ARTIGOS

O PRINCÍPIO DA SEGURANÇA NA ERA DOS CIBERATAQUES: UMA ANÁLISE A PARTIR DO ESCOPO PROTETIVO DA LGPD

THE PRINCIPLE OF SECURITY IN THE ERA OF CYBER-ATTACKS: AN ANALYSIS BASED ON THE PROTECTIVE SCOPE OF THE LGPD

Gabriel Cemin Petry
Haide Maria Hupffer

RESUMO: O crescente número de ataques cibernéticos se tornou uma grande ameaça à segurança cibernética, causando sérios danos para Estados, organizações, indivíduos e sociedade. O artigo objetiva evidenciar o papel do princípio da segurança, esculpido no texto da LGPD, para proteção de dados pessoais, evitando consequentemente a ocorrência de incidentes de segurança dessa natureza. A pesquisa é qualitativa e exploratória, desenvolvida a partir do método dedutivo, com utilização de pesquisa bibliográfica e documental. Os resultados apontam que ataques cibernéticos são um problema recorrente no Brasil, sendo imprescindível, que sejam estabelecidas medidas técnicas e administrativas voltadas a garantir a funcionalidade de sistemas e proteção dos titulares de dados, garantindo-lhes seus direitos, desde a concepção até execução das atividades.

Palavras-chave: Princípio da Segurança. LGPD. Incidentes de Segurança. Proteção de Dados. Infraestruturas críticas.

ABSTRACT: The growing number of cyber-attacks has become a major threat to cyber security, causing serious harm to states, organizations, individuals and society. The article aims to highlight the role of the security principle, carved in the text of the LGPD, for the protection of personal data, consequently avoiding the occurrence of security incidents of this nature. The research is qualitative and exploratory, developed from the deductive method, with the use of bibliographical and documental research. The results indicate that cyber-attacks are a recurring problem in Brazil, and it is essential that technical and administrative measures are established to guarantee the functionality of systems and the protection of data subjects, guaranteeing their rights, from conception to execution of activities.

Keywords: Security Principle. LGPD. Security Incidents. Data Protection. Critical infrastructures.

1. INTRODUÇÃO

Com o avanço das novas tecnologias da informação e comunicação, na atualidade é experienciado um processo de digitalização e migração de ambientes analógicos para virtuais. Inúmeros são os benefícios do oferecimento de produtos e prestação de serviços no ambiente digital, o que é explorado até mesmo na prestação de serviços públicos; no entanto, a exposição em rede costuma atrair riscos que, embora invisíveis, possuem um potencial destrutivo alto: fala-se dos ciberataques e o seu impacto para as organizações, empresas e pessoas envolvidas.

No intuito de auxiliar na compreensão da terminologia técnica empregada, expõe-se brevemente alguns dos termos e significados que serão comentados no decurso do presente trabalho: (i) *malware*: programa (*software*) malicioso utilizado por *hackers* para danificar ou explorar vulnerabilidades de rede ou dispositivo; (ii) *hacker*: é o atacante da rede ou dispositivo invadido ou comprometido; (iii) *social engineering*: a engenharia social busca a manipulação da vítima para o acesso a dados e informações confidenciais; *phishing*: uma forma de engenharia social utilizada para furto de dados da vítima, costumeiramente realizada por contatos via e-mail; (iv) *ransomware*: um programa malicioso que pode bloquear dados, informações e até mesmo o dispositivo da vítima, sendo exigido resgates para liberação do dispositivo e dados criptografados; (v) *cyberwarfare*: o termo "guerra cibernética" diz respeito a prática de ataques a sistemas informacionais de países ou instituições com o fim de danificar ou destruir infraestruturas essenciais; *(vi) Critical infrastructures*: geralmente são os grandes alvos de ataques, pois, assim como cadeias de suprimento (*Supply Chains*) são responsáveis pela distribuição de produtos, as infraestruturas críticas são ativos e serviços essenciais para vida em sociedade (*v.g.* serviços de saúde, comunicação, transporte, energia etc.).

Os ataques cibernéticos podem ter como alvos pessoas, organizações políticas e sociais, empresas públicas e privadas, postos fiscais, tribunais, bases militares, autarquias e ministérios do Estado, variando conforme a motivação que ensejou o ataque, como: interrupção de sistemas e serviços essenciais, resgate de valores em troca de arquivos criptografados, extração de dados, repercussão política ou até mesmo a lesão física de pessoas. O instrumental empregado pelos *hackers* também é variado

e demanda atenção de profissionais da segurança da informação, contando com *malwares* e ardilosas técnicas de engenharia social.

O número de ataques, diante desse contexto de digitalização, é exponencial e a problemática é relevante em nível global. Neste sentido, de se destacar que desde 2020 o Brasil lidera rankings internacionais no quesito de detecção de ofensivas virtuais realizadas por meio de *phishing*, descortinando a quantidade de tentativas de ataques cibernéticos no país. A necessidade de proteção contra os recorrentes ataques cibernéticos é, de forma inegável, vital para a garantia do exercício de direitos fundamentais de pessoas físicas e jurídicas no Brasil, de forma que diversas normas legais consagram o dever de segurança para com o manejo de dados e informações de consumidores (Código de Defesa do Consumidor), usuários (Marco Civil da Internet) e titulares de dados pessoais submetidos a determinada atividade de tratamento de dados (Lei Geral de Proteção de Dados).

Ante ao panorama apresentado, a presente investigação se propõe a examinar a importância do princípio da segurança, consagrado no texto da Lei Geral de Proteção de Dados, nesse cenário em que ataques cibernéticos são uma realidade cada vez mais presente na vida em sociedade – sendo até mesmo esperados, de modo a demandar cautelas e precauções preventivas nas atividades internas das empresas e organizações responsáveis por realizar operações de tratamento de dados.

A pesquisa é de natureza exploratória e qualitativa com utilização do método dedutivo. Quanto aos procedimentos técnicos, utiliza-se de pesquisa bibliográfica, documental e abordagem de casos práticos. A análise é realizada por um viés crítico e dialético, acompanhada de revisão da literatura especializada das principais bases científicas nacionais e internacionais, análise do princípio da segurança para a proteção de dados no contexto da LGPD e legislações correlatas, assim como pelo exame das contribuições do Conselho Nacional de Justiça frente aos desafios impostos à segurança cibernética do Poder Judiciário.

O estudo se desenvolveu em três partes. O primeiro tópico contextualiza a problemática dos incidentes de segurança e ataques cibernéticos. Na sequência, expõe-se alguns dos principais *malwares* e técnicas de engenharia social que exploram vulnerabilidades e são utilizados para ataques cibernéticos. Por fim, são incorporadas reflexões sobre a fundamentalidade do princípio da segurança para a proteção de dados pessoais no contexto da LGPD, diante do constante risco (e expectativa) da ocorrência incidentes de segurança.

2. AMEAÇAS INVISÍVEIS: A RECORRENTE PROBLEMÁTICA DOS INCIDENTES DE SEGURANÇA E ATAQUES CIBERNÉTICOS NA ATUALIDADE

Ao tratar dos riscos à liberdade digital, Ulrich Beck apresenta um paradoxo implícito: quanto mais próximo do dano (ou da "*catástrofe*"), menos visível ele é (BECK, 2018, p. 185). Em que pese o trecho em comento trate do risco de um controle hegemônico global de dados, entende-se apropriado ao caso dos perigos cibernéticos, visto que, além de objetivarem vantagens patrimoniais sobre organizações, oferecem riscos à liberdade digital e autodeterminação informativa dos titulares de dados – riscos, então, imateriais. Neste sentido, ameaças cibernéticas, como o *ransomware,* viabilizam a ação de grupos criminosos em ações contra diversas organizações e empresas. Por exemplo, segundo o relatório "Como os executivos de empresas interpretam a ameaça do *ransomware*", produzido pela Kaspersky, 80% das organizações atingidas pelo ataque pagariam pelo resgate dos dados criptografados. O relatório ilustra, ainda, que 56% das empresas brasileiras afirmam terem sido vítimas de ataques de *ransomware*, assim como 54% das entrevistadas acreditam que no futuro eventualmente serão atingidas (KASPERSKY, 2022).

Para além de ataques voltados à obtenção de vantagens patrimoniais sobre a constrição de dados e interrupção da atividade de organizações ou empresas, os ciberataques tornaram-se verdadeiras armas de guerra (*cyberwarfare*). Ofensivas militares neste sentido foram empregadas, de forma "*hibrida*", isto é, concomitantemente a ataques por solo, pela Rússia em ataque ao satélite KA-SAT da empresa Viasat, por meio do *malware* chamado de "*AcidRain*" e, posteriormente, "*HermeticWiper*", apagando dados do sistema e desativandobas máquinas atacadas, com o intuito de desabilitar as capacidades militares da Ucrânia (MIT TECH REVIEW, 2022).

Neste caso, concentraram-se ataques cibernéticos em sites do governo Ucraniano e em setores críticos, como provedores de telecomunicação, energia elétrica, instituições financeiras e, entre outros, meios de comunicação. Segundo observa James A. Lewis (2022), o objetivo dessas "*Cyber Operations*" reside na degradação de vantagem informacional e de ativos intangíveis, como dados, comunicações e acesso à sistemas para garantir vantagem operacional. Por vezes, o objetivo é a obtenção de um efeito político: "interrompendo finanças, energia, transporte e serviços governamentais para sobrecarregar a tomada de decisões dos defensores e criar turbulência social" (LEWIS, 2022)[1]. Na atualidade, a guerra avança também sobre o ciberespaço.

1 No original: "*Cyber operations can also be used for political effect by disrupting finance, energy, transportation, and government services to overwhelm defenders' decision-making and create social turmoil*" In: (LEWIS, 2022).

Trata-se, pois, da inauguração de uma "*quinta dimensão da guerra*":

> A tecnologia se tornou fundamental em uma batalha, e a guerra adquiriu cinco dimensões: terra, água, ar, espaço e o ciberespaço — onde as batalhas pelas informações são travadas. [...] Essa dimensão bélica é baseada em operações psicológicas, guerras eletrônicas e operações computacionais. Mas, além das questões vistas anteriormente, por que ela é tão complicada e tão perigosa? Porque, antes de tudo, a guerra cibernética é silenciosa e anônima. Ela não tem um território definido. Os oponentes são difíceis de ser detectados e, por conseguinte, a reação se torna extremamente complicada. Baseando-se no desenvolvimento tecnológico, na descoberta de vulnerabilidades e exploração das falhas e psicologia humanas, a quinta dimensão da guerra exige a inteligência e o preparo (BRANQUINHO e BRANQUINHO, 2021, p. 51).

Observa-se uma revolução significativa nos conflitos armados contemporâneos, com a utilização de *Big Data* e sistemas de Inteligência Artificial que incluem a digitalização de armamentos e canais de comunicação, aquisição de dados significativos, ações preventivas ou sabotagem no ciberespaço e inteligência baseada em imagens de satélite. As ações técnicas ofensivas passam a incluir o ciberespaço para atos sabotagem, espionagem e ciberterrorismo, com possibilidade de paralisar infraestruturas críticas que incluem ataques à administração pública, governos, comunicação, mercados financeiros, aeroportos, hospitais, sistemas de transportes, usinas nucleares, assim como a produção e fornecimento de energia, alimentos, água, matérias-primas, combustíveis ou destruição de instalações importantes. Qualquer interrupção, falha ou ação planejada pode trazer danos e riscos à segurança pública e com graves consequências a comunidade local e global. Como exemplo, a sabotagem de um software que altera prioridades, alvos e cronogramas pode interromper ou paralisar operações militares (GÓRKA, 2021, pp. 17-20).

Percebe-se que ciberataques podem ser fatais para empresas, organizações, pessoas e, inclusive, governos. Ataques de *ransomware* podem ser estrategicamente empregados para desestabilização geopolítica de um Estado, instaurando o caos e demonstrando a incapacidade de ação (e impotência) de empresas e organizações estatais diante desse tipo de evento (CANO, 2022). Atacantes com a pretensão de desestabilização estatal costumam ter como alvo a *Supply Chain* (cadeia de suprimento) de sua vítima e suas infraestruturas críticas: "todas aquelas atividades que, mesmo que não percebamos, são engrenagens sem as quais a grande máquina que é nosso país deixaria de funcionar ou o faria de forma precária" (BRANQUINHO e BRANQUINHO, 2021, p. 48). Em vista a probabilidade de ataques, segundo atenta Lewis, a preparação e fortalecimento de alvos prováveis revela-se medida notadamente importante para monitoramento e reação aos incidentes (LEWIS, 2022).

É possível citar, neste sentido, o incidente paradigmático ocorrido na Costa Rica em 2022, em que um ataque *ransomware* implicou no fechamento de plataformas alfandegarias e fiscais do país, assim como agências governamentais, provocando colapsos no fornecimento de energia em uma cidade e a desativação de alguns serviços digitais prestados pelo Ministério da Fazenda. Observe-se que um ataque *ransomware*, em suma, foi responsável por levar o governo costarriquenho a edição do Decreto Executivo n. 42.542/2022, que determinou estado de emergência nacional (CANO, 2022).

Constituem exemplos de infraestruturas críticas: o fornecimento água, distribuição e produção de alimentos, combustível, saúde e transporte público, serviços financeiros, e, entre outros, a distribuição de energia elétrica (BRANQUINHO e BRANQUINHO, 2021, p. 48). Não à toa, o setor de energia foi um dos alvos de ataques cibernéticos durante o período da pandemia de COVID-19 no Brasil (PEREIRA e NEVES, 2021, p. 74), fazendo com que a Agência Nacional de Energia Elétrica -ANEEL editasse a Resolução Normativa N° 964/2021, sobre a consolidação da política de segurança cibernética a ser adotada pelos agentes de energia elétrica (ANEEL, 2021).

Os incidentes de segurança podem ser categorizados como *cyber crime* (atos criminosos que podem envolver a invasão de dispositivos), *hacktivism* (convergência entre o processo de invasão e intenções ativistas), *cyberwarfare* (utilização do ciberespaço para ataques a capacidade de combate de adversários militares) e, entre outros, *cyber espionage* (que pode envolver ataques a companhias e instituição com o fim de adquirir vantagem corporativa ou não). De fato, diversos setores podem ser alvos de ataques cibernéticos, assim como variadas são as motivações do ataque, que podem, por exemplo, objetivar a morte, o acesso e interrupção de um sistema (isto é, a manipulação de permissões, troca de acessos, impedimento de acesso à informação ou à vítima), atrasos no fornecimento de um serviço (interferindo no sistema a fim de causar atrasos ou colapsos na prestação de serviços), extração de dados (acesso não autorizado a dados pessoais de usuários ou informações privadas), repercussões políticas (referindo-se a eventos de impacto político ou afetando líderes de governos) (AL-MHIQANI, 2018, pp. 500-501).

Marcelo Branquinho e Thiago Branquinho (2021, p. 88-99) listam uma série de incidentes graves que demonstram o potencial destrutivo de incidentes de segurança, que causaram danos patrimoniais e financeiros, ao meio ambiente e inclusive lesões físicas a pessoas. Cons-

tituem exemplos históricos mencionados pelos autores: (1) o incidente de segurança que gerou a explosão de oleoduto em Belingham (EUA), em 1999; (2) o ataque à estação de tratamento de resíduos em Maroochy (Austrália), em 2000; (3) o ataque ao satélite ROSAT (2008) (BRANQUINHO e BRANQUINHO, 2021, p. 88-99).

Em 2021, The Harris Poll (2022, p. 4) conduziu, em nome da NortonLifeLock, pesquisa com cerca de 10.003 adultos com mais de 18 anos em 10 países (Brasil, Austrália, França, Alemanha, Índia, Itália, Japão, Nova Zelândia, Reino Unido e Estados Unidos da América). A pesquisa resultou no "*2022 Cyber Safety Insights Report: Global Results*", o qual aponta o Brasil como um líder global no quesito de número de ciberataques, estando ao lado da Índia no ranking de países com adultos mais propensos a dizer que sofreram um ataque por vírus de computador ou dispositivo móvel (THE HARRIS POOL, 2022, p.4). O relatório ainda destaca que, no cenário global, "a prevalência contínua da vida virtual forneceu terreno fértil para cibercriminosos – mais de 415 milhões adultos em 10 países sofreram crimes cibernéticos nos últimos 12 meses" (traduziu-se)[2]. De fato, estar-se-á diante de uma verdadeira transformação digital nos mais diversos campos da vida social (economia, cultura, política, comunicações, relações de consumo etc.) que se amplificou com a pandemia de COVID-19 e a necessidade de isolamento físico (HOFFMANN-RIEM, 2021, p. 3-5), forçando um avanço de projetos de transição digital e fazendo com que o Poder Público, por exemplo, intensificasse esforços na digitalização de serviços públicos (WIMMER, 2021, pp. 127-128).

O sistema bancário vive um verdadeiro "tsunami tecnológico" com o desenvolvimento de estratégias da economia digital centradas no cliente, o que mudou radicalmente a relação banco-cliente, como bem registra Schiavi (2018). A digitalização de pagamentos passa a exigir sistemas sofisticados de segurança para o relacionamento neste novo contexto, com o desafio de atualizações nos sistemas de proteção de dados e de segurança das informações, novas condições de contratos, disponibilização segura de canais para informar e conscientizar o cliente sobre benefícios e riscos de movimentações financeiras eletrônicas. Por outro lado, a criminalidade digital evolui com a mesma rapidez e a cada dia a sociedade é surpreendida com sofisticadas ações criminosas, que forçam as instituições financeiras a ampliar e manter ferramentas e protocolos com vistas a propiciar a segurança da informação (SCHIAVI, 2018).

Incidentes de segurança nos mercados digitais podem restringir direitos dos usuários e causar danos materiais e imateriais de difícil reparação. Falhas na proteção de dados, negligências no gerenciamento de informações e eventos de exposição de dados atrelados a fins ilícitos e obscuros são cada vez mais frequentes e possuem potencial de ocasionar riscos severos, tanto para os usuários, empresas, governos, como para a sociedade no seu todo (REBOUÇAS, 2021, p. 181-184). A adoção de uma postura preventiva de incidentes, a preservação da privacidade do usuário, a construção de sistemas seguros em todo o ciclo de processamento da informação, com auditorias e verificações constantes e a priorização dos interesses e direitos dos usuários, são práticas responsáveis e medidas essenciais para mitigar riscos de ataques cibernéticos e incidentes de segurança (REBOUÇAS, 2021, p. 185-188).

O cenário pandêmico foi igualmente problemático no quesito de segurança cibernética, de modo que não apenas órgão públicos foram alvos de ataques cibernéticos, mas, igualmente, empresas que buscavam se adequar a essa nova realidade, por meio do trabalho remoto. Hackers, neste período, aproveitavam-se para tentar realizar furto de informações, técnicas de *phishing*, explorar novos domínios na web e promover os mais variados tipos de ataque (BRANQUINHO e BRANQUINHO, 2021, p. 101). No fim do ano de 2020, o Superior Tribunal de Justiça foi vítima de um ataque hacker que criptografou os dados existentes no sistema da Corte Superior (PEREIRA e NEVES, 2021, p. 75) constituindo um entre os numerosos exemplos de ataques cibernéticos dirigidos às Cortes e Tribunais brasileiros, testemunhados pela sociedade brasileira entre 2020 e 2022. Preparar-se contra incidentes de segurança tornou-se indispensável. Nesse sentido, a Resolução CNJ n. 396/2021, instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), reconhecendo que é imprescindível garantir a segurança cibernética do Poder Judiciário, de modo que se faz necessário abordar aspectos da segurança da informação – fazendo menção direta à adequação com a NBR ISO/IEC 27001:2013, que trata justamente do referencial técnico acerca da segurança da informação (CNJ, 2021a).

Sendo assim, é possível consignar que a ocorrência de ataques cibernéticos tem se tornado, dentro da conjuntura nacional e internacional (HOFFMANN-RIEM, 2021, p. 117), uma problemática séria e recorrente, da qual o despreparo, ignorância e até mesmo negligência podem ter consequências gravíssimas – para organizações, autarquias, empresas, Estados e pessoas. A seguir serão apresentadas algumas das técnicas empregadas em ataques cibernéticos.

2 No original: "*The continued prevalence of virtual life has provided fertile ground for cybercriminals – more than 415 million adults in 10 countries* experienced cybercrimes in the past 12 months*" (THE HARRIS POLL, 2022, p. 4).

3. INSTRUMENTOS AO DISPOR DO ATAQUANTE: A NECESSÁRIA ATENÇÃO AOS *MALWARES* E TECNICAS DE ENGENHARIA SOCIAL

Além do *ransomware*, existem diversos métodos e técnicas empregados para o cometimento de crimes informáticos, os quais atualizam-se e reinventam-se no decurso de tempo. Patrícia Peck Pinheiro (2021a, p. 82) esclarece que o *ransomware* trata-se de um *malware* malicioso que explora vulnerabilidades encontradas no sistema e desenha uma cadeia de ataques, bloqueando o acesso aos dados e normalmente exigindo um resgate para recuperação. Atenta a autora que, desde 2012, o crescimento do número de ataques de *ransomware* é exponencial, representando um aumento de 229% entre os anos de 2017 e 2018, razão pela qual a implementação de medidas de segurança (antes, durante e após o incidente) é imprescindível (PINHEIRO, 2021a, p. 82).

De forma sintética, Damásio de Jesus e José Antônio Milagre listam parte do ferramental utilizado por atacantes há algum tempo: a) *vírus*: genericamente uma espécie de *malware* que, quando capaz de se replicar na web, recebe o nome de *worm;* b) *trojan*: popularmente chamado de "*cavalo de troia*", na medida em que o *malware* é ocultado ou disfarçado como outro *software*; c) *sniffing*: captura de pacote de dados transmitidos em rede, podendo ser combinado com outras técnicas de invasão; d) *backdoor*: código malicioso que permite acesso facilitado ao sistema, viabilizando o escalonamento ou privilégio na invasão; e) ***s**pyware*: *software* voltado a coleta de informações e atividade de um dispositivo, posteriormente enviando os dados ao destinatário; f) *keylogging*: técnica utilizada para monitorar o que é remetido pela vítima por meio do uso do teclado (*keyboard*); g) *screenloggin*: realiza capturas da tela *(screenshots*) da vítima pra monitorar sua atividade e extrair informação; h) *rootkits: software* utilizado para corromper a atividade do sistema operacional de um dispositivo; i) *DoS* e *DDoS*: trata-se de ataque de negação de serviço (*Denial of Service*) e negação de serviço distribuída (*Distributed Denial of Service*), voltadas indisponibilizar a prestação de serviços por meio de sobrecargas, que podem ocorrer das mais variadas formas; j) *força bruta*: técnica automatizada para tentativa reiterada de combinações de senha, e; k) *DNS poisoning:* alteração de resolução no sistema de domínios de um serviço, direcionando um acesso para um site falso, criado pelo responsável pelo ataque (JESUS e MILAGRE, 2016, p. 35-41).

A segurança dos dados pode ser posta em xeque por *crackers* de senhas (*Softwares* voltados a adivinhar senhas, podendo prever em até 29 milissegundos senhas com até 7 caracteres), *eavesdropping* (registro de tráfego de dados em rede), *soulder surfing* (utilização de dispositivos para espionar a vítima), permanência de dados (recuperação de dados existentes no disco rígido) e *trashing* (coletar o "*lixo*" descartado pelas empresas e analisá-lo a fim de extrair informações) (BRANQUINHO e BRANQUINHO, 2021, p. 282-285). Técnicas de "*engenharia social*" também podem ser utilizadas por atacantes para persuadir as vítimas a transmitir informações secretas ou dados importantes.

Conforme a lição de Patrícia Peck Pinheiro:

> [...] engenharia social pode ser compreendida como um conjunto de práticas e ações aplicadas na busca de informações sigilosas ou de grande importância e valor, pertencentes a uma pessoa ou a uma empresa, de maneira que essas práticas utilizam a manipulação, a persuasão e a influência sobre o comportamento humano como estratégia de ataque.[...] Com isso em mente, é de primordial pertinência que a empresa se preocupe com a engenharia social, seja através da conscientização dos funcionários, seja por meio da criação de mecanismos que dificultem a quebra dos protocolos de acesso à informação pela via humana (PINHEIROa, 2021, p. 96).

Técnicas de engenharia social acabam por explorar o fator mais fraco do elo da segurança da informação: o denominado "*fator humano*". Quando não há treinamento ou educação sobre cibersegurança, atentam Marcelo Branquinho e Thiago Branquinho, os próprios colaboradores de uma organização podem se tornar uma ameaça potencial, eis que "os seres humanos podem cometer erros, introduzir vulnerabilidades no ambiente industrial e enfraquecer as medidas de monitoramento e proteção adquiridas" (BRANQUINHO e BRANQUINHO, 2021, p. 61). Alguns pontos explorados pelo atacante que se vale da engenharia social são: a) retribuição: necessidade de retribuir um favor que recebe; b) compromisso: pessoas tem a inclinação a agir de forma repetitiva em situações cotidianas; c) prova social: reproduzir comportamento do próximo quando se está em uma situação de dúvida; d) simpatia: vulnerabilidade diante de uma situação envolvendo familiar ou amigo; e) autoridade: o atendimento a requerimentos de uma autoridade; f) escassez: propensão em oportunidades que estão menos disponíveis (PINHEIRO, 2021a, p. 99).

A prática de *phishing* e *vishing* consistem em práticas comuns de engenharia social. A primeira trata-se de contatos (*v.g.* e-mails) mal-intencionados que, devido ao caráter inofensivo ou importante, levam a vítima a clicar em links enviados ou enviar informações ou documentos ao atacante (contendo variantes como *spear phishing* e *clone phishing*); a segunda (*voice phising* ou *vishing*), trata-se da prática de ligações telefônicas para vítima, adotando falsa identidade, a fim de angariar informações relevantes ou induzir suas ações (PINHEIRO, 2021a, p. 100). Por vezes a prática de *phishing* pode ser a "porta de entrada" para

um *malware* combinado, como foi o caso, em 2017, dos ataques do *ransomware* "Wannacry" – posteriormente otimizado na nova geração de *ransomware* "NotPetya", que, ao contrário do primeiro (que criptografava acesso aos arquivos), realiza o bloqueio de forma completa o acesso ao dispositivo afetado pelo ataque (BRANQUINHO e BRANQUINHO, 2021, p. 99). Segundo o relatório da Kapersky, em 2020 o Brasil recuperou a liderança global no quesito de deteções anti-*phishing*, permanecendo no topo do ranking inclusive em 2021, o que revela que se trata de um dos países do mundo com maior índice de tentativas de ataques por meio de *phishing*[3] (KULIKOVA e SHCHERBAKOVA, 2022).

4. A FUNDAMENTALIDADE DO PRINCÍPIO DA SEGURANÇA PARA PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DA LGPD

O desenvolvimento da digitalização e a utilização de ferramentas de *Big Data* e Inteligência Artificial demandam responsabilidade e especiais precauções no tocante a segurança cibernética – especialmente quando empregada em infraestruturas críticas (como aquelas que foram anteriormente exemplificadas), segundo adverte Wolfgang Hoffmann-Riem. Para o autor, é imprescindível assegurar a funcionalidade de sistemas e constantemente monitorá-los, eis que "os riscos vão muito além dos perigos específicos da lei de proteção de dados, talvez se devam ao fato de que o *hardware* e/ou *software* contém lacunas de segurança" (HOFFMANN-RIEM, 2021, p. 116). O avançar das novas tecnologias da informação e comunicação (TICs), essencialmente fruto da "*quarta revolução industrial*"[4], por exemplo, fez com que infraestruturas tecnológicas e digitais se tornassem indispensáveis tanto para o setor público quanto privado (LORÈ e MUSACCHIO, 2021, p. 82), de modo que, conforme advertem Filippo Lorè e Paolo Musacchio, "a segurança de dados não deve ser encarada como um fardo económico, mas sim como um bem indispensável, dado o aumento exponencial dos ataques cibernéticos nos últimos anos" (traduziu-se)[5].

Os principais focos jurídicos da segurança da informação são:

> a) estar em conformidade com as leis vigentes; b) proteger a empresa de riscos e contingências legais relacionados ao mau uso da informação, ao uso não autorizado, o vazamento de informação confidencial, danos a terceiros, crime e fraude eletrônica, invasão de privacidade etc.; c) atender aos preceitos da Constituição Federal, do Código Civil, do Código Penal, da Lei de Direitos Autorais, da Lei de Software (antipirataria), da Consolidação das Leis do Trabalho e outros dispositivos legais nacionais e internacionais; d) garantir que, na hipótese de investigação de um incidente, a empresa possa usar as provas coletadas, e que, de forma preventiva, possa praticar monitoramento, sem que isso gere riscos legais; e) garantir que os contratos estejam adequados no tocante às responsabilidades relacionadas aos níveis de serviço acordados e aos termos de confidencialidade exigidos; f) fazer com que o time de resposta a incidentes atue com segurança jurídica, ou seja, com legitimidade jurídica (PINHEIRO, 2021b, p. 78).

O "dever de segurança", consagrado no regime de proteção de dados por meio da LGPD, segundo pontuam Fabiano Menke e Guilherme Damasio, possui como antecedentes institutos jurídicos como o Código de Defesa do Consumidor (CDC) e o Marco Civil da Internet (MCI) (MENCKE e GOULART, 2021, p. 351), também tidos como *microssistemas* de proteção de dados, ao lado da Lei do Cadastro Positivo (LCP) e Lei de Acesso à Informação (LAI)[6]. Alguns dos diplomas legais suscitados chamam a atenção a critérios técnico-ocupacionais, como é o caso do MCI, por meio do Decreto n°. 8.771/2016, que, a teor do art. 13, assegura algumas medidas de segurança, como por exemplo: mecanismos de autenticação; controle estrito sobre acesso aos dados; inventário dos acessos de registro, e; uso de soluções de gestão dos registros (MENCKE e GOULART, 2021, p. 346).

O CDC, em seu art. 4°, inc. IV e V, estabelece como objetivo da Política Nacional das Relações de Consumo a educação e informação de fornecedores e consumidores, assim como a criação pelos fornecedores de qualidade e segurança dos produtos e serviços. Segundo Humberto Theodoro Júnior, o primeiro diz respeito à conscientização quanto a direitos e deveres nas relações de consumo; o segundo, compreende a garantia da utilização segura e adequada do produto ou serviço pelo consumidor (THEODORO JÚNIOR, 2021, p. 36).

3 Literalmente, segundo as autoras: "*Users living in Brazil made the most attempts to follow phishing links, with the Anti-Phishing protection triggered on devices belonging to 12.39% of users in this country. Brazil was also the top phishing target in 2020*" (KULIKOVA; SHCHERBAKOVA, 2022).

4 Para Schwab (2016, p. 19), a quarta revolução industrial é caracterizada "por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos e pela inteligência artificial e aprendizagem automática (ou aprendizado de máquina)".

5 No original: "*La sicurezza dei dati, infatti, non deve essere percepita, come un aggravio economico, bensì come un asset indispensabile, considerato l'aumento esponenziale degli attacchi informatici degli ultimi anni*" (LORÈ; MUSACCHIO, 2021, p. 82).

6 Segundo assevera Bruno Ricardo Bioni (2021, p. 270), sob a perspectiva do diálogo das fontes, a LGPD e outras leis podem servir de base conceitual uma para outra, se influenciando reciprocamente (Coerência-sistemática); complementam-se de forma coordenada com as anteriores (complementariedade-subsidiariedade), e; redefinem o escopo de aplicação e os parâmetros delas, do especial ao geral e do geral no especial (coordenação-adaptação sistêmica).

O Marco Civil da Internet estabelece, sequencialmente, como princípios atrelados à segurança da informação: proteção da privacidade (inc. II), proteção de dados (inc. III) e segurança e funcionalidade da rede (inc. V). O dever de informação está exposto no MCI em seu art. 7°, inc. VI, estabelecendo como garantia do usuário o direito à informações claras e completas constantes dos contratos de prestação de serviços, inclusive "com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade" e, no inc. VII, a disponibilização informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais.

Neste sentido, por pertinência ao dever informacional esculpido no CDC e no MCI, a lição de Fabiano Menke e Guilherme Damasio Goulart:

> O controle do risco também está relacionado com o provimento de informações pelo fornecedor do produto e do serviço. A informação deve ser transmitida de forma clara e ostensiva, sob pena de o dever não ser cumprido, como ocorre no caso em que as informações de segurança dadas pelo banco estão escondidas em vários níveis de links em seu site ou, até mesmo, não foram fornecidas. Ainda, nesse contexto, são comuns as situações em que o fornecedor dá instruções de uso de seus produtos ou serviços, visando evitar um comportamento descuidado do consumidor. Como consequência, nas situações de descumprimento das orientações pelo consumidor, ocorre a configuração de sua culpa exclusiva diante da ocorrência do dano. Isso significa que, além do dever de fornecer as informações, há, por outro lado, um dever de cuidado a ser observado pelo próprio consumidor ao utilizar serviços e produtos que possuam algum tipo de risco (MENCKE e GOULART, 2021, p. 352).

Daí a necessidade de uma ação coordenada "entre o setor público e o setor privado, no sentido de aperfeiçoar a política vigente de proteção ao consumidor digital e mitigar os riscos de exposição de dados pessoais", a fim de promover um ambiente digital seguro e confiável, bem como manter o ritmo de desenvolvimento da economia digital (REBOUÇAS, 2021, p. 185).

A LGPD, consoante seu art. 6º, estabelece como princípios: a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, não discriminação, responsabilização e prestação de contas e, entre eles, com enfoque especial, a precaução e segurança. Esses dois últimos, segundo Ruth e Teixeira, podem ser traduzidos na adoção de medidas técnicas e organizativas (como estabelecimento de políticas, treinamentos e medidas de conscientização) para evitar a ocorrência de incidentes de segurança a partir de um "*raio X*" dos processos de tratamento de dados da empresa, assim como seus riscos e vulnerabilidades (TEIXEIRA e GUERREIRO, 2022, p. 20). Ante ao refinamento das técnicas de invasão e recorrência de ataques cibernéticos, entende-se pertinente a advertência de Filippo Lorè e Paolo Musacchio, no sentido de que o termo conformidade (*compliance*) não coincide automaticamente com o termo segurança (*security*) (LORÈ; MUSACCHIO, 2021, p. 82), de forma que "não pode ser considerado suficiente o genérico respeito das normas em vigor para minimizar os riscos de violação" (traduziu-se)[7].

Filippo Lorè e Paolo Musacchi (2021, p. 82) reforçam a necessidade de atenção ao tripé que sustenta a segurança da informação: (i) disponibilidade; (ii) integridade, e; (iii) confidencialidade dos dados (LORÈ e MUSACCHIO, 2021, p. 82). É possível falar também em um quarto elemento que coexiste entre esse clássico tripé: a "*resiliência*", cujo cerne, segundo Menke e Goulart, é a capacidade de reestabelecimento das funcionalidades comprometidas após o erro ou incidente (MENCKE e GOULART, 2021, p. 354). Para Arturo Di Corinto a resiliência é "a capacidade de recomeçar depois de um choque, neste caso informático" (traduziu-se) [8] (DI CORINTO, 2022, pp. 31-37). Além de providências de gerenciamento de segurança e vulnerabilidade, devem ser adotadas medidas de "*Identity and Access management*" (gerenciamento de identidade e acesso – sigla em inglês IAM), "*Secure Content and Threat Management*" (gerenciamento de conteúdo e ameaças – sigla em inglês SCTM) (LORÈ e MUSACCHIO, 2021, p. 82).

Com efeito, além da observância aos ditames da legislação vigente, faz-se essencial observar as normas de padronização existentes, as quais auxiliam no preenchimento de lacunas técnicas. Cita-se algumas normas técnicas que cumprem esse papel: (i) ISO/IEC 27001:2013 (recomendações sobre Sistemas de Gestão de Segurança da Informação); (ii) ISO/IEC 27002:2013 (código de práticas para Gestão de Segurança da Informação); (iii) ISO/IEC 27035:2011 (gestão de incidentes de segurança da informação; (iv) ABNT NBR 15999-1:2007 (gestão de continuidade dos negócios); (v) ISO/DIS 31000:2008 (gestão de risco), e; (vi) ABNT ISO/IEC 2009 (gerenciamento de serviços) (PINHEIRO, 2021b, pp. 78-79).

Conforme aponta Patrícia Peck Pinheiro (2021a, p. 31-40), que pese cada organização, através do conhecimento do seu funcionamento próprio, possa estabelecer e aplicar a política de segurança da informação que melhor lhe sirva, existem medidas "*macroexistenciais*" que po-

7 No original: "*non può ritenersi sufficiente il generico rispetto delle norme in vigore per minimizzare il rischio di violazion*" (LORÈ; MUSACCHIO, 2021, p. 82).

8 No original: "*la capacità di ripartire dopo uno shock, inquesto caso informatico*" (DI CORINTO, 2022).

dem ser categorizadas como boas práticas em proteção de dados, tais como: (i) adotar políticas de segurança sólidas e implementar um Sistema de Gestão de Segurança da Informação (SGSI); (ii) definir e identificar os agentes responsáveis (consubstanciados na figura do controlador, operador e encarregado); (iii) assegurar acesso aos direitos do titular de dados (art. 17, 18, 19 e 20 da LGPD); (iv) adotar medidas de anonimização ou pseudoanonimização quando possível; (v) realizar Relatório de Impacto de Proteção de Dados (RIPD); (vi) estabelecer comitê especializado em proteção de dados e enfocar na figura do encarregado; (vii) atentar as particularidades dos processos de transferência de dados em nível nacional e internacional (PINHEIRO, 2021a, pp. 31-40).

O princípio da responsabilização e prestação de contas (ou princípio da *accountability*), esculpido no inc. X, do art. 6°, da LGPD, também é de acentuada relevância. Segundo leciona Bruno Ricardo Bioni, em seu quesito histórico (atinente a evolução normativa da LGPD[9]), o princípio harmoniza um raciocínio jurídico voltado à reparação e, ainda, à prevenção, de modo que: "deve haver uma demonstração de tais medidas, o que pode ser materializado mediante um maquinário precaucionário que foi gradualmente esculpido ao longo das mais de sete fases em quase dez anos de (in)evolução do texto legal" (BIONI, 2022, p. 52). Essa racionalidade que se extrai da interpretação do inc. X, do art. 6°, revela que "o grau de responsabilidade de uma atividade de tratamento de dados é correspondente ao nível de demonstração das medidas adotadas para o cumprimento das normas de proteção de dados" (BIONI, 2022, p. 77).

O princípio da segurança, em sua definição esculpida no inc. VII, do art. 6°, da LGPD, consiste na "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (BRASIL, 2018). Medidas técnicas e administrativas "*aptas*" consistem em conceito jurídico indeterminado – replicado no *caput* do art. 46 -, o qual, segundo Menke e Goulart, pode ser suprido na forma do §1º, do art. 46, da LGPD: através do estabelecimento de guias e parâmetros pela Autoridade Nacional de Proteção de Dados (ANPD) (MENCKE e GOULART, 2021, p. 357), em sua atribuição pedagógica, nos termos do inc. V, VI, XIII e XVIII, do art. 55-J, da LGPD.

Medidas neste sentido podem ser citadas, como o "Guia Orientativo: segurança da informação para agentes de tratamento de pequeno porte", abarcando uma série de medidas de segurança da informação voltadas aos agentes definidos no art. 2° da Resolução CD/ANPD n. 2/2022, tais como: i) medidas administrativas (políticas, gerenciamento de contratos, conscientização e treinamento; ii) medidas técnicas (gerenciamento de vulnerabilidades, controle de acessos, segurança da comunicação e dos dados armazenados); iii) medidas relacionadas ao uso de dispositivos móveis, e; iv) medidas relacionadas aos serviços em nuvem (ANPD, 2021). Outra interessante participação da ANPD nesse sentido foi na contribuição para a "Cartilha de Segurança para Internet. Fascículo: Vazamento de dados", desenvolvido pela Cert.br, Nic.br e Cgi.br, apresentando riscos e orientações no caso da ocorrência de vazamentos de dados (NIC.BR, 2021).

A instituição de estratégias dedicadas a implementação da LGPD e a segurança nas operações de tratamentos de dados e segurança da informação também se destaca. Neste sentido, vale a reprise da importância da contribuição do Conselho Nacional de Justiça diante dos desafios impostos à segurança cibernética do ecossistema digital do Poder Judiciário que instituiu, por exemplo, a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), por meio da Resolução CNJ n. 396/2021, que em seu art. 11 elenca uma série de medidas voltadas ao aumento do nível de segurança das infraestruturas críticas (CNJ, 2021a). A Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), instituída pela Resolução CNJ n. 370/2021, conta com guia estratégico para o período de 2021 – 2026, a fim de aprimorar a segurança e gestão dos dados, assim como implementação à LGPD, nos processos internos (CNJ, 2021b).

O Conselho Nacional de Justiça (2018), pela competência a ele atribuída de fiscalizar os serviços notariais e de registro, publicou em 31 de julho de 2018 o Provimento n. 74/18 com o objetivo de "instruir Cartórios e garantir a segurança sobre os serviços prestados por eles" (JABUR e MARTINELLI, 2021, p. 166). O Provimento n°. 74/18 estabelece padrões mínimos de segurança técnica e administrativa assentado nos três pilares clássicos da segurança da informação: disponibilidade, integridade, confidencialidade. Para atender ao disposto no Provimento, cada serventia deverá elaborar um plano estratégico para instituir um Sistema de Gestão de Segurança da Informação com a participação de todos os colaboradores, promovendo mapeamento de todos os processos e de todo portfólio de serviços, classificando-os por grau de risco, atendendo aos requisitos legais e as "obrigações contratuais e plano de contingência para continuidade dos serviços do ativo" (JABUR e MARTINELLI, 2021, p. 166).

Por seu turno, o Provimento n. 134, de 24 de agosto de 2022, trata particularmente de medidas que as serven-

9 Bioni (2022, p. 41-52) atenta ao mapeamento, de 2010 até 2019, de nove fases do texto normativo da LGPD. Houve, portanto, uma guinada no texto legislativo acerca da matéria de proteção de dados no que toca a criação de instrumentos pelos quais seria possível demonstrar a eficácia de salvaguardas e medidas de mitigação de risco voltadas a preservação da LGPD, tais como boas práticas, registros de atividade, a concepção do *privacy by desing* e no tocante a figura do encarregado.

tias extrajudiciais devem adotar em nível nacional para adequação à Lei Geral de Proteção de Dados Pessoais. Além das contribuições específicas para cada serventia (*i.e.,* Tabelionato de Notas, Registros de Imóveis etc.), em relação a segurança informacional, o Provimento dedica o Capítulo VII especialmente para tratar de medidas de segurança, técnicas e administrativas (art. 12 -15), assim como Capítulo VIII, que estabelece medidas de treinamento e capacitação de todos os envolvidos no tratamento dos dados pessoais (art. 16) (CNJ, 2022a).

Outra importante iniciativa do CNJ é a criação do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), instituído pela Portaria n. 172, de 25 de maio 2022, como apoio às ações de governança, educação, segurança cibernética e segurança da informação. Como órgão técnico para assuntos de segurança da informação e cibernéticos, o CPTRIC-PJ é composto pela Rede de Cooperação do Judiciário que integra representantes de Equipes de Tratamento e Resposta a Incidentes de Segurança Cibernética de todos os tribunais com a responsabilidade de criar um canal seguro de comunicação entre os integrantes da Rede para trocas de informações sobre segurança da informação, reportar ameaças e incidentes, disseminar boas práticas, divulgar possíveis ameaças e possíveis ações de defesa ou mitigação, além de "auxiliar, na medida do possível, com troca de informações, o órgão do Poder Judiciário que esteja sob ameaça ou ataque cibernético" (a teor do art. 4 e seus incisos) (CNJ, 2022b).

Com efeito, o Capítulo VII, Seção I (art. 46 – 49), da LGPD está dedicado a segurança e sigilo de dados. Suscintamente, além do parágrafo supracitado, o § 2º, do art. 46, estabelece expressamente que as medidas de segurança deverão ser tomadas em consideração "da fase de concepção do produto ou do serviço até a sua execução" e, a teor do *caput* do art. 47, as medidas de segurança devem ser observadas pelos agentes de tratamento mesmo após o término do tratamento (*cf.* art. 15 e 16 da LGPD). Isto é, o que se convencionou como *"Privacy by Design"* ou, como abordado na alínea b, do inc. I, do art. 12 do Provimento 134/2022, *"Security by Design"* (CNJ, 2022a), que, segundo Bruno Ricardo Bioni, de rigor implica "a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais" (BIONI, 2021, p. 171).

Cabe, sem dúvida, à organização implementar medidas de segurança e salvaguardas para ataques ou vazamentos de dados. Identifica-se que a análise dos fatores de segurança empregados pela organização se faz presente, ainda, na comunicação de ocorrência de incidente de segurança, conforme preceitua o inc. III (medidas técnicas e de segurança utilizadas) e VI (medidas adotadas para mitigar e reverter o prejuízo), do art. 48, da LGPD. Inclusive, a ANPD poderá exigir comprovação de que foram adotadas as medidas técnicas, durante o juízo de gravidade do incidente, conforme o comando do § 3º. Nesta esteira, pertinente reforçar que o art. 44 expressamente prevê a possibilidade de reparação de danos no caso de violação da segurança dos dados:

> Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano (BRASIL, 2018).

Não responderão pelos danos causados os agentes de tratamento que comprovadamente não realizaram o tratamento de dados ou, tendo-o realizado, não havendo violação ao texto da legislação ou, ainda, na hipótese de dano decorrente de culpa exclusiva do titular ou de terceiros. É o que prevê o art. 43 e incisos da LGPD. Salta, então, o seguinte questionamento: sendo o ataque hacker realizado por terceiro, estar-se ia diante de uma excludente de responsabilidade, de modo que, diante de sua suposta "*imprevisibilidade*" do evento, poder-se-ia aduzir se estar diante de caso fortuito externo?

Primeiro, deve-se investigar como ocorreu o acesso indevido e, por decorrência, o dano: a culpa pelo vazamento ou incidente de segurança, por vezes, pode decorrer de ato imprudente ou negligente do próprio usuário, ao revelar suas credenciais e senhas a terceiro, por exemplo (falta de cuidado no manejo do dispositivo e de seus dados); contudo, havendo violação por parte daquele a quem incumbia a proteção, ou seja, a falha no dever de segurança por conta de quem deveria assegurá-lo, estará esse incumbido da reparação pelos danos causados[10]. Segundo atenta Arnaldo Rizzardo, o mesmo ocorre com provedores de acesso e aplicação na internet, diante de caso de contaminação de computadores e equipamentos através de *malwares* invólucros a e-mails, que dentro de da organização são constantemente transmitidos: cabe

10 Arnaldo Rizzardo (2019, p. 934) assunta a responsabilização do usuário de sistema bancário online para conferir saldo, movimentar quantias e realizar aplicações bancárias, no caos de fornecimento das credenciais a terceiro. Entretanto, salienta que caso seja comprovado que o fato gerador do dano derivou de problema no sistema do banco, permitindo o acesso indevido, deverá esse repor as quantias indevidamente sacadas.

ao provedor a implementação de mecanismos de proteção e prevenção, estancando a transmissão maliciosa, conforme determina o MCI (RIZZARDO, 2019, p. 934).

Na lição de Arnaldo Rizzardo (2019, p. 70), o caso fortuito externo, assim como o interno, é *imprevisível* e *inevitável*, diferindo-se do segundo em razão de ser *estranho a atividade ou organização do negócio* (RIZZARDO, 2019, p. 70). No entanto, a LGPD, como visto, imputa ao responsável pelo tratamento de dados uma série de medidas e salvaguardas de segurança (art. 46 a 49), assim como a observância de diligências de boas práticas e governança de dados (art. 50 a 51), desde a concepção do produto ou serviço até a sua execução, independentemente da natureza do negócio, de modo a assemelhar-se ao fortuito interno – fazendo parte da atividade do fornecedor do produto ou serviço e exigindo desse a observância de cautelas e precauções em sua atividade.

Sobre o caso fortuito externo no caso de ataque cibernético, entendeu a 20ª Câmara Cível do Tribunal de Justiça do Estado de São Paulo, na oportunidade do julgamento da Apelação Cível de nº. 1000568-46.2021.8.26.0007, que a invasão de dispositivo ou sistema por ataque cibernético (com obtenção de dados pessoais de consumidores) consistiria em evento extraordinário e fortuito externo, praticado por terceiro estranho ao serviço prestado pela empresa ré (TARTUCE, 2022, p. 932). O precedente é examinado, e, sobre o quesito da reparação de danos decorrente da violação dos dados, atenta Flávio Tartuce:

> [...] entendo que o citado ataque pode ser enquadrado como evento interno, se a empresa não toma medidas para evitá-lo a gerar a sua eventual responsabilização civil. Feita esse importante nota prática, a norma ainda estabelece, no seu art. 44, que o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: a) o modo pelo qual é realizado; b) o resultado e os riscos que razoavelmente dele se esperam; e c) as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Nos termos do seu parágrafo único, responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 da própria lei, der causa ao dano. A menção ao risco parece indicar mais uma vez um modelo de responsabilização sem culpa, diante da cláusula geral de responsabilidade objetiva prevista no art. 927, parágrafo único, segunda parte, do Código Civil (TARTUCE, 2022, p. 933).

Ademais, diante da recorrência do número de ataques (assim como a notoriedade dos incidentes e seus violentos impactos), é possível questionar ainda até que ponto pode-se falar na *imprevisibilidade do evento*. O dever de segurança, sendo um dos princípios norteadores das atividades de tratamentos de dados, objetiva salvaguardar o direito à autodeterminação informativa do titular de dados, apresentando acentuada importância diante do panorama de crescimento exponencial do número de incidentes de segurança e ciberataques em âmbito nacional e internacional. Por outro lado, é pertinente referir que cumpre a autodeterminação informativa seu papel como fundamento da LGPD, estando atrelada a outros direitos do titular, notadamente personalíssimos, como a sua liberdade e privacidade, de modo que, segundo atenta Wolfgang Hoffmann-Riem (2021, p. 73), concretiza a proteção da dignidade da pessoa humana neste contexto de irrefreável digitalização.

Com efeito, o processamento e a análise de dados tornam possível, além do acesso e interpretação de informações privadas, a viabilidade de previsão comportamental do indivíduo ou grupo de indivíduos analisados, potencializando a violação de sua privacidade. Deste modo, conforme aponta Arturo Di Corinto (2022, p. 33), a questão da segurança é determinante para a autodeterminação informativa do titular de dados, na medida em que "num mundo digital digitalizam-se os dados que identificam os nossos comportamentos; se falharmos em proteger esses dados digitais, falhamos em proteger nosso comportamento"[11]. Para o autor, nesse contexto digitalizado, a privacidade e segurança cibernética são precondições para o exercício de direitos fundamentais, como liberdade de expressão, movimento, associação e, entre outros, a garantia de igualdade (DI CORINTO, 2022, p. 34).

CONSIDERAÇÕES FINAIS

Ataques de hackers a dispositivos e sistemas informacionais de pessoas, empresas, organizações, tribunais e até mesmo autarquias estatais podem ter os mais diversos objetivos e motivações, assim como podem ocorrer das mais variadas formas. O instrumental pelo qual se vale o atacante é vasto e desafia os profissionais da segurança da informação, na medida em que constantemente se reinventa – aproveitando brechas e vulnerabilidades que eventualmente são constatadas. Nada obstante, pode o atacante valer-se de técnicas de engenharia social, explorando o fator humano para fisgar aquele que, destreinado, é o elo mais fraco da segurança da informação.

11 No original: "*in un mondo digitale i dati che identificano inostri comportamenti sono digitalizzati; se non riusciamo a tutelare questi dati digitali, non riusciamoa tutelare i nostri comportamenti*" (DI CORINTO, 2022, p. 33).

O catastrófico impacto que um ataque cibernético pode ter é inegável. Ao longo da presente investigação foram apresentados exemplos históricos de ataques que causaram muito mais do que prejuízos financeiros, mas, concomitantemente, a interrupção a serviços públicos essenciais, danos ao meio ambiente e igualmente lesões físicas a pessoas. *Supply Chains* e infraestruturas críticas, dada a sua essencialidade para sociedade, costumam ser alvos significativos para atacantes e, uma vez comprometidos, os resultados podem ser irreversíveis. Com efeito, a letalidade de ataques cibernéticos é tanta que atualmente consistem em perigosas estratégias de guerra (*Cyber Operations*) voltadas a degradação de vantagens informacionais e desestabilização política do alvo.

O fato é que, de forma paralela a impetuosa marcha de digitalização das coisas, vivemos na *era dos ciberataques*: onde incidentes de segurança dessa natureza e ataques cibernéticos são um problema vital e recorrente, de importância nacional e internacional. Neste cenário, o número de ataques cresce exponencialmente e lastimavelmente o Brasil revela-se como um recorrente alvo à nível global, razão pela qual a normativas atreladas a segurança da informação são cada vez mais presentes. A recorrência de ataques põe em xeque a imprevisibilidade deste tipo de evento, de forma que a deliberada ignorância acerca dos riscos de um ataque pode equivaler a um ato de negligência ou imprudência.

Com efeito, a operação de tratamento de dados (seja em âmbito público ou privado) atraí os efeitos normativos da LGPD, de modo que se faz imperiosa a atenção ao arcabouço principiológico da Lei. Nessa conjuntura, entre os princípios da legislação suscitada, entende-se que se sobressai o princípio da segurança – com medidas complementares presentes em institutos jurídicos como o CDC e o MCI – na medida em que se revela como condicionante para um seguro e adequado tratamento de dados, assim como para que efetivamente possa o titular dos dados pessoais exercer seus direitos e, em suma, sua autodeterminação informativa.

Em que pese a abstração constante no termo "medidas técnicas e administrativas '*aptas*' a proteger os dados pessoais", a leitura e interpretação do princípio não deve se dar de forma isolada, mas conjuntamente com os diplomas legais pertinentes, como Código Civil, MCI, CDC, LAI, entre outros. Nada obstante, deve-se atentar às normas de padronização existentes e ao estabelecimento de parâmetros de segurança por entidades competentes, como constitui exemplo os guias orientativos da ANPD e, também, as Resoluções emanadas pelo CNJ, que, a título de exemplo, inauguram medidas voltadas ao aumento do nível de segurança de infraestruturas críticas no Poder Judiciário.

Para além do título de conformidade com os *standards* da lei, são bem-vindas medidas e boas práticas voltadas a guarnecer os pressupostos de disponibilidade, integridade e confidencialidade dos dados, assim como a capacidade de resiliência da organização submetida a ataque cibernético. Destacam-se, neste sentido, treinamento de colaboradores, gerenciamento de vulnerabilidades, identidade e acessos e, através de um criterioso olhar interno das atividades, um gerenciamento do conteúdo e dos possíveis riscos e ameaças.

Os deveres de segurança imputados pela LGPD aos responsáveis pelas operações de tratamento de dados devem ser observados pelos agentes de tratamento desde a concepção até a completa execução da operação, de modo que, nos processos internos da atividade exercida, caberá a observância das cautelas e precauções pertinentes, sob pena de responsabilização pelos danos decorrentes da violação de segurança.

REFERÊNCIAS

AL-MHIQANI, Mohammed Nasser et al. Cyber-security incidents: a review cases in cyber-physical systems. **(IJACSA) International Journal of Advanced Computer Science and Applications**, v. 9, n. 1, p. 500-501, 2008. Disponível em: http://dx.doi.org/10.14569/IJACSA.2018.090169. Acesso em: 6 mar. 2023

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA (ANEEL). **Resolução Normativa n. 964/2021**. Dispõe sobre a política de segurança cibernética a ser adotada pelos agentes do setor de energia elétrica. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-normativa-aneel-n-964-de-14-de-dezembro-%20de-2021-369359262. Acesso em: 10 fev. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia orientativo: segurança da informação para agentes de tratamento de pequeno porte**: versão 1.0. Brasília: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em: 13 dez. 2022.

BECK, Ulrich. **A metamorfose do mundo**: novos conceitos para uma nova realidade. Tradução Maria Luiza X. de A. Borges. Rio de Janeiro: Zahar, 2018.

BRANQUINHO, Thiago; BRANQUINHO Marcelo. **Segurança cibernética industrial**. Rio de Janeiro: Alta Books, 2021.

BIONI, Bruno Ricardo. **Regulação e proteção de dados pessoais:** o princípio da *accountability***.** Rio de Janeiro: Forense, 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: A função e os limites do consentimento. 3. ed. Rio de Janeiro: Forense, 2021.

BRASIL. Presidência da República. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais

(LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 dez. 2022.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Provimento n. 74 de 31 de julho de 2018**. Dispõe sobre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de

registro do Brasil e dá outras providências. Disponível em: https://atos.cnj.jus.br/files/provimento/provimento_74_31072018_01082018113730.pdfAcesso em: 16 maio 2023.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução n. 396 de 7 de junho de 2021.** Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). 2021a. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3975. Acesso em: 1º fev. 2023.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Guia da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) 2021-2026**: versão 1.1. Brasília: CNJ, 2021b. Disponível em: https://atos.cnj.jus.br/files/compilado184145202110266178 4be9efedd.pdf. Acesso em: 20 jan. 2023.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Provimento n. 134, de 24 de agosto de 2022**. Estabelece medidas a serem adotadas pelas serventias extrajudiciais em âmbito nacional para o processo de adequação à Lei Geral de Proteção de Dados Pessoais. Brasília: CNJ, 2022a. Disponível em: https://atos.cnj.jus.br/files/original141307202208256307837 3a0892.pdf Acesso em: 16 maio 2023.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Portaria n. 172 de 25 de maio de 2022**. Brasília: CNJ, 2022b. Disponível em: https://atos.cnj.jus.br/atos/detalhar/4559 Acesso em: 26 fev. 2023.

CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Provimento n. 134, de 24 de agosto de 2022**. Estabelece medidas a serem adotadas pelas serventias extrajudiciais em âmbito nacional para o processo de adequação à Lei Geral de Proteção de Dados Pessoais. Brasília: CNJ, 2022b. Disponível em: https://atos.cnj.jus.br/files/original141307202208256307837 3a0892.pdf. Acesso em: 16 maio 2023.

CANO M., Jeimy J. El ransomware: una estrategia de desestabilización geopolítica. El Caso de Costa Rica. **Global strategy report**, n. 15, 2022. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=8473340. Acesso em: 6 fev. 2023.

DI CORINTO, A. Data commons: privacy e cybersecurity sono diritti umani fondamentali. **Rivista italiana di informatica e diritto**, v. 4, n. 1, p. 31-37, 16 mar. 2022, p. 33. Disponível em: https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/92. Acesso em: 28 jan. 2023.

GÓRKA, Marek. Współczesne zagrożenia cybernetyczne na przykładzie zjawiska cyberwojny: Analiza teoretyczna. **Acta Politica Polonica**, v. 1, n. 51, p. 5-21, 2021, p. 17-20. Disponível em: www.wnus.edu.pl/ap. DOI: 10.18276/ap.2021.51-01. Acesso em: 26 fev. 2023.

HOFFMANN-RIEM, Wolfgang**. Teoria geral do direito digital:** transformação digital: desafios para o Direito. Rio de Janeiro: Forense, 2021.

JABUR, Mirian Aparecida Esquárcio; MARTIMELLI, Anielle Eisenwiener. A influência da segurança da informação no Provimento n. 74 e na LGPD. *In*. TEIXEIRA, Tarcisio et al. (Coord.). **LGPD e cartórios**: implementação e questões práticas. São Paulo: Saraiva, 2021, p. 162-169.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de crimes informáticos.** São Paulo: Saraiva, 2016.

KASPERSKY. Ransomware: caso haja novo ataque, 80% das empresas no Brasil pagariam resgate. **Kapersky daily**, 19 mai. 2022. Disponível em:<https://www.kaspersky.com.br/blog/80-das-empresas-pagariam-resgate/19416/>. Acesso: 7 fev. 2023.

KULIKOVA, Tatyana; SHCHERBAKOVA, Tatyana. Spam and phishing in 2021. Spam and phishing reports. **Securelist by Kaspersky**, 9 fev. 2022. Disponível em: https://securelist.com/spam-and-phishing-in-2021/105713/. Acesso em: 20 fev. 2023.

LEWIS, James A. Cyber War and Ukraine. **Center For Strategic & International Studies (CSIS).** Report. June 16, 2022. Disponível em: https://www.csis.org/analysis/cyber-war-and-ukraine. Acesso em: 06 mar. 2023.

LORÈ, Filippo; MUSACCHIO, Paolo. Cybersecurity e protezione dei dati personali ai tempi dell'accountability: verso un cambio di prospettiva? **Rivista scientifica trimestrale di diritto amministrativo,** n. 1, p. 65-90, 2021. Disponível em: http://amministrativamente.com/index.php/formez/article/view/13201/11916. Acesso em: 20 fev. 2023.

MENKE, Fabiano; GOULART, Guilherme Damasio. Segurança da informação e vazamento de dados. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfganf; RODRIGUES JR., Otavio Luiz (Coord.); BIONI, Bruno (Coord. Exec.). **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, p. 339-360.

MIT TECHNOLOGY REVIEW. Uma hora antes da invasão da Ucrânia, hackers russos já haviam iniciado o ataque. **MIT**

Technology Review, 10 jun. 2022. Disponível em: https://mittechreview.com.br/uma-hora-antes-da-invasao-da-ucrania-hackers-russos-ja-haviam-iniciado-o-ataque/. Acesso em: 6 fev. 2023.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.BR). **Cartilha de Segurança para Internet**. Fascículo: Vazamento de dados. Brasília: ABNP, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes. Acesso em: 13 dez. 2022.

PEREIRA, Nicholas de Lucas Bastos; NEVES, Lucas Miranda. Ransomeare e Phishing durante a pandemia de COVID-19. **Revista Tecnológica da Fatec Americana**, v. 9, n. 01, jan./jun. 2021. Disponível em: https://fatec.edu.br/revista/index.php/RTecFatecAM/article/view/256. Acesso em: 10 fev. 2023.

PINHEIRO, Patricia P. **Segurança digital:** proteção de dados nas empresas. São Paulo: Atlas, 2021a.

PINHEIRO, Patrícia Peck. **Direito digital.** 7. edição. São Paulo: Saraiva Educação 2021b.

REBOUÇAS, Marina de Siqueira Campos. Segurança do consumidor nos mercados digitais: considerações sobre uso e proteção de dados pessoais. **Revista Brasileira de Direito Público**, Belo Horizonte, ano 19, n. 72, p. 175-191, jan./mar. 2021.

RIZZARDO, Arnaldo. **Responsabilidade Civil**. 8. ed. Rio de Janeiro: Forense, 2019.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. Tradução Daniel Moreira. São Paulo: Edipro, 2016.

SCHIAVI, Pablo. Los servicios financieros a través de plataformas tecnológicas. **Revista Iberoamericana de Derecho Administrativo y Regulación Económica**, n. 20, mar. 2018. Disponível em: https://ijeditores.com/pop.php?option=articulo&Hash=eeac5424e67e88a263f2a5d2598d5061 Acesso em: 18 maio 2023.

TARTUCE, Flávio. **Responsabilidade civil**. Rio de Janeiro: Grupo GEN, 2022.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD):** Comentada Artigo por Artigo. São Paulo: Saraiva, 2022.

THE HARRIS POLL. **2022 Cyber Safety Insights Report. 2022**. Disponível em: https://www.nortonlifelock.com/us/en/newsroom/press-kits/2022-norton-cyber-safetyinsights-report-special-release-online-creeping/. Acesso em: 8 jan. 2023.

THEODORO JÚNIOR, Humberto. **Direitos do Consumidor**. 10. ed. Rio de Janeiro: Forense, 2021.

WIMMER, Mirian. Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia. **Revista Brasileira de Políticas Públicas**, v. 11, n. 1, abr. 2021. Disponível em: https://doi.org/10.5102/rbpp.v11i1.7136. Acesso em: 20 jan. 2023.

Gabriel Cemin Petry
Bolsista do CNPq. Graduando em Direito pela Universidade Feevale. Integrante do Grupo de Pesquisa CNPq/Feevale: Direito e Desenvolvimento. Integrante do Projeto de Pesquisa CNPq/Feevale: Inteligência Artificial para um Futuro Sustentável: Desafios Jurídicos e Éticos.

Haide Maria Hupffer
Pós-Doutora e Doutora em Direito pela UNISINOS. Pesquisadora no Programa de Pós-Graduação em Qualidade Ambiental e no Curso de Direito da Universidade Feevale. Líder do Grupo de Pesquisa CNPq/Feevale Direito e Desenvolvimento. Líder do Projeto de Pesquisa FAPERGS: Inteligência Artificial e Sociedade de Algoritmos: regulação, riscos discriminatórios, governança e responsabilidades.