ISBN: 978-65-986235-6-2

Aurum EDITORA

CAPÍTULO 4

SEGURANÇA DA INFORMAÇÃO E A PROTEÇÃO DE DADOS

INFORMATION SECURITY AND DATA PROTECTION

https://doi.org/10.63330/aurumpub.006-004

Alessandro Virgini de Oliveira
Pós-graduação em direito notarial e Registral
Faculdade Anhanguera

RESUMO

A segurança da informação e a proteção de dados pessoais constituem o eixo central deste Trabalho de Conclusão de Curso, que discute a importância de preservar os ativos informacionais das organizações diante de ameaças físicas, lógicas, acidentais ou intencionais. O objetivo principal é analisar os fundamentos da segurança da informação, os riscos envolvidos, as ameaças contemporâneas e a legislação aplicável, com ênfase na Lei Geral de Proteção de Dados (LGPD) e no Regulamento Geral sobre a Proteção de Dados (RGPD). A metodologia adotada é de natureza bibliográfica e documental, com base em autores especializados e em normativas nacionais e internacionais. O trabalho está estruturado em três capítulos: o primeiro aborda os conceitos fundamentais, princípios e evolução da segurança da informação; o segundo trata das ameaças que comprometem a integridade e a confiabilidade dos sistemas; o terceiro analisa os dados pessoais, os mecanismos de proteção e os requisitos legais para o tratamento seguro das informações. Os resultados da produção indicam que a segurança da informação deve ser tratada como um processo contínuo e estratégico, envolvendo a participação de todos os níveis da organização, políticas claras, práticas preventivas e o cumprimento rigoroso da legislação vigente. Conclui-se que, em um cenário digital cada vez mais complexo, é essencial que organizações públicas e privadas adotem uma cultura sólida de proteção informacional, integrando tecnologia, governança e responsabilidade jurídica.

Palavras-chave: Segurança da informação; Proteção de dados; Riscos digitais; Privacidade.

ABSTRACT

Information security and the protection of personal data form the central axis of this Final Paper, which discusses the importance of preserving organizations' information assets in the face of physical, logical, accidental or intentional threats. The main objective is to analyze the fundamentals of information security, the risks involved, contemporary threats and applicable legislation, with an emphasis on the General Data Protection Law (LGPD) and the General Data Protection Regulation (GDPR). The methodology adopted is of a bibliographical and documentary nature, based on specialized authors and national and international regulations. The work is structured in three chapters: the first deals with the fundamental concepts, principles and evolution of information security; the second deals with the threats that compromise the integrity and reliability of systems; the third analyzes personal data, protection mechanisms and legal requirements for the secure processing of information. The results indicate that information security must be treated as a continuous and strategic process, involving the participation of all levels of the organization, clear policies, preventive practices and strict compliance with current legislation. The conclusion is that, in an increasingly complex digital landscape, it is essential for public and private organizations to adopt a solid culture of information protection, integrating technology, governance and legal responsibility.

Keywords: Information security; Data protection; Digital risks; Privacy.

1 INTRODUÇÃO

A crescente dependência das organizações modernas em relação às tecnologias da informação trouxe à tona a necessidade de estratégias eficazes para garantir a segurança dos dados e a proteção da privacidade. No contexto atual, marcado por transformações digitais aceleradas e pela proliferação de ameaças cibernéticas, a segurança da informação tornou-se um componente estratégico essencial à governança corporativa, ultrapassando sua concepção tradicional e técnica para abranger aspectos organizacionais, legais e humanos. Autores como Mitnick e Simon (2003) e Wood (2004) destacam que a segurança da informação não pode ser tratada como um produto técnico isolado, mas como uma prática contínua, multidisciplinar e integrada à cultura organizacional.

Este trabalho tem como tema a segurança da informação e a proteção de dados pessoais, com foco na compreensão de seus fundamentos, riscos associados, regulamentações legais e práticas organizacionais voltadas à sua aplicação. A abordagem se ancora na literatura especializada, como Andress (2014), Peltier (2013) e Dibble (2020), que defendem a importância da gestão de riscos e da implementação de políticas robustas de proteção da informação em conformidade com a legislação vigente. O objetivo geral é analisar os principais conceitos e práticas relacionadas à segurança da informação e à proteção de dados, especialmente à luz da Lei Geral de Proteção de Dados (LGPD) e do Regulamento Geral de Proteção de Dados da União Europeia (RGPD). Como objetivos específicos, busca-se compreender os fundamentos e princípios da segurança da informação; identificar os tipos de ameaças existentes e seus impactos sobre os sistemas organizacionais; examinar a importância da proteção de dados pessoais; e discutir os marcos normativos e iniciativas internacionais relacionados ao tema.

Parte-se da hipótese de que a adoção de políticas integradas de segurança da informação, alinhadas à legislação vigente e à cultura institucional, é essencial para mitigar riscos e garantir a proteção de dados sensíveis, promovendo a confiança dos usuários e a vantagem competitiva das organizações. A justificativa desta pesquisa está na relevância crescente do tema frente à expansão dos crimes cibernéticos, à crescente digitalização de processos e à necessidade de conformidade com normas nacionais e internacionais. Além disso, como argumenta Dinis (2005), a informação tornou- se um ativo estratégico e, ao mesmo tempo, um alvo vulnerável em tempos de guerra informacional, demandando ações preventivas e estruturadas.

A metodologia adotada é baseada em pesquisa bibliográfica e documental, com foco na análise de obras consagradas na área da segurança da informação, bem como nas principais legislações e normativas aplicáveis ao tema. O trabalho está dividido em quatro capítulos. O primeiro capítulo aborda a segurança da informação, seus conceitos fundamentais, evolução histórica e os princípios do chamado triângulo da segurança: confidencialidade, integridade e disponibilidade. O segundo capítulo discute as ameaças à segurança da informação, tanto de natureza física quanto lógica, abordando a guerra da informação, o papel da Internet como novo “teatro de guerra” e os riscos associados à cibercriminalidade, conforme discutido

por Dinis (2005). O terceiro capítulo trata dos dados pessoais, da proteção de dados e da segurança do tratamento, explorando os conceitos definidos por autores como Sharma e Menon (2020), Lin e Kifer (2014) e Dibble (2020), além das exigências do RGPD e da LGPD.O quarto capítulo trata da Lei Geral de Proteção de Dados (LGPD).

O quinto e último capítulo apresenta a conclusão do estudo, retomando os principais pontos discutidos, avaliando o alcance dos objetivos propostos e sugerindo possíveis direções para futuras pesquisas e boas práticas organizacionais.

Com essa estrutura, o presente Trabalho de Conclusão de Curso pretende contribuir com o debate acadêmico e com a prática profissional sobre a importância de proteger os ativos informacionais e os dados pessoais em um cenário cada vez mais digital e vulnerável.

2 DESENVOLVIMENTO

2.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação configura-se como um campo essencial no contexto organizacional contemporâneo, pois tem como objetivo a proteção dos ativos informacionais de uma entidade — sejam dados digitais, sistemas, hardware, software, processos ou pessoas — contra ameaças internas e externas que possam comprometer sua confidencialidade, integridade e disponibilidade. Com o avanço da tecnologia e sua crescente integração aos processos empresariais, a segurança da informação deixou de ser uma responsabilidade meramente técnica, passando a constituir um elemento estratégico da governança corporativa (Mitnick e Simon,2003).

Historicamente, a segurança da informação era tratada como um conjunto de medidas técnicas voltadas à proteção de equipamentos e redes computacionais. No entanto, com o crescimento da digitalização, da mobilidade e da interconectividade, essa visão reducionista revelou-se inadequada. Atualmente, entende-se que a segurança da informação é um processo contínuo, multidisciplinar e dinâmico, envolvendo não apenas aspectos tecnológicos, mas também gestão, cultura organizacional, políticas internas, capacitação dos usuários e conformidade legal. Conforme salientam Mitnick e Simon (2003), assim como Wood (2004), a segurança não pode ser adquirida como um produto de prateleira; ela precisa ser incorporada como uma prática constante nas organizações, fundamentada na análise de riscos e na implementação de controles apropriados.

Os princípios fundamentais da segurança da informação compreendem a confidencialidade, a integridade e a disponibilidade, formando o conhecido "triângulo da segurança da informação". A confidencialidade assegura que apenas pessoas autorizadas tenham acesso às informações sensíveis; a integridade garante que os dados permaneçam inalterados de forma indevida ou acidental, assegurando sua exatidão e confiabilidade; e a disponibilidade assegura que as informações estejam acessíveis sempre que

necessárias, garantindo a continuidade das operações organizacionais. Para Andress (2014), essas propriedades são vitais para que uma organização opere de maneira segura, eficiente e confiável.

O risco em segurança da informação refere-se à possibilidade de uma ameaça explorar uma vulnerabilidade e causar dano aos ativos informacionais. Esse risco está relacionado à incerteza diante de eventos adversos, como ataques cibernéticos, falhas de sistemas, erros humanos, desastres naturais ou violações de políticas internas, os quais podem acarretar prejuízos financeiros, danos à reputação, responsabilidades legais e até a paralisação de operações críticas. A gestão de riscos exige uma abordagem sistemática, envolvendo identificação, avaliação, tratamento e monitoramento constante dos riscos relevantes. Conforme argumenta Purdy (2010), essa abordagem é essencial para assegurar a resiliência organizacional. Peltier (2013) também destaca que a segurança da informação deve proteger não apenas os ativos digitais, mas o próprio valor do negócio, preservando a confiança dos stakeholders e a sustentabilidade institucional.

A ocorrência de falhas nos sistemas ou a existência de brechas na proteção de dados pode gerar consequências graves. As perdas podem se manifestar de forma direta, como o roubo de informações estratégicas ou a destruição de dados, ou de forma indireta, como interrupções em serviços, perda de vantagem competitiva ou danos à imagem institucional. Em paralelo, diversas legislações ao redor do mundo impõem obrigações rigorosas quanto à proteção de dados pessoais. No Brasil, por exemplo, a Lei Geral de Proteção de Dados (LGPD) reforça a necessidade de adoção de políticas robustas de segurança da informação (Peltier, 2013).

Dessa maneira, a segurança da informação não deve ser tratada como um projeto pontual ou uma simples exigência de compliance. Ao contrário, precisa ser incorporada como um processo organizacional permanente, vinculado à estratégia empresarial e sustentado por uma cultura de segurança disseminada em todos os níveis da organização. Isso envolve ações como a conscientização e o treinamento dos colaboradores, o estabelecimento de políticas e normas claras, o uso de tecnologias apropriadas, a realização de auditorias regulares e a execução de testes de vulnerabilidade. A construção de um ambiente organizacional seguro depende, portanto, da integração eficaz entre pessoas, processos e tecnologias, orientada por uma perspectiva holística de proteção e resiliência (Peltier, 2013).

No cenário internacional, a preocupação com a cibersegurança tem sido reiteradamente reforçada. Em 2006, a Organização das Nações Unidas estabeleceu o dia 17 de maio como o Dia Mundial da Sociedade da Informação, dedicando essa data à promoção da cibersegurança. Na ocasião, o então Secretário-Geral da ONU, Kofi Annan, destacou que, em um mundo cada vez mais interligado, proteger sistemas e infraestruturas vitais contra ataques cibernéticos, ao mesmo tempo em que se promove a confiança nas transações eletrônicas, é fundamental para o desenvolvimento do comércio, das relações bancárias, da telemedicina, da administração pública eletrônica e de outras aplicações digitais (ONU,1948).

Segundo Vaz (2007), o Conselho da Europa também demonstrou preocupação com a criminalidade informática, especialmente considerando seu caráter frequentemente transfronteiriço. Em 1989, aprovou a Recomendação nº R(89)9, com o objetivo de harmonizar legislações e práticas internacionais nessa área. Do mesmo modo, a Organização para Cooperação e Desenvolvimento Econômico (OCDE) estabeleceu, em 1992, diretrizes para a segurança dos sistemas de informação, que foram posteriormente revistas em 1997. A reavaliação foi motivada pelo crescimento das ameaças, incluindo os impactos dos atentados de 11 de setembro. Em 2002, o Conselho da OCDE aprovou novas diretrizes para a segurança dos sistemas de informação e das redes (Vaz, 2007).

No âmbito da União Europeia, foi criada, em 2004, a Agência Europeia para a Segurança das Redes e da Informação, com a missão de reforçar a capacidade dos Estados-Membros na prevenção, tratamento e resposta a problemas de segurança informacional e de redes. Paralelamente, a International Standardization Organization (ISO) passou a estabelecer normas específicas para os padrões de segurança, como a ISO 17799:2000, que abrange aspectos como política de segurança, segurança organizacional, segurança física e ambiental, controle de acesso, desenvolvimento e manutenção de sistemas, além da ISO 15443, voltada para a segurança em informática (Vaz,2007).

Em Portugal, também houve esforços para a definição de normas de segurança da informação, especialmente para o tratamento de informações classificadas. Foram estabelecidas diretrizes como o SEGNAC 1, que trata da segurança nacional e informática na administração pública; SEGNAC 2, voltado à segurança industrial, tecnológica e de pesquisa; SEGNAC 3, sobre segurança nas telecomunicações; e SEGNAC 4, especificamente direcionado à segurança da informação. Os programas e documentos são classificados conforme critérios específicos, em categorias como "Muito Secreto", "Secreto", "Confidencial" ou "Reservado", sendo essa responsabilidade atribuída aos diretores de empresas e órgãos públicos. Informações classificadas como “Muito Secreto” ou “Secreto” só podem ser processadas por meios eletrônicos se não houver oposição da entidade emissora (Vaz,2007).

Para assegurar a proteção dessas informações, foi criada a Autoridade Nacional de Segurança no âmbito da OTAN. No Brasil, o Instituto de Informática do Ministério das Finanças e a Autoridade Nacional de Segurança publicaram, em 1995, o "Manual Técnico de Segurança dos Sistemas e Tecnologias de Informação", contendo os princípios que devem ser seguidos pelos responsáveis por sistemas informáticos tanto da administração pública quanto de instituições privadas. Já o Decreto-lei nº 217/97, de 20 de agosto, estabeleceu a transformação da Autoridade Nacional de Segurança no Gabinete Nacional de Segurança, com competência para inspecionar periodicamente os órgãos de segurança, garantindo o cumprimento das normas aplicáveis às comunicações, à informática e aos sistemas de informação (Vaz,2007).

2.2 AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

Dada a sua relevância estratégica, a informação e o conhecimento passaram a ocupar uma posição central nos conflitos contemporâneos, a ponto de surgir o conceito de Guerra de Informação. Essa expressão refere-se, em sentido amplo, à necessidade de proteger os interesses de cidadãos, Estados e organizações — sejam elas nacionais ou supranacionais — contra ações que busquem prejudicá-los. Em sentido mais restrito, trata-se da utilização da informação como instrumento de conflito entre diferentes atores sociais. Nesse contexto, a Guerra do Golfo é frequentemente apontada como o primeiro conflito da chamada Era da Informação (Dinis, 2005).

A transmissão de dados por meio da Internet tornou-se essencial para a vida em sociedade moderna. No entanto, essa mesma dependência acarreta riscos significativos, pois a rede apresenta um elevado grau de vulnerabilidade. Os sistemas informáticos estão constantemente sujeitos a ataques conduzidos por hackers e *crackers*, que podem agir de forma autônoma ou como integrantes de organizações terroristas. Assim, Segundo Dinis (2005), a Internet passou a ser considerada um novo "Teatro de Guerra", conforme destacou o General Loureiro dos Santos durante conferência do Curso de Defesa Nacional de 2005/2006. Segundo ele, a Internet funciona também como uma “grande madrassa” da guerra santa, pois é por meio dela que muitos ensinamentos e comandos de operações terroristas são disseminados.

As ameaças à segurança da informação têm como propósito desencadear incidentes capazes de provocar danos a sistemas de informação ou às entidades que os utilizam. Tais ameaças podem ser deliberadas ou acidentais e assumir naturezas físicas ou lógicas. A informação, por sua vez, encontra-se armazenada em suportes diversos, como edifícios, cofres de segurança e dispositivos eletrônicos — todos suscetíveis a ameaças físicas, sejam elas de origem natural (como terremotos, inundações ou incêndios) ou decorrentes de ações humanas (como incêndios criminosos, bombardeios, disseminação de gases tóxicos ou sabotagens nas redes de abastecimento público) (Dinis, 2005).

No campo das ameaças lógicas, destacam-se práticas como o acesso e uso ilegítimo de informações, a interceptação de comunicações e outras ações criminosas, entre elas: fraude informática, falsidade informática, espionagem digital, sabotagem, danos a dados ou programas, e acessos não autorizados. Uma das formas mais comuns de obtenção ilícita de segredos militares ou comerciais é justamente a interceptação de comunicações. A conexão dos sistemas de informação à Internet elevou substancialmente o risco de vulnerabilidades, pois torna essas comunicações mais expostas à interceptação e ao desvio indevido de dados (Dinis, 2005).

2.3 PROTEÇÃO DE DADOS PESSOAIS

Dados pessoais são todas as informações relativas a uma pessoa física identificada ou identificável, independentemente de sua função social ou vínculo com a organização, podendo incluir clientes,

funcionários, parceiros, membros, apoiadores, contatos comerciais, servidores públicos ou qualquer outro indivíduo. Esses dados não precisam ser estritamente privados; mesmo informações de domínio público ou relacionadas à vida profissional podem ser consideradas dados pessoais. O critério essencial é a possibilidade de identificar uma pessoa com base nesses dados, isoladamente ou combinados com outras informações. Por outro lado, informações verdadeiramente anônimas não se enquadram como dados pessoais, exceto nos casos em que, por meio da combinação com outros elementos, ainda seja possível reidentificar alguém. Documentos em papel também são considerados dados pessoais apenas quando estiverem organizados ou destinados à digitalização (Sharma & Menon, 2020).

A proteção de dados consiste na utilização justa, adequada e responsável das informações pessoais, sendo uma dimensão concreta do direito fundamental à privacidade. Mais do que um princípio jurídico, trata-se de fomentar a confiança entre indivíduos e organizações. Isso implica tratar as pessoas de maneira justa, transparente e aberta, reconhecendo seu direito de controlar sua identidade e suas interações, ao mesmo tempo em que se busca equilibrar esse direito com os interesses coletivos e institucionais mais amplos. A proteção de dados, nesse sentido, contribui para uma cultura de respeito às liberdades individuais e para a legitimação das práticas organizacionais (Sharma & Menon, 2020).

O tratamento de dados compreende todas as operações realizadas com dados pessoais, incluindo a coleta, registro, armazenamento, utilização, análise, combinação, divulgação e eliminação. É essencial compreender o papel que uma organização exerce em relação aos dados que processa, pois isso define suas obrigações legais e operacionais. As responsabilidades variam de acordo com o papel assumido: se a organização atua como responsável pelo tratamento (controladora) ou como subcontratada (operadora). A principal questão para essa distinção é quem determina as finalidades e os meios do tratamento. Quando uma organização define os objetivos e os métodos do processamento, ela será considerada a controladora, independentemente da forma como é descrita em contratos ou acordos de prestação de serviço (Lin & Kifer, 2014).

O Regulamento Geral de Proteção de Dados (RGPD) é composto por um conjunto de regras voltadas à garantia da privacidade dos indivíduos no tratamento de seus dados pessoais e na sua circulação. Ao serem integradas ao funcionamento dos sistemas de informação, essas normas tornam-se operacionais e juridicamente aplicáveis nesse contexto. O modelo regulatório permite a análise das práticas organizacionais no uso de dados pessoais, oferecendo subsídios para mapear e aprimorar as capacidades de proteção das empresas, conforme os princípios e exigências do RGPD (Dibble, 2020).

Dentro do escopo do RGPD, a segurança do tratamento está condicionada ao cumprimento de um conjunto de requisitos e propriedades que assegurem a proteção contra o tratamento não autorizado ou ilícito, bem como contra a perda, destruição ou danificação acidental dos dados. Isso exige a adoção de medidas técnicas e organizacionais adequadas, sustentadas pelos princípios da licitude, lealdade e

transparência. Além disso, há a exigência de limitação das finalidades: os dados devem ser coletados com propósitos específicos, explícitos e legítimos, não podendo ser tratados de maneira incompatível com esses fins. Os dados também devem ser mantidos exatos e atualizados sempre que necessário, e conservados apenas pelo tempo estritamente necessário para as finalidades para as quais foram processados, garantindo assim a identificação dos titulares apenas durante o período permitido (Dibble, 2020).

2.4 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados (LGPD), também conhecida como Lei nº 13.709, foi instituída no Brasil em 14 de agosto de 2018, com a finalidade de regular a utilização, manejo, armazenamento, compartilhamento e salvaguarda de dados no país, aplicando-se tanto a indivíduos quanto a instituições, sejam elas do setor público ou privado (Brasil, 2018).

Após um período de adaptação de dois anos, a lei passou a ter plena validade posteriormente. O artigo 2º da LGPD define os princípios que orientam a aplicação do tratamento de dados pessoais no Brasil, incluindo: respeito pela privacidade; poder de autoinformação; liberdade de expressão, informação, comunicação e opinião; proteção da intimidade, honra e imagem; fomento ao desenvolvimento econômico, tecnológico e à inovação; promoção da livre iniciativa, concorrência e proteção dos consumidores; bem como a afirmação dos direitos humanos, desenvolvimento pessoal, dignidade e exercício da cidadania para todos os indivíduos (Brasil, 2018).

Além dos princípios fundamentais, a LGPD inclui dez diretrizes (finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas) que servem como pilares para a compreensão e implementação de condutas adequadas por parte dos envolvidos. Um aspecto a ser enfatizado é a ampla aplicação da LGPD, que promove mudanças em organizações tanto públicas quanto privadas. Assim, a coleta de dados pessoais e identificáveis só poderá ocorrer com a autorização do titular para acessar essas informações. Em casos de violação, sanções serão aplicadas conforme a natureza da infração (Brasil, 2018).

3 CONCLUSÃO

A segurança da informação e a proteção de dados pessoais se impõem, na atualidade, como dimensões imprescindíveis à sustentabilidade das organizações, à preservação da privacidade individual e à confiança nas interações digitais. A evolução da sociedade da informação, marcada pela interconectividade global e pela crescente digitalização de processos organizacionais, ampliou significativamente os riscos associados à integridade, à confidencialidade e à disponibilidade dos dados. Nesse sentido, o presente trabalho procurou demonstrar que a segurança da informação deixou de ser apenas uma responsabilidade técnica ou departamental e passou a integrar o núcleo estratégico da governança

corporativa.

No primeiro capítulo, foi possível compreender que os fundamentos da segurança da informação envolvem um processo contínuo, dinâmico e multidisciplinar, centrado na gestão de riscos, no desenvolvimento de políticas institucionais e na criação de uma cultura organizacional voltada à prevenção de ameaças. Como afirmam Mitnick e Simon (2003) e Wood (2004), a segurança não pode ser adquirida como um produto pronto, mas deve ser cultivada como uma prática organizacional estruturada. O chamado "triângulo da segurança", composto pelos princípios da confidencialidade, integridade e disponibilidade, conforme Andress (2014), fornece a base conceitual para compreender os objetivos essenciais da proteção da informação em ambientes corporativos e institucionais.

No segundo capítulo, o trabalho abordou as ameaças à segurança da informação, distinguindo entre ameaças físicas e lógicas, acidentais ou deliberadas, internas ou externas. A análise demonstrou que, além de vulnerabilidades técnicas, há ameaças geopolíticas e sociais que tornam o espaço cibernético um novo "teatro de guerra", como alertou Dinis (2005). A informação, nesse contexto, transforma-se não apenas em ativo estratégico, mas também em alvo de disputas entre Estados, organizações e indivíduos, sendo explorada em conflitos, ações de espionagem, fraudes e ataques cibernéticos. A Guerra do Golfo, por exemplo, é frequentemente citada como o marco inaugural da chamada Era da Informação.

O terceiro capítulo focou na proteção de dados pessoais, evidenciando a importância de se tratar esses dados com justiça, responsabilidade e transparência. Conforme Sharma e Menon (2020), os dados pessoais abrangem todas as informações que possam identificar um indivíduo, direta ou indiretamente, e seu tratamento impõe às organizações o dever de adotar mecanismos de proteção compatíveis com os princípios legais e éticos. A partir da promulgação da LGPD no Brasil e do RGPD na União Europeia, as empresas passaram a ser juridicamente responsáveis pela coleta, armazenamento, uso e descarte dos dados pessoais. Lin e Kifer (2014) destacam que compreender o papel da organização — se controladora ou operadora — é fundamental para garantir o cumprimento das obrigações legais. Já Dibble (2020) reforça que a segurança do tratamento exige a adoção de medidas técnicas e organizacionais capazes de evitar acessos não autorizados, perdas ou danos acidentais, e de garantir que os dados sejam utilizados somente para finalidades lícitas, legítimas e explícitas.

Ao longo do trabalho, demonstrou-se que as boas práticas em segurança da informação não se limitam à adoção de ferramentas tecnológicas, mas envolvem também a implementação de políticas claras, o treinamento constante de colaboradores, a realização de auditorias e testes de vulnerabilidades, e o comprometimento da alta gestão. Como afirma Peltier (2013), proteger os ativos digitais é também proteger o valor do negócio, a imagem institucional e a relação de confiança com stakeholders internos e externos. Nesse sentido, a segurança da informação se entrelaça com a governança organizacional, com a responsabilidade social e com os direitos fundamentais do indivíduo.

A análise das normativas internacionais e nacionais, como as diretrizes da OCDE, os regulamentos da União Europeia e os instrumentos legais brasileiros, mostrou que há um esforço global pela harmonização de práticas e pela criação de um ambiente jurídico que garanta a segurança no tratamento das informações. A atuação de entidades como a ISO, com normas como a ISO 17799:2000 e a ISO 15443, e de órgãos como a Autoridade Nacional de Segurança, também reforça a necessidade de padronização e conformidade na proteção dos sistemas e das redes.

Diante do exposto, conclui-se que a segurança da informação e a proteção de dados pessoais devem ser encaradas como dimensões fundamentais do funcionamento das organizações e da vida em sociedade. Em um mundo cada vez mais digital, globalizado e orientado por dados, negligenciar essas áreas significa expor-se a riscos operacionais, legais, éticos e reputacionais. Portanto, é imperativo que empresas, governos e indivíduos invistam em conhecimento, políticas e tecnologias que assegurem não apenas o cumprimento das normas, mas a efetiva proteção da dignidade, da liberdade e da integridade informacional dos cidadãos.

Acredita-se, por fim, que este trabalho contribui para o aprofundamento da reflexão sobre os desafios e os caminhos possíveis para fortalecer a cultura de segurança da informação nas organizações. Fica como sugestão para estudos futuros a análise da efetividade das políticas de segurança da informação em empresas de diferentes portes e setores, bem como a investigação sobre o impacto das novas tecnologias — como inteligência artificial e big data — sobre os direitos à privacidade e à autodeterminação informativa.

Enfim, ressalta-se a relevância da LGPD para proteger a privacidade dos cidadãos, porquanto num cenário em que os dados pessoais se caracterizam como um “bem”, combinar a falta de privacidade do cidadão com a comercialização de dados pessoais não-sensíveis ou sensíveis produzirá, progressivamente, a perda de autodeterminação dos indivíduos, logo, de sua liberdade, não se efetivando, consequentemente, a justiça.

Desse modo, o regulamento à proteção de dados demonstra a atuação estatal voltada a assegurar aos cidadãos a liberdade em um Estado Democrático de Direito (Oliveira; Silva, 2021).

REFERÊNCIAS

ANDRESS, Jason. The Basics of Information Security: Understanding the Fundamentals of InfoSec. 2. ed. Amsterdam: Syngress, 2014.

Brasil. (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Recuperado de http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

CONSELHO DA OCDE. Recomendações sobre a Política de Criptografia. Paris: OCDE, 1997.

CONSELHO DA UNIÃO EUROPEIA. Directiva 2002/58/CE, de 12 de Julho de 2002, relativa à privacidade e às comunicações eletrónicas.

CONSELHO DA UNIÃO EUROPEIA. Directiva 2006/24/CE, de 15 de Março de 2006, sobre conservação de dados gerados no contexto de comunicações eletrónicas.

CONSELHO DA UNIÃO EUROPEIA. Directiva 95/46/CE, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

DIBBLE, Caroline. GDPR: A Guide to the General Data Protection Regulation. London: IT Governance Publishing, 2020.

DINIS, José António Rodrigues. Guerra de Informação. 1. ed. Lisboa: Silabo, 2005.

DINIS, Pedro. Segurança da Informação e Cibercrime. Lisboa: Instituto da Defesa Nacional, 2005.

LIN, Jimmy; KIFER, Daniel. Data Management and Data Systems: Concepts and Applications. New York: Pearson, 2014.

LOPES, J. de Seabra. A proteção da privacidade e dos dados pessoais na sociedade da informação: tendências e desafios numa sociedade em transição. In: Estudos em homenagem ao Prof. Almeida Costa. Lisboa: Universidade Católica Portuguesa, s.d.

MITNICK, Kevin D.; SIMON, William L. The Art of Deception: Controlling the Human Element of Security. Indianapolis: Wiley Publishing, 2003.

Oliveira, C. G. B., & Silva, R. M. (2021). A Proteção dos Dados Pessoais Sensíveis: Questões Jurídicas e Éticas. In: Lima, Cíntia R.P. ANPD e LGPD: desafios e perspectivas. São Paulo: Almedina.

ONU – Organização das Nações Unidas. Declaração Universal dos Direitos Humanos, 1948.

PARLAMENTO EUROPEU. Regulamento (CE) nº 45/2001, relativo à proteção de dados nas instituições da União Europeia.

PELTIER, Thomas R. Information Security Risk Analysis. 3. ed. Boca Raton: Auerbach Publications, 2013.

PURDY, Grant. ISO 31000:2009 – Setting a New Standard for Risk Management. Risk Analysis, v. 30, n. 6, p. 881–886, 2010.

SHARMA, H.; MENON, S. Understanding Data Privacy and Protection. Delhi: Academic Press, 2020.

VAZ, Ana. Segurança da informação, proteção da privacidade e dos dados pessoais. Nação e Defesa, Lisboa, v. 117, p. 35-63, verão 2007. 3.ª série.

WOOD, Charles Cresson. Information Security Policies Made Easy. 12. ed. Baseline Software, 2004.