ARTIGO

CIBERSEGURANÇA, COMPLIANCE DIGITAL E CUSTO REPUTACIONAL

POR

Flúvio Cardinelle Oliveira Garcia
fluvio.fcog@pf.gov.br | fluvio.garcia@pucpr.br

Num mundo global e hiperconectado onde se estima que os custos decorrentes de atividades espúrias on-line serão de US$ 10,5 trilhões anualmente[1] em 2025 e que o Brasil figura como líder do *ranking* de ataques DDoS[2] na América Latina pelo 10º ano consecutivo, segundo no top 5 mundiais,[3] além de ser considerado o

1 MORGAN, Steve. Cybercrime to cost the world $10,5 trillion annually by 2025. Cybercrime Magazine, nov. 13, 2020. Disponível em: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/. Acesso em: 15 abr. 2024.

2 Um ataque DDoS (Distributed Denial of Service) é uma tentativa maliciosa de tornar um serviço on-line indisponível, sobrecarregando-o com um grande volume de tráfego de internet. Nesse tipo de ataque, os computadores de diversos dispositivos comprometidos, conhecidos como bots ou "zumbis", são coordenados por um atacante para enviar tráfego para o alvo simultaneamente. Isso sobrecarrega os recursos do sistema, como largura de banda, capacidade de processamento ou memória, impedindo que os usuários legítimos acessem o serviço. Os ataques DDoS podem causar interrupções graves em serviços on-line, como sites, servidores de jogos, serviços em nuvem e aplicativos web. Eles são frequentemente usados por motivos diversos, incluindo extorsão, protestos políticos, sabotagem ou simplesmente para causar interrupções e danos.

3 MARIN, Jorge. Brasil é líder do ranking de ataques DDoS na América Latina pela 10ª vez; entenda. TECMUNDO, out. 2023. Disponível em: https://www.tecmundo.com.br/seguranca/272995-brasil-lider-ranking-ataques-ddos-america-latina-10-vez-entenda.htm. Acesso em: 15 abr. 2024.

segundo maior alvo de ciberataques do planeta,[4] a iniciativa dos Referenciais de Formação em Cibersegurança não é apenas inovadora e bem-vinda, mas necessária.

Dentre os eixos de formação considerados como referenciais para o curso de Cibersegurança, destaca-se o de Segurança Organizacional, o qual, conforme diretrizes da Sociedade Brasileira de Computação, "envolve a proteção da organização contra ameaças e gestão de risco para apoiar os objetivos da organização" e estabelece como competência a ser atingida "elaborar estratégias de governança de acordo com **regulamentações**, boas práticas e propósito do negócio"[5] (grifei).

Ao esquadrinhar as competências derivadas do eixo em questão, depara-se com conteúdos específicos que objetivam o conhecimento e a implementação de identificação de riscos de segurança, avaliação, análise e controle de riscos, governança e políticas de segurança, governança de privacidade, planejamento estratégico de cibersegurança, plano de resposta a incidentes, **leis, ética e conformidade de segurança,** dentre outros tantos.

Os grifos previamente feitos chamam a atenção para elementos que precisam nortear, rigorosamente, o planejamento, a implementação e a execução de toda e qualquer atividade a ser devolvida por um profissional de cibersegurança: o respeito às normas jurídicas (princípios e regras) vigentes no país.

É nesse contexto que o *compliance* digital tem lugar. Numa tradução literal, a palavra *compliance* advém do verbo to *comply*, do inglês cumprir, e significa estar em conformidade.[6] Trata-se de um conceito relacional, cujo escopo somente é conhecido em face do objeto com o qual se relaciona, afinal de contas, quem está em conformidade o está em relação a algo.[7] Sendo assim, o estado de conformidade a que se refere o *compliance* digital diz respeito ao cumprimento de leis, princípios, procedimentos, regras, regulamentos internos e externos, contratos e quaisquer outras espécies normativas, formais ou não, nacionais e internacionais, que permeiam e disciplinam as condutas que se desenvolvem no mundo digital.[8]

Faleiros Júnior,[9] acertadamente, afirma que o estudo do *compliance* está vinculado, obrigatoriamente, com os assuntos

4 R7 TECNOLOGIA E CIÊNCIA. Brasil é o 2º maior alvo mundial de ciberataques, revela estudo. out. 2021, atualizado em abr. 2024. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-2-maior-alvo-mundial-de-ciberataques-revela-estudo-27062022/. Acesso em: 15 abr. 2024.

5 SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. Referenciais de formação para o curso de Bacharelado em CiberSegurança. Porto Alegre: Sociedade Brasileira de Computação (SBC), 2023. 40p. DOI 10.5753/sbc.ref.2023.125. Disponível em: https://books-sol.sbc.org.br/index.php/sbc/catalog/book/125. Acesso em: 15 abr. 2024.

6 SAAVEDRA, Giovani Agostini; CRESPO, Liana I. A. Cunha. Compliance: origem e aspectos práticos. In: CRESPO, Marcelo Xavier de Freitas (coord.). Compliance no direito digital. São Paulo: Thomson Reuters Brasil, 2020 - (Coleção compliance; vol. 3), pp. 30-31.

7 No Brasil, o compliance tornou-se mais conhecido após a Lei nº 12.846, de 1º de agosto de 2013, também chamada de Lei Anticorrupção. Precipuamente, a ideia foi evitar condutas corruptivas e fraudulentas nas empresas. Depois, os programas de compliance foram estendidos para outras frentes.

8 Ibidem, pp. 30-31 e 37.

9 FALEIROS JÚNIOR, José Luiz de Moura. Notas introdutórias ao compliance digital. In: CAMARGO et al (coords.). Direito digital: novas teses jurídicas. vol. 2. 2ª ed. Rio de Janeiro: Lumen Juris, 2019, pp. 116-118.

de governança corporativa, gestão de risco, ética e moral, representado pela sigla GRC:

> O "G" representa Governança e relaciona-se a controle, supervisão e gestão de uma companhia, envolvendo análise, organizações, metas, processos e objetivos. O "R" trata dos riscos existentes, inerentes ao negócio e outros que possam ocorrer por fatores internos ou externos, envolvendo um trabalho preventivo de mapeamento para que condutas indesejadas não sejam praticadas. O "C" cuida do Compliance, que se liga [a] questões de diversas matérias e não só financeiras, jurídicas ou contáveis.

A importância do aspecto preventivo do *compliance* digital é potencializada num ambiente globalizado e competitivo onde segurança, transparência, qualidade e integridade são exigidos a todo tempo e compõem o denominado custo reputacional da empresa.[10]

O paralelismo existente entre os pilares de um programa efetivo de *compliance* e aqueles utilizados em sistemas de gerenciamento de risco na segurança da informação é evidente. Ambos pressupõem, em síntese: apoio da liderança, código de ética, políticas e procedimentos bem definidos, educação, comunicação e treinamento constantes, monitoramento e auditoria, análise e aplicação de medidas de correção, mapeamento de risco e, se cabível, *due diligence* de terceiros.[11]

O processo de concretização de programa de *compliance* digital é contínuo, precisa se adaptar e responder aos riscos decorrentes de fatores internos e externos da empresa. Não se trata apenas de respeito às leis, regras, regulamentos, normas e procedimentos. Mais do que isso, busca implantar uma verdadeira cultura de prevenção de ações antiéticas, amorais e ilegais a fim de resguardar e, preferencialmente, incrementar de modo positivo o custo reputacional da organização.

O alcance e a relevância do *compliance* digital têm se ampliado significativamente, sobretudo a partir de 2014, com a promulgação da Lei nº 12.965, de 23 de abril de 2014, mais conhecida como Marco Civil da Internet (MCI).[12] Considerada como uma espécie de Constituição da Internet,[13] o referido texto normativo

10 Custo reputacional é o prejuízo financeiro ou impacto negativo que uma empresa sofre devido a danos em sua reputação. Esses danos podem ser causados por uma série de fatores, como escândalos, má conduta corporativa, produtos defeituosos, práticas comerciais antiéticas, entre outros. O custo reputacional pode se manifestar de várias formas, incluindo perda de clientes, queda nas vendas, desvalorização da marca, litígios, multas e até mesmo penalidades regulatórias. Manter uma boa reputação é crucial para a sustentabilidade e sucesso a longo prazo de uma empresa.

11 SAAVEDRA, Giovani Agostini; CRESPO, Liana I. A. Cunha. Compliance: origem e aspectos práticos. In: CRESPO, Marcelo Xavier de Freitas (coord.). Compliance no direito digital. São Paulo: Thomson Reuters Brasil, 2020 - (Coleção compliance; vol. 3), pp. 37-41.

12 Por óbvio, antes de 2014 já existiam leis e regulamentações às quais os profissionais das mais diversas áreas de Tecnologias da Informação e Comunicação (TICs) estavam (e estão) sujeitos, como a Constituição Federal de 1988, o Código Penal de 1940 e as leis especiais sobre direitos autorais (Lei nº 9.610/1998) e de propriedade industrial (Lei nº 9.279/1996), o Código Civil de 2002, o Código de Defesa do Consumidor (Lei nº 8.078/1990), a Lei de Acesso à Informação (Lei nº 12.527/2011), a Lei do E-Commerce (Decreto nº 7.962/2013), as normas ISO/IEC, dentre outras tantas. Contudo, foi a partir da regulamentação da internet no Brasil, por meio da Lei nº 12.965/2014 e do Decreto nº 8.771/2016, e da proteção legal e específica de dados pessoais, pela Lei nº 13.709/2018, que o compliance digital ganhou maior vulto no país.

13 GUERRA FILHO, Willis Santiago; CARNIO, Henrique Garbellini. Metodologia jurídica político-constitucional e o marco civil da internet: contribuição ao direito digital. In: MASSO, Fabiano Del; ABRUSIO, Juliano; FLORÊNCIO FILHO, Marco Aurélio. Marco civil da internet: Lei 12.965/2014. São Paulo: RT, 2014, p. 23. Não obstante reconhecerem que o MCI é chamado de Constituição da Internet, os autores salientam que, como legislação federal, deve ser utilizado e interpretado em conformidade com a Constituição Federal de 1988 (p. 26).

veio a estabelecer princípios, garantias, direitos e deveres para o uso da rede mundial de computadores no Brasil, determinando as diretrizes de atuação da União, dos Estados, do Distrito Federal e dos Municípios quanto à matéria (art. 1º, MCI).

O MCI entra em vigor quase 20 anos após a internet estar em uso no país. Sua mensagem principal: deixar claro que a rede mundial de computadores não pode ser considerada uma "terra sem lei". A premissa maior, que fica clara quando da leitura da lei, é que a utilização da internet deve ser feita de forma ética, respeitando-se a *novatio legis* que dispõe, expressamente, acerca de direitos e garantias dos usuários da rede, obrigações impostas aos provedores de conexão e de aplicações e sanções administrativas que poderão ser infligidas a todos aqueles que ofenderem as regulamentações ora positivadas.

Fundamentado no respeito à liberdade de expressão, no reconhecimento da escala mundial da rede, nos direitos humanos, na pluralidade e diversidade, na abertura e na colaboração, nas livres iniciativa e concorrência, na defesa do consumidor e na finalidade social da rede (art. 2º, MCI), o Marco Civil da Internet parece estar sedimentado em três pilares: a neutralidade da rede, a privacidade dos usuários e a liberdade de expressão.[14]

Dentre os direitos e garantias assegurados aos usuários encontram-se a inviolabilidade da intimidade e da vida privada, bem como do fluxo de suas comunicações pela internet e de suas comunicações privadas armazenadas; a não suspensão da conexão à rede, salvo por falta de pagamento do serviço; a manutenção da qualidade contratada da conexão; a publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; a acessibilidade; a observância às normas de proteção e defesa do consumidor; o direito à privacidade, à liberdade de expressão e à proteção de seus dados pessoais (art. 7º, MCI).

Mais do que resguardar as prerrogativas legais dos usuários de internet, há outras obrigações que precisam ser cumpridas pelos provedores de conexão e de aplicativos, como, por exemplo: tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação (neutralidade, art. 9º, MCI); fornecer às autoridades administrativas competentes o acesso aos dados cadastrais dos usuários (nome, prenome, estado civil, profissão, filiação, e endereço), independentemente de ordem judicial (art. 10, §3º, MCI c/c art. 11, Decreto nº 8.771/2016[15]); e guardar, pelo tempo determinado na lei, os registros de conexão e de acesso a aplicações, preservando seu sigilo e somente fornecendo-os às autoridades competentes mediante ordem judicial (arts. 10, 13 e 15, MCI).

14 Ibidem, p. 24.

15 O Decreto nº 8.771, de 11 de maio de 2016, tem por objetivo regulamentar a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

Consoante preconiza o artigo 17 do Decreto nº 8.771/2016, cabe à Agência Nacional de Telecomunicações (Anatel) a regulação, a fiscalização, a apuração de ofensas aos ditames do MCI e a aplicação das sanções administrativas. O descumprimento às normas sujeita o infrator, sem prejuízo das demais sanções cíveis (indenizações e reparações de danos, morais e/ou patrimoniais) e penais (penas privativas de liberdade, restritivas de direito e/ou multas), às sanções administrativas previstas no artigo 12 do MCI, quais sejam: advertência, multa simples de até 10% do faturamento do grupo econômico no Brasil no seu último exercício; multa diária limitada ao mesmo patamar da multa simples; e suspensão temporária ou proibição de exercício de atividades. É importante ressaltar que a conformidade com o Marco Civil da Internet é obrigatória mesmo para entidades jurídicas sediadas no exterior, desde que o serviço seja disponibilizado ao público brasileiro ou que pelo menos uma empresa do mesmo conglomerado possua uma sede no Brasil (art. 11, §3º, MCI).

A rigorosa observância aos ditames do Marco Civil da Internet é fundamental para assegurar a proteção dos direitos dos usuários on-line, promover a transparência e a equidade na rede. Obedecer a essa lei é crucial não apenas para garantir a segurança e a privacidade dos usuários, mas também para promover um ambiente digital mais ético e confiável, com chances mais efetivas de se combater ataques cibernéticos e, assim, aperfeiçoar a cibersegurança na rede mundial de computadores.

Não se trata apenas de conformidade legal, mas de medida essencial para proteger a reputação e a confiança do público na empresa, posto que, como se sabe, incidentes de segurança cibernética, como vazamento de dados ou violações de privacidade, podem acarretar sérios reflexos negativos para a imagem da organização. Sendo assim, o profissional de cibersegurança precisa estar atento para evitar ofensas ao MCI e adotar medidas preventivas concretas para garantir uma presença on-line sólida e confiável da empresa nos mais diversos ambientes digitais em que atua, preservando sua reputação, credibilidade e integridade no mercado.

Na mesma esteira normativa, a Lei nº 13.709, de 14 de agosto de 2018, denominada Lei Geral de Proteção de Dados Pessoais (LGPD), é reconhecida como um marco jurídico importantíssimo na consolidação do direito à proteção de dados pessoais no Brasil, hoje estampado em cláusula pétrea na Constituição Federal de 1988 (CF/88) como direito fundamental,[16] incluída pela Emenda Constitucional nº 115, de 2022.

Inspirada na *General Data Protection Regulation* (GDPR), publicada em 25 de maio de 2018, com força de lei, no âmbito da União Europeia, a LGPD brasileira sistematiza e estabelece, em seus 65 artigos, direitos para os titulares de dados, obrigações para os agentes de tratamento (controladores e operadores) e procedimentos documentais relativos à privacidade e à proteção de dados, digitais ou não,

16 CF/88, art. 5º, LXXIX: "é assegurado, nos termos da lei [LGPD], o direito à proteção dos dados pessoais, inclusive nos meios digitais".

como, por exemplo, a confecção de ROPA (*Records Of Processing Activities*), DPIA (*Data Protection Impact Assessment*), PIA (*Privacy Impact Assessment*) e LIA (*Legitimate Interest Assessment*), conforme se depreende da leitura dos artigos 5º, XVII, 10, §3º, 18, 30, 32, 37 e 38, da lei.

Os fundamentos que disciplinam a proteção de dados pessoais adotados pela LGPD assemelham-se àqueles já consagrados pelo MCI,[17] com especial distinção à autodeterminação informativa, vale dizer, ao poder e à capacidade de o indivíduo decidir se seus dados - digitais e/ou físicos - poderão ser tratados[18], de que forma e com qual finalidade. Como regra, basta que a operação de tratamento seja realizada no território nacional; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou que os dados pessoais objeto do tratamento tenham sido coletados no território nacional, para que haja a plena incidência dos rigores da LGPD (art. 3º, LGPD).[19]

Se a privacidade é um direito consagrado na CF/88 (art. 5º, X)[20], no MCI (arts. 3º, II, e 8º, 11, caput e §3º)[21] e na LGPD (arts. 1º, 2º, II e 17),[22] a proteção de dados é incontestavelmente um dos meios para se efetivar o referido direito, assegurando

17 LGPD, art. 2º. "A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais".

18 A LGPD, em seu art. 5º, X, define tratamento como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

19 Por força do art. 4º da LGPD, não se aplica a lei ao tratamento de dados pessoais: "I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei; III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

20 CF/88, art. 5º, X. "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

21 MCI, art. 3º, II. "A disciplina do uso da internet no Brasil tem os seguintes princípios: (...) II - proteção da privacidade;"; art. 8º. "A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet"; art. 11, caput, §3º. "Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros" e "Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações".

22 LGPD, art. 1º. "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"; art. 2º, II. "A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade;"; e art. 17. "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei".

ao titular, pessoa natural a quem se referem os dados pessoais que serão objeto de tratamento (art. 5º, V, LGPD), o amplo rol de prerrogativas listadas nos artigos de 18 a 22 do normativo. Dentre essas, destacam-se: ser informado sobre incidentes envolvendo seus dados; receber explicação e esclarecimentos sobre algoritmos e modelos que fazem uso de seus dados; acessar seus dados e obter cópia; solicitar a correção, alteração, anonimização, bloqueio, exclusão e/ou eliminação de dados; confirmar a existência de tratamento; revogar consentimento previamente concedido; e de pleitear portabilidade informacional.

Aos agentes de tratamento de dados, classificados como controladores e operadores,[23] a LGPD determina observar, dentre outras obrigações, as de resguardar os direitos dos titulares de dados; adotar medidas técnicas, administrativas e de gestão para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas que impliquem em tratamento inadequado ou ilegal (art. 46); indicar o controlador um encarregado para tratamento de dados (art. 41); obedecer aos princípios da finalidade, adequação, necessidade, livre acesso, preservação da qualidade dos dados, transparência, segurança (*privacy by default e privacy by design*), prevenção e não discriminação, responsabilização e prestação de contas (art. 6º);[24] e comunicar, com a devida urgência, à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares envolvidos a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (art. 48).

Além disso, incumbe-lhes tratar dados pessoais somente se presente ao menos uma das hipóteses legais autorizativas, a saber, o consentimento, o cumprimento de obrigação legal, a execução de políticas públicas, estudos por órgãos de pesquisa, execução de contrato, exercício regular de direito, proteção da vida, tutela da saúde, proteção do crédito e legítimo interesse (arts. 7º ao 14); garantir a segurança

23 Conforme art. 5º, incisos IX, VI e VII, o controlador e o operador são considerados agentes de tratamento de dados. O primeiro definido como "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais"; e o segundo, "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

24 LGPD, art. 6. "I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: 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; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas".

da informação (disponibilidade, integridade e confidencialidade) em relação aos dados pessoais (art. 47); elaboração de ROPA, DPIA, PIA e/ou LIA, nas hipóteses em que a lei exigir (artigos 5º, XVII, 10, §3º, 18, 30, 32, 37 e 38).[25]

Tal qual ocorre com os violadores do MCI, aqueles que transgredirem os preceitos da LGPD estarão sujeitos a diversas sanções administrativas que podem ser aplicadas pela ANPD, criada por força do artigo 55-A da LGPD, com autonomia técnica e decisória para, entremeio a outras relevantes atividades (art. 55-J, LGPD), fiscalizar e sancionar condutas, comissivas e omissivas, que atentem contra as normas de proteção de dados instituídas pela lei.

Dentre as sanções administrativas possíveis de serem aplicadas pela ANPD, sem prejuízos de outras punições administrativas, civis e/ou penais previstas em outras legislações (p.ex., MCI), estão: advertência; multa simples, de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício; multa diária; publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio e/ou eliminação dos dados pessoais; suspensão parcial do funcionamento do banco de dados e/ou do exercício da atividade de tratamento dos dados pessoais a que se refere a infração; e a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (art. 52, LGPD). O artigo 42 da LGPD é cristalino ao prever que os agentes de tratamento de dados (controladores e operadores) serão obrigados a reparar eventuais danos patrimoniais, morais, individuais ou coletivos, decorrentes de violação à legislação de proteção de dados pessoais, em razão de seu exercício de atividade de tratamento de dados.

Sob a perspectiva do *compliance* digital, importa salientar que a boa-fé e a cooperação do infrator, a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, a adoção de política de boas práticas e governança e a pronta adoção de medidas corretivas são parâmetros legais levados em consideração quando da aplicação de sanções pela ANPD, podendo resultar em um abrandamento significativo da penalidade (art. 52, §1º, II, VII a X, LGPD).

Eis aí, estreme de dúvidas, reflexos positivos e benefícios concretos reconhecidos pela legislação diante da implementação de políticas internas, controle, capacitação, treinamento e demais ações, protocolos e procedimentos de natureza preventiva visando à identificação precoce de irregularidades, à conformidade organizacional com os normativos vigentes e à minimização de responsabilidades.

Resta evidente a relação existente entre a LGPD e as atividades desenvolvi-

25 Para mais informações sobre os documentos citados (ROPA, DPIA, PIA e LIA), sugere-se a leitura do texto Risk assessments e relatório de impacto: ferramentas para avaliação de riscos em programas de compliance digital e de proteção de dados, de autoria de Marcelo Xavier de Freitas Crespo (In: CRESPO, Marcelo Xavier de Freitas (coord.). Compliance no direito digital. São Paulo: Thomson Reuters Brasil, 2020 - (Coleção compliance; vol. 3), pp.157-182.

das pelos profissionais de cibersegurança, sobretudo no que se refere à implementação de medidas adequadas para proteção de dados pessoais contra acessos não autorizados, vazamentos e outras ameaças cibernéticas.

A segurança da informação (conjunto de práticas, tecnologias e procedimentos projetados para proteger sistemas de informação contra ataques cibernéticos), a identificação e a gestão de riscos (avaliação de vulnerabilidades, ameaças e impactos potenciais sobre dados pessoais e sistemas de informação), a resposta a incidentes (implementação de planos de resposta e ações para mitigar danos e proteger os direitos e liberdades dos titulares dos dados) e a cultura de segurança (conscientização e educação sobre os riscos de segurança envolvendo todos os colaboradores e fornecedores da empresa) são pautas comuns e cruciais tanto à cibersegurança quanto à proteção e à privacidade de dados.

A desconformidade organizacional quanto às disposições da LGPD representa não apenas um risco financeiro direto, mas também pode ter um impacto duradouro e prejudicial em sua reputação, sobretudo diante da possibilidade de publicização da infração como sanção administrativa (art. 52, IV, LGPD). O custo reputacional da organização pode ser gravemente atingido pela perda de confiança dos clientes diante de eventual violação da privacidade de seus dados pessoais; pelos danos à imagem e à credibilidade da empresa, notadamente em tempos digitais onde as notícias se espalham rapidamente; pelo ajuizamento de ações judiciais reparatórias e indenizatórias diante de prejuízos causados aos titulares; e pelo impacto negativo nos relacionamentos comerciais (fornecedores, parceiros e outras partes interessadas).

A implementação de um efetivo *compliance* digital requer uma abordagem abrangente, não apenas para o atendimento de leis e regulamentos, mas também para estabelecer uma imagem ética e íntegra perante o mercado. Uma reputação positiva é essencial para se destacar no mercado competitivo atual, especialmente em ambientes digitais, onde as informações circulam com velocidade e uma má conduta pode resultar em danos irreparáveis à imagem e à credibilidade da empresa.

Para alcançar uma cultura de integridade, é necessário o comprometimento de toda a organização, desde a alta diretoria até os colaboradores e parceiros comerciais. Isso inclui o estabelecimento de políticas claras, treinamento constante e efetivo, e a criação de canais de comunicação abertos para denúncias, sugestões e *feedback*.

A mudança cultural é essencial e deve ser apoiada por iniciativas como treinamento, conscientização e orientação. Além disso, avaliações de risco regulares são indispensáveis para identificar vulnerabilidades e implementar medidas preventivas e corretivas.

O programa de *compliance*, por sua vez, deve ser visto como um processo contínuo e adaptativo, fundamental para garantir a integridade e o sucesso da empresa no ambiente digital e além dele.

E nesse contexto, a atuação proativa do profissional de cibersegurança se mostra fundamental.

Há muito mais a se dizer acerca de outras regulamentações, algumas em vigor, outras em discussão no Congresso Nacional, que envolvem assuntos tecnológicos de interesse da cibersegurança, como é o caso da Inteligência Artificial e da Internet das Coisas. Contudo, a importância dos temas impõe certo aprofundamento, o qual deixaremos para outra oportunidade.

Referências

1. BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. Proteção de Dados e Privacidade: do direito às novas tecnologias na sociedade da informação. Rio de Janeiro: Lumen Juris, 2018.
2. CAMARGO et al (coords.). Direito digital: novas teses jurídicas. vol. 2. 2ª ed. Rio de Janeiro: Lumen Juris, 2019.
3. CRESPO, Marcelo Xavier de Freitas (coord.). Compliance no direito digital. São Paulo: Thomson Reuters Brasil, 2020 - (Coleção compliance; vol. 3).
4. MARIN, Jorge. Brasil é líder do ranking de ataques DDoS na América Latina pela 10ª vez; entenda. TECMUNDO, out. 2023. Disponível em: https://www.tecmundo.com.br/seguranca/272995-brasil-lider-ranking-ataques-ddos-america-latina-10-vez-entenda.htm. Acesso em: 15 abr. 2024.
5. MASSO, Fabiano Del; ABRUSIO, Juliano; FLORÊNCIO FILHO, Marco Aurélio. Marco civil da internet: Lei 12.965/2014. São Paulo: RT, 2014.
6. MORGAN, Steve. Cybercrime to cost the world $10,5 trillion annually by 2025. Cybercrime Magazine, nov. 13, 2020. Disponível em: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/. Acesso em: 15 abr. 2024.
7. PIRONTI, Rodrigo. Lei Geral de Proteção de Dados: estudos sobre um novo cenário de governança corporativa. Belo Horizonte: Fórum, 2020.
8. PONTIFÍCIA UNIVERSIDADE CATÓLICA DO PARANÁ. CiberSegurança: bacharelado. Disponível em: https://www.pucpr.br/cursos-graduacao/ciberseguranca/. Acesso em: 15 abr. 2024.
9. R7 TECNOLOGIA E CIÊNCIA. Brasil é o 2º maior alvo mundial de ciberataques, revela estudo. out. 2021, atualizado em abr. 2024. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-2-maior-alvo-mundial-de-ciberataques-revela-estudo-27062022/. Acesso em: 15 abr. 2024.
10. SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. Referenciais de formação para o curso de Bacharelado em CiberSegurança. Porto Alegre: Sociedade Brasileira de Computação (SBC), 2023. 40p. DOI 10.5753/sbc.ref.2023.125. Disponível em: https://sol.sbc.org.br/livros/index.php/sbc/catalog/book/125. Acesso em: 15 abr. 2024.

FLÚVIO CARDINELLE OLIVEIRA GARCIA é Graduado em Ciências da Computação pela Universidade Católica de Brasília. Graduado em Direito pelo Centro Universitário de Brasília. Pós-graduado em Direito Eletrônico e Tecnologia da Informação pelo Centro Universitário da Grande Dourados. Mestre em Direito Processual Penal pela Pontifícia Universidade Católica de São Paulo. Doutor em Direito Penal Econômico pela Pontifícia Universidade Católica do Paraná. Pós-doutorado pela PUCPR. Delegado de Polícia Federal atualmente lotado na Superintendência da Polícia Federal no Paraná, sediada em Curitiba/PR. Desde 2002 tem atuado e se especializado na investigação de crimes de alta tecnologia praticados pela rede mundial de computadores.