identificar e avaliar os riscos de privacidade ao longo do ciclo de vida de desenvolvimento de uma organização, pública ou privada. Assim, uma avaliação de impacto de privacidade deverá apontar quais informações de identificação pessoal, dados pessoais, foram coletadas e explicar, também, como esses dados são mantidos e compartilhados, bem como são ou serão protegidos, incluindo os métodos para os titulares de dados fornecerem consentimento para a coleta de dados pessoais (CNIL, 2015, p. 10-16).

Por outro lado, o *Data Protection Impact Assessment* (DPIA) está expressamente declarado no GDPR, artigo 35 (1), de modo a: "Quando um tipo de tratamento (...) é suscetível de resultar em um alto risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamen-

to deve, antes do processamento, realizar uma avaliação do impacto (...) sobre a proteção de dados pessoais."[13] Portanto, um DPIA é o estudo dos impactos de um projeto apenas na privacidade de dados pessoais, enquanto uma PIA considera todas as dimensões da privacidade. Por isso, Gellert (2017, p. 08) alerta que o termo avaliação de impacto na proteção de dados (DPIA) é um termo de escopo mais limitado do que uma avaliação de impacto na privacidade (PIA).

A LGPD explicita que o Relatório de Impacto à Proteção de Dados (RIPD) será necessário sempre que o tratamento de dados pessoais puder expor a risco liberdades civis e direitos fundamentais (art. 5º, inciso XVII, da LGPD) ou, quando o fundamento para essa atividade for o interesse legítimo (artigo 10 da LGPD). Será responsabilidade do controlador e o RIPD detalhará as operações com dados pessoais, as medidas, salvaguardas e mecanismos de mitigação de riscos adotadas (art. 5º, inciso XVII, da LGPD). Trata-se de instrumento que atende aos princípios da transparência, segurança, prevenção e prestação de contas (art. 6º, incisos VI, VII, VIII e X, da LGPD).

Necessário observar que de acordo com a LGPD, o RIPD deverá ser gerado apenas em casos de tratamento de dados que expuserem o titular de dados a risco, não se referindo a todos ou qualquer processo ou sistema organizacional. Especificamente, o artigo 38, parágrafo único da LGPD aponta: "a descrição dos tipos de dados coletados, a metodologia utilizada para coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mitigação de riscos adotados".

Todo o estudo ora realizado permite não ver uma ambiguidade ou uma contradição entre riscos para os direitos e liberdades dos titulares de dados pessoais e os impactos na privacidade e, consequentemente, na proteção de dados pessoais. Essa ambiguidade não pode existir, uma vez que a definição de risco envolve observar os cenários, incluindo seus

---

[13] Texto original: Where a type of processing (. . .) is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact (. . .) on the protection of personal data".

eventos e consequências. Cabe questionar que esses direitos e liberdades não se referem apenas ao direito à privacidade, mas incluem outros direitos fundamentais, como liberdade de expressão, liberdade de pensamento, liberdade de movimento, proibição de discriminação, direito à liberdade, consciência e religião. Envolvendo-se assim dados pessoais e dados pessoais e sensíveis.

Nesse entendimento, a proteção de dados pessoais pode ser um evento dentro da análise de riscos, visto que quando os dados pessoais não são protegidos de forma adequada, ou seja, quando as disposições e obrigações de proteção de dados não são cumpridas, não se tem conformidade, tal evento leva à violação potencial de todos os direitos fundamentais dos titulares dos dados afetados por operações de tratamento de dados.

Não há como violar direitos fundamentais sem que dados pessoais sejam utilizados, tratados e, infelizmente, vazados. É a não proteção de dados pessoais que permite a violação de direitos fundamentais. A proteção de dados pessoais é ferramenta, enquanto a não proteção e a porta de entrada às violações. E não há como proteger dados sem que se considere a Segurança da Informação. A proteção de dados age sobre o objeto originário, como analisado anteriormente, ou seja, dados, sem semântica. A Segurança da Informação atua sobre a semântica, visto que a informação já constitui resultado a partir de processamento, seja manual ou computacional. Assim, tem-se estabelecida uma forma para a informação, portanto, a proteção é base também para a segurança.

CONCLUSÃO

Analisar riscos sob a perspectiva da proteção de dados pessoais, tendo por premissas aspectos jurídicos e tecnológicos, bem como a privacidade como ponto focal, não é tarefa trivial.

O artigo iniciou pelo estudo e definição de risco, abrangendo diferentes aspectos e pontuando algumas reflexões sobre evento, probabilidade e consequência; visto que estar em conformidade com legislações

ou regramentos de proteção de dados é mitigar riscos. Em seguida, adentrou-se à análise de riscos estabelecendo uma conexão com a segurança da informação e normas técnicas, a exemplo da família ISO/IEC 27000. E, então, foram apresentadas as definições de PIA, DPIA e RIPD para contextualizar tanto a complexidade quanto os caminhos possíveis a serem observados em uma análise de riscos no contexto da privacidade visando a proteção de dados pessoais.

Finalmente, concorda-se com Gellert que quanto menor a conformidade, ou maior o "evento de não conformidade"[14], maior será o risco no sentido vernáculo, ou seja, em termos de consequências ou danos aos direitos fundamentais, para os titulares de dados pessoais. Eis o desafio, seja do PIA, DPIA ou RIPD.

REFERÊNCIAS

ABNT ISO/IEC Guia 73. Gestão de riscos – Vocabulário: recomendações para uso em normas. 2005.

BECK, Ulrich. Conversation 3: global risk society. I*n:* BECK, Ulrick; WILLMS, Johannes (Org.). **Conversations with Ulrich Beck.** Trad. de Michael Pollak. Cambridge: Polity, 2004.

BECK, Ulrich. **La sociedad del riesgo**: hacia una nueva modernidad. Trad. de Jorge Navarro, Daniel Jiménez, Maria Rosa Borrás. Barcelona: Paidós, 1998.

BERNSTEIN, Peter L. **Against the gods**: the remarkable story of risk. New York: John Wiley & Sons Inc., 1996.

BOFF, Salete Oro; FORTES, Vinicius Borges, FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade**: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.

BRAVO, Rogério. **Segurança da informação, cibersegurança e cibercrime**: contributos para um alinhamento de conceitos. Lisboa, v. 12, 2021.

BRASIL. **Lei 13.709, de 14 de agosto de 2018**, Lei Geral de Proteção de Dados - LGPD, 2018.

[14] Texto original: non-compliance event.

CALDAS, Alexandre; FREIRE, Vicente. **Cibersegurança**: das preocupações à ação. Instituto de Defesa Nacional – IDN, Working Paper 2, Lisboa, Portugal, 2013.

CASTRO, Leandro Nunes de; FERRARI, Daniel Gomes. **Introdução à mineração de dados. Conceitos básicos, algoritmos e aplicações.** São Paulo: Saraiva, 2016.

CAVEDON, Ricardo; FERREIRA, Heline Sivini; FREITAS, Cinthia Obladen de Almendra. **O Meio Ambiente Digital sob a Ótica da Teoria da Sociedade de Risco**: os avanços da informática em debate. Revista Direito Ambiental e Sociedade, v. 5, p. 194-223, 2015.

CNIL. **Privacy Impact Assessment (PIA)**: methodology. French Data Protection Authority, 2018.

DATA-POP ALLIANCE. **Beyond data literacy**: reinventing community engagement and empowerment in the age of data. White paper series, set., 2015.

DATA PROTECTION WORKING PARTY. Guidelines on data protection impact assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 (WP29). Artic. 29 Data Prot. Work. Party. WP 248 rev 22 (2017). 2017.

FREITAS, Cinthia Obladen de Almendra; SANTOS, Henrique Guilherme; PASINATO, Rita. A Segurança da Informação como Ferramental Técnico da Proteção de Dados Pessoais. *In*: Mariana Pereira Faria; Rafael Aggens Ferreira da Silva; Rhodrigo Deda Gomes. (Org.). **Direito e Inovação** - Volume 3. 1ed.Curitiba: NCA - Comunicação e Editora LTDA, 2020, v. 3, p. 233-265.

FREITAS, Cinthia Obladen de Almendra; BARBOSA, Claudia Maria; TAVARES NETO, José Querino. Privacidad y Protección Legal de Datos de Servicios en Línea bajo la Óptica de la Legislación Brasileña. *In:* Lorena Muñoz Sánchez. (Org.). **Hacia uma Justicia 2.0**. 1ed.Salamanca: FIADI - Federación Iberoamericana de Associaciones de Derecho y Informática, 2016, v. III, p. 127-140.

FREITAS, Cinthia Obladen de Almendra. O. A., PAMPLONA, Danielle Anne. Cooperação entre Estados Totalitários e Corporações: O uso da segmentação de dados e profiling para violação de direitos humanos. *In:* Regina Linden Ruaro; José Luis Piñar Mañas; Carlos Alberto Molinaro. (Org.). **Privacidade e proteção de dados pessoais na sociedade digital.** 1ed. Porto Alegre: Editora Fi, v. 1, p. 119-144, 2017.

GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. **Computer Law & Security Review: The International Journal of Technology Law and Practice**, p. 1-10, 2017.

GODARD, Olivier; HENRY, Claude; LAGADEC, Patrick; MICHEL-KERJAN, Erwann. **Traité des nouveaux risques,** Paris: Éditions Gallimard, 2002.

ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. 2022.

ISO/IEC 27001. Information technology — Security techniques — Information security management systems — Requirements. 2013.

ISO/IEC 1333-1. Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management. 2004.

ISO. Risk management - Principles and guidelines. International Organization for Standardization, Geneva, Switzerland, 2009.

KAZMIER, Leonard J. **Estatística Aplica à Economia e Administração**. Trad. Carlos Augusto Crusius; Revisão Técnica Jandyra M. Fachel. São Paulo: Pearson Makron Book, 1982.

LAUDON, K. C., LAUDON, J. Price. **Sistemas de informação**. Rio de Janeiro: Livros Técnicos e Científicos S.A., 1999.

PARDO, José Esteve. **Técnica, riesgo y derecho**. Barcelona: Ariel, 1999.

UNIÃO EUROPEIA. **General Data Protection Regulation**, 2016. Disponível em: https://gdpr-info.eu/ Acesso em: 09.mar. 2023.