A necessidade de segurança dos dados sensíveis no Sistema Processual Penal

Ives Nahama Gomes dos Santos[1]

Dhean Lucca Alves da Silva[2]

Resumo: Os dados sensíveis são dados que permitem reconhecer cada indivíduo. Estima-se que esses dados, nos casos de vazamento, por serem totalmente frágeis e individuais, podem prejudicar os indivíduos que eles retratam. Diante disso, no processo penal, esses dados podem prejudicar aqueles que estão envolvidos em suspeitas e em procedimentos. Nota-se, assim, que é necessário compreender como esses dados são protegidos e utilizados na atualidade no processo penal. Para isso, procede-se a uma ampla pesquisa teórica, utilizando a técnica de revisão de literatura, buscando compreender a suficiência dos instrumentos jurídicos nesse tema, como esses dados são tratados no processo penal e o que a falta de segurança no manuseio pode prejudicar.

Palavras-chave: Dados sensíveis. Processo penal. Segurança de dados.

Abstract: Sensitive data is data that allows us to recognize each individual. It's estimated that these data, in cases of leakage, being totally fragile and individual, can harm the individuals they portray. Therefore, in criminal proceedings, these data can harm those involved in

[1] Mestranda em Direito Constitucional Público pela Universidade Federal do Ceará (PPGD/UFC), com mobilidade acadêmica na Universidade Federal de Minas Gerais (UFMG). Coordenadora do Núcleo de Estudos em Ciências Criminais (NECC/UFC). Pesquisadora do Projeto Pesquisa Empírica em Direito - PROPED (UNIFOR). Pesquisadora do Grupo de Direito Penal Econômico e da Empresa (G.DPEE) da FGV/SP. Pesquisadora do grupo de estudos Dimensões do Conhecimento do Poder Judiciário da Escola Superior da Magistratura do Estado do Ceará (ESMEC). Especialista em Direito Penal Econômico pela Universidade de Coimbra e IBCCRIM. Advogada criminal com ênfase em criminalidade econômica e de empresa. Associada ao Instituto Brasileiro de Ciências Criminais - IBCCRIM. Associada ao Instituto do Nordeste de Direito Penal Econômico - INEDIPE. Desenvolve pesquisas e possui publicações nas áreas de Direito Penal, Direito Penal Econômico e Mercado de Capitais. Graduada em Direito pelo Centro Universitário 7 de Setembro. E-mail: ives-nahama@hotmail.com

[2] Graduando de Direito pela Universidade Federal do Ceará (UFC). Coordenador do Núcleo de Estudos em Ciências Criminais da Universidade Federal do Ceará (NECC/UFC). Pesquisador do Grupo de Estudos em Processo Penal (EPP/UFC). E-mail: dheanlucca@gmail.com

suspicions and proceedings. It's noted, therefore, that's necessary to understand how these data are currently protected and used in criminal proceedings. For this, a broad theoretical research is carried out, using the literature review technique, seeking to understand the sufficiency of legal instruments on this subject, how these data are treated in criminal proceedings and what the lack of security in handling can harm.

Keywords: Sensitive data. Criminal proceedings. Data security.

1. Introdução

O direito brasileiro já possui matérias legislativas que falam sobre a quebra de sigilo de dados. Contudo, ainda há falhas nos deveres de cuidado e manuseio dos dados no processo penal, visto a falta de legislação específica. Diante disso, apesar da diversidade de matérias em que esse dever é tratado, é necessário debater sobre a consolidação dele no sistema processual penal, conferindo um alinhamento referente às normas vigentes de proteção de dados. É importante destacar também que a Constituição Federal prevê a proteção de dados pessoais, além do STF reconhecer a proteção de dados como um direito fundamental.

Em uma realidade moderna e tecnológica, onde esses dados possuem maior liberdade, podendo prejudicar a coletividade e causar questionamentos, há a necessidade de uma governança, onde é importante observar a postura doutrinária e legislativa referente à segurança desses dados sensíveis, além do estudo sobre o seu manuseio sob a visão do processo penal. Isso é necessário pois quaisquer algoritmos de reconhecimento facial, números telefônicos ou outros dados podem entender que alguém é suspeito, mesmo não sendo. Portanto, as lacunas na utilização de dados pessoais no domínio processual penal podem ter efeitos irreparáveis.

Além disso, conforme o Artigo 47 da Lei Geral de Proteção de Dados (LGPD), qualquer pessoa envolvida no processamento de dados é obrigada a garantir a segurança dos dados pessoais. Desse modo, para fins de investigações e processos criminais, é importante definir os dados sensíveis porque há distinções entre eles, já que são essenciais para identificar criminosos, além dos dados confidenciais relacionados a questões políticas, crenças, afiliação, orientação sexual, etc. A repercussão que isso tem em termos de tratamento desses dados é que há mecanismos diferentes de utilização para persecução penal.

Daí, surge a relevância do presente estudo, visto que é importante ter uma visão atualizada sobre a proteção desses dados e sobre seu dever na atual legislação brasileira e no

atual momento, além de trazer uma perspectiva processual penal sobre o tema. Dessa forma, os instrumentos jurídicos existentes não são suficientes para garantirem essa proteção? Como os dados sensíveis são tratados no âmbito processual penal? Como a falta de segurança no manuseio dos dados pode prejudicar o processo penal?

Com a finalidade de alcançar o objetivo do presente estudo, em um primeiro momento, é abordada a importância dos dados sensíveis, além de mostrar o seu mérito. Após isso, no segundo momento, pretende-se mostrar como esses dados devem ser manuseados no devido processo legal. Em um terceiro momento, busca-se mostrar o papel do processo penal na segurança desses dados, e como eles devem ser utilizados de maneira que englobe a segurança coletiva. Ademais, constatar como o vazamento desses dados podem afetar as pessoas.

A partir da estratégia metodológica qualitativa, pretende-se utilizar um modelo teórico de pesquisa, partindo de uma revisão de literatura, nas bases de dados nacionais e internacionais, baseado em duas estratégias de busca: automática e *snowballing* (WOHLIN, 2014). Para isso, foi realizada uma ampla pesquisa teórica, utilizando a técnica de revisão de literatura e buscando a regulamentação presente no Código de Processo Penal, na Constituição e na Lei Geral de Proteção de Dados, além de artigos científicos e jornalísticos sobre o tema. Ademais, também foram analisadas jurisprudências e doutrinas sobre o assunto, visando uma pesquisa explicativa por meio do método de compreensão que tratam desse tema, justificando esse estudo e buscando dar significado às hipóteses desenvolvidas.

2. Previsão de proteção de dados pessoais

Conforme a Lei Geral de Proteção de Dados os dados sensíveis, inseridos dentro dos dados pessoais, são dados relativos à intimidade e natureza de cada um. Todos eles podem gerar algum tipo de discriminação e preconceito e por isso eles recebem uma maior proteção e deve trazer uma maior responsabilidade para quem os trata. Nesse sentido, o Supremo Tribunal Federal, ao julgar a Medida Provisória nº 954/2020, teve o entendimento de que o direito à proteção de dados pessoais é direito fundamental, traduzido no fundamento da dignidade da pessoa humana, inserido no inciso III do Artigo 1º da Constituição Federal da República Federativa do Brasil de 1988 (CRFB/88), e nas garantias de proteção à inviolabilidade da intimidade, à vida privada, à honra e à imagem das pessoas, assim como à autodeterminação informativa e ao sigilo dos dados, presentes nos incisos X e XII do Art. 5º da Constituição (SILVA; LIMA, 2020).

Segundo Molina e Lima (2020), o Supremo Tribunal Federal declarou inconstitucional a Medida Provisória nº 954/2020 que determinava o compartilhamento dos dados da população brasileira (telefone, nome completo e endereço) com o IBGE a fim de que fosse criada uma estatística oficial sobre a pandemia. O julgamento foi interessante na medida em que houve o reconhecimento de um direito fundamental à proteção dos dados pessoais. Assim, o Direito protege e tutela a proteção dos dados pessoais independentemente da legislação própria e específica. E a tutela tem natureza constitucional e é cláusula pétrea.

Daí, segundo o Guia de Elaboração de Programa de Governança em Privacidade (BRASIL, 2020, p. 20), na etapa de Construção e Execução do PGP que o Relatório de Impacto à Proteção de Dados Pessoais - RIPD deve ser elaborado. O RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição e serve tanto para a análise quanto para a documentação do tratamento dos dados pessoais. O RIPD visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Ademais, um PGP deve ser projetado para proteger os direitos do cidadão em relação à privacidade da informação e deve ser desenvolvido e implementado seguindo as leis jurisdicionais relevantes. Ainda sobre isso, acima de tudo, a privacidade desde a concepção exige que as instituições respeitem os direitos dos titulares dos dados pessoais. Isso é alcançado por meio de medidas como padrões fortes de privacidade, avisos apropriados e interfaces amigáveis que emponderem o titular dos dados. Os melhores resultados da privacidade desde a concepção, geralmente, são aqueles projetados de acordo com os interesses e necessidades dos titulares dos dados pessoais, que têm o maior interesse em gerenciar seus próprios dados (BRASIL, 2020, p. 19).

Esses dados devem ser utilizados com responsabilidade, além de haver uma prestação de contas sobre quem os possui, para que haja uma governança em relação aos dados pessoais para garantir o cumprimento efetivo das obrigações legais e para implementar um conjunto de documentos ou ferramentas que possam comprovar tal cumprimento. Assim, como esse dever de proteção já existia na Constituição de 1988, essa nova legislação apenas o reiterou, inovando nas hipóteses em que se consideram as proteções, dando mais segurança ao processo de dados e reforçando a necessidade de uma segurança de qualidade para que o devido processo seja garantido (LOPES JÚNIOR, 2020, p. 202).

Para que haja a privacidade e a proteção de dados incorporada, não basta apenas a redação de documentos e o estabelecimento de políticas. É necessário todo um desenvolvimento dos colaboradores, que é dificultado pela falta de conhecimento prévio do tema e exige grande esforço e criatividade, permitindo às pessoas a absorverem e aplicarem os conhecimentos necessários. Esta medida é essencial, tendo em vista que a regulamentação da LGPD não está completa e traz muitas obrigações e responsabilidades, sem indicar uma forma objetiva de atendê-las (SILVEIRA, 2021).

3. Manuseio dos dados sensíveis

A Política para Manuseio de Dados Pessoais tem como objetivo, para Orizon (2021), determinar e documentar que a coleta e o uso de dados pessoais sejam legais, bem como a base legal atribuída para o tratamento, nos termos do art. 7º e 11º da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados ("LGPD"), e com propósitos claramente definidos e legítimos.

A LGPD tem o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e de livre formação da personalidade de cada indivíduo. A Lei determina ainda que a revogação do consentimento para utilização de dados pessoais do titular possa ser solicitada pelo mesmo, seja por descumprimento da lei ou apenas pela simples vontade. Ou seja, o cliente ou usuário pode retirar a concessão sobre seus dados sensíveis apenas solicitando a exclusão ou bloqueio de acesso às suas informações pessoais. A própria Lei Geral de Proteção de Dados (LGPD) criou a Autoridade Nacional de Proteção de Dados (ANPD) para ser a agência responsável pela fiscalização do uso dos dados sensíveis presentes na internet.

Além das políticas e práticas (BRASIL, 2020, p. 18), papéis específicos dos servidores envolvidos na coleta, retenção, processamento, compartilhamento e eliminação de dados pessoais devem ser colocados em prática, assim como a educação dos colaboradores em relação a políticas e práticas de proteção de privacidade e dos cidadãos em relação aos seus direitos quanto à privacidade da informação. Logo, os direitos dos titulares precisam ser gerenciados. Devem ser destacadas e elucidadas questões como a diferença entre o titular e o custodiante do dado pessoal, bem como as obrigações quanto ao fornecimento de informações aos titulares com relação ao tratamento dos dados pessoais, termo de uso e política de privacidade.

Nesse cenário, gerenciamento de segurança e risco, bem como seus respectivos responsáveis, encontram, cada vez mais, requisitos complexos e restritivos a serem cumpridos para se ter, assim, uma efetiva governança de privacidade e manuseio de dados pessoais ao

longo de seu ciclo de vida. Uma implementação ampla e inclusiva de um Programa de Governança em Privacidade é necessária para gerenciar riscos, em ascensão, nas mais variadas áreas (BRASIL, 2020, p. 6). Aumentar a confiança de todas as partes interessadas necessita que os gestores do gerenciamento de segurança e risco ampliem tanto a frequência quanto a amplitude da comunicação, para assim assegurar que o uso dos dados pessoais seja granular, com finalidades específicas e com riscos mapeados e sob controle.

Dessa forma, surge a importância de destacar que deve haver um manuseio por meio de protocolo adequado dos vestígios digitais que forem recolhidos pelo seu potencial interesse para produção de provas, visto que os dados sensíveis também devem ser manuseados em todo o processo penal.

4. O Código de Processo Penal e os Dados Pessoais

No contexto do Código de Processo Penal (CPP), no Juiz das Garantias, a obtenção de informação confidencial pode ser utilizada como prova, mas deve possuir acesso separado (PRADO, 2020). Além disso, no Artigo 3º-B, há regras que tratam sobre sigilo nas comunicações, porém é algo que não pode ser tão simples, já que existem milhares de meios de comunicação com dados envolvidos que podem ser utilizados com o devido cuidado para que não haja vazamento ou corrompimento dos dados utilizados como prova ou na fase de investigação.

Além disso, provas sem dados ou comprovações podem ser facilmente alteradas ou excluídas. Ademais, a evidência será inútil se não for tratada adequadamente no processo de manuseio. Portanto, todo o processo de identificação, coleta, aquisição e preservação das evidências deve ser realizado por profissionais treinados e de acordo com os princípios e normas técnicas aplicáveis à espécie, a fim de manter a integridade, confiabilidade, imutabilidade e confiabilidade. É importante destacar que quaisquer normas técnicas destinadas a orientar a produção de provas em processo penal constituirão a composição e garantia do processo penal. Portanto, sua leitura deve ser norteada pelos valores da presunção de inocência, do devido processo e do processo justo.

Em diferentes sistemas jurídicos pelo mundo, iniciando-se na União Europeia, o estado tem discutido a coleta de materiais biológicos de suspeitos ou suspeitos de crimes, o rastreamento de seus respectivos perfis genéticos, o armazenamento dos perfis no banco de dados e o escopo do poder de usar e armazenar essas informações. Assim, a privacidade e a

intimidade protegidas pela constituição podem afetar as finanças pessoais, a vida bancária e financeira, mas para efeitos de justiça penal, para além da autorização legal de acesso à informação para fins específicos, afeta também as finanças pessoais e a vida financeira (SCHÜNEMANN, 2013). Portanto, a divulgação de tais dados e registros deve ser realizada dentro do âmbito objetivo e subjetivo de investigações ou processos criminais.

Nesse contexto de proteção, é importante citar também que não há incompatibilidade entre o processamento de solicitações que violam os requisitos de confidencialidade e oponentes anteriores. Dados e informações financeiras, bancárias e fiscais incluem registros e documentos de instituições públicas e privadas, que não devem ser perdidos ou adulterados pelo investigador ou réu (QUEIROZ, 2017, p. 138).

A partir da realidade do uso da Internet, à medida que deixamos rastros em tudo que praticamos na Internet, a personalidade digital torna-se cada vez mais característica (CRIMINAIS, 2018). Logo, muitas decisões sobre crimes são baseadas em evidências que sobraram do ciberespaço e, por conta disso, na reforma feita pela Lei nº 13.964 de 2019, a cadeia de custódia pode ser definida como um conjunto de procedimentos de registro de procedimentos para registro de origem, identidade, coleta, guarda, controle, análise e, por fim, descarte as evidências, assim como deveriam ser tratados os dados.

5. Os dados sensíveis no âmbito processual penal

A LGPD apontou a possibilidade de promulgar uma legislação específica sobre o âmbito processual penal em seu Artigo 4º, já que ela excluiu a segurança pública e o processo penal de sua estrutura. Neste caso, a LGPD criou uma lacuna que requer supervisão única sobre este assunto, bem como um marco regulatório (MIGLIORINI; TRIVINO, 2020).

Ainda segundo Migliorini e Trivino (2020), o Brasil possui normas sobre sigilo e violações, e os dados pessoais não são protegidos. Vale lembrar que a Constituição Federal prevê a proteção de dados pessoais (dados que identificam ou podem identificar pessoas físicas), mas de maneira geral. Para finalizar essas proteções, em 2020, o STF protegeu os dados pessoais como um direito fundamental e, por isso, devemos inferir que ele também engloba o processo penal.

Na União Europeia, embora o GDPR não resolva questões de segurança pública em um sentido amplo, o tratamento da Diretiva 2016/680 de leis específicas e do GDPR ocorre ao mesmo tempo, portanto não há vazio regulatório. No entanto, no Brasil, a LGPD foi lançada

em 2018, e somente em 2019 a Câmara dos Deputados tomou a iniciativa de criar uma comissão de juristas para redigir leis de segurança pública e processos criminais que tratam de casos de dados pessoais (COSTA; REIS, 2021).

Entre todas as posições apresentadas nesse assunto, o interesse comum é a promulgação de uma lei que não inviabilize o processamento de dados na atividade policial, mas que garanta direitos básicos e crie uma situação de confiança entre o Estado e os cidadãos. Portanto, segundo Costa e Reis (2021), é uma realidade utilizar ferramentas técnicas no processo penal para auxiliar na coleta de provas e nas investigações criminais. Portanto, o princípio da proporcionalidade deve nortear o uso da tecnologia, para que, por meio desse julgamento, seja possível determinar o grau de intrusão proporcional na privacidade do sujeito.

Ainda consoante as autoras Costa e Reis (2021), no anteprojeto sobre a LGPD Penal, foram também estabelecidos os princípios aplicáveis ao tratamento de dados na segurança pública e à investigação criminal. Algumas delas são iguais às da LGPD, mas outras tratam especificamente de atividades dessa natureza, como a legalidade e a legalidade estrita. Ademais, há direitos e obrigações que já são orientados pela LGPD, mas outros assuntos específicos foram adicionados ao escopo do projeto preliminar sobre a parte penal. Nesse anteprojeto, os direitos se aplicam principalmente aos titulares dos dados, enquanto as obrigações são direcionadas aos agentes de processamento. Assim, o anteprojeto instituiu o Conselho Nacional de Justiça (CNJ) como órgão fiscalizador do cumprimento das futuras legislações. Diferente da opção adotada pela LGPD, que criou a Agência Nacional de Proteção de Dados (ANP) para exercer as mesmas funções de fiscalização do processamento geral.

Em qualquer caso, o processamento de dados pessoais para tais fins penais traz benefícios diferentes. Por um lado, o Estado exerce poderes relacionados com a segurança pública e investigação. Por outro lado, salvaguarda os direitos e interesses dos cidadãos envolvidos. O equilíbrio e a compatibilidade dos dois são precisamente onde o projeto de lei se encaixa, já que no campo do processo penal, o uso da tecnologia, em algumas de suas variáveis, é imprescindível para a investigação.

Voltando ao exemplo da União Europeia, segundo Mangeth e Carneiro (2020), tal construção é realizada entre o RGPD e a Diretiva de Aplicação da Proteção de Dados, que também se destina a complementar a proposta da Comissão no Brasil. Dito isso, a experiência europeia conseguiu encontrar o equilíbrio necessário entre a proteção da privacidade individual

e a utilização dos seus dados para a segurança pública e os processos penais e da confiança dos cidadãos e da cooperação transfronteiriça.

Por outro lado, embora as regras da LGPD Penal se baseiem no princípio da legalidade, elas criarão um sistema rígido de interesse público e processual penal. A utilização de dados pessoais para fins de segurança pública e contencioso penal exige um sistema diferente daquele que pode ser utilizado para os fins gerais, já que esta relação tem uma natureza jurídica única e inerente conflito de interesses, conforme já explicitado.

Tudo isso é necessário já que denúncias indevidas podem comprometer a liberdade de uma pessoa, pois o algoritmo de reconhecimento facial pode entender que a pessoa é suspeita, quando na verdade não é, levando a uma falsa discriminação. Portanto, as lacunas na utilização de dados pessoais no domínio penal podem ter efeitos irreparáveis, como a liberdade (MANGETH; CARNEIRO, 2020). Logo, a LGPD Penal tem a harmonia necessária, pois por um lado é de interesse da comunidade nas investigações criminais, e por outro se preocupa em minimizar o impacto no domínio público dos cidadãos.

Sendo assim, podemos inferir que a LGPD Penal se faz necessária ante a exclusão dada pela própria lei de proteção de dados (MIGLIORINI; TRIVINO, 2020). Além disso, considerando a situação de discriminação e que o uso indevido de dados pode causar danos irreparáveis e requer maior segurança jurídica para os titulares de certos direitos (como a privação de liberdade), é importante dar proteção plena e digna aos titulares. Por fim, toda essa forma de punição que visa impor novos direitos básicos altamente reconhecidos pelo STJ e pelo STF, conforme já foi citado neste artigo.

6. Considerações finais

Apesar de haver avanços, ainda é necessário esclarecer as informações solicitadas e obtidas pelas autoridades que não possam ser divulgadas a terceiros e, caso não cumpram, terão responsabilidades funcionais e criminais. A preparação de um projeto de lei sobre a proteção dos dados no setor da segurança pública e investigações criminais, principalmente no processo penal, deve ter em conta vários fatores, começando pelo estabelecimento das suas orientações centrais de como manuseá-los.

Assim, o ciclo de vida dos dados pessoais deve estar em conformidade com LGPD. A importância de documentos relacionados a todo o ciclo de vida de dados pessoais e procedimentos correspondentes e a criação de rastros auditáveis, bem como o desenvolvimento

- e implementação contínua - de arquitetura, estratégias, práticas e procedimentos, podem gerenciar adequadamente os requisitos de dados pessoais e as proteções de reivindicação que devem chegar ao processo penal.

Além disso, mesmo que não seja um alvo da lei, a LGPD certamente levantará suspeitas sobre a natureza do crime, especialmente no que diz respeito às possíveis responsabilidades dos atores envolvidos na Lei Geral de Proteção de Dados. A abordagem narrativa de nossa disciplina da Lei Geral de Proteção de Dados (LGPD) se deve às respostas dos países ao uso de dados que as empresas podem usar para gerenciar, o que os obriga a cumprir os programas de integridade que respeitam a privacidade do usuário, não sendo pensada totalmente para o Processo Penal.

Diante do exposto, evidencia-se que o papel fundamentação dessa proteção de dados, sendo citado como um princípio e sendo utilizado em julgados e casos práticos. Entretanto, sua utilização encontra barreiras e desafios nas novas obrigações de cuidados. No âmbito dos processos penais, tais reservas devem estar no sentido estrito e garantir o respeito pelo processamento inicial da cadeia de custódia até ao final de cada entrada, processamento, transmissão e destruição de dados pessoais, pois todas as intervenções na proteção dos direitos dos dados devem ser formalizadas e significativas. Além disso, nesse processamento, a utilização de dados deve estar vinculada à finalidade estabelecida em legislação específica.

Mesmo que a proteção desses dados esteja amparada na legislação e na CRFB/88, sua utilização não é absoluta e nem ilimitada, visto que há correntes contrárias à sua utilização e a sua utilização em casos práticos é insuficiente. Apesar disso, não pode confundir a sua efetividade com o seu vigor, visto que a lei tem seu valor e pode ser, a qualquer momento, utilizada para obrigar o cuidado com todos os dados sensíveis. Embora os direitos de informação e o controle dos dados pessoais dos cidadãos para fins preventivos se concentrem nas mãos de um sujeito, o uso desses dados em processos penais - atividades de investigação ou no próprio processo penal - deve ser concentrado nas mãos de outro sujeito responsável nessa área criminal, com transmissão clara e acesso restrito.

Em razão disso, é necessário o contínuo estudo sobre a utilização desses dados na esfera processual penal, para que ela seja contemplada independentemente da lei utilizada. Assim, a essencialidade da segurança desse princípio será de extrema resolutividade, evitando danos e problemas decorrentes da ausência de cuidados. Assim, é necessário debater a lei de proteção

de dados destinada à segurança pública e ao processo penal, que também deve ser coerente com as recomendações que já existem no Código de Processo Penal.

Assim, podemos destacar que mudanças legislativas tendentes a ampliar a necessidade de proteção dos dados evitam arbitrariedades e podem ser consideradas modificações positivas para o Estado Democrático de Direito, visando a segurança dos indivíduos e, no âmbito processual penal, serem utilizadas com mais cautela e cuidados.

Desse modo, ao armazenar dados sensíveis, os tribunais devem executar uma série de medidas para que haja segurança na manutenção desses dados, visto que devem ter mecanismos de gerenciamento, arquivamento, entrada e saída desses dados. Ademais, eles podem ser eliminados após a prescrição do prazo estabelecido em lei para a prescrição do delito. Dessa forma, o controle efetivo deve ser realizado desde a coleta até o descarte dos dados.

7. Referências

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília: Senado Federal, 1988.

_____. Decreto-Lei nº 3.689, de 3 de outubro de 1941. Brasília: Senado Federal, 1941.

_____. Guia de Elaboração de Programa de Governança em Privacidade. Brasília: Ministério da Economia, 2020.

_____. Lei nº 13.709, de 14 de agosto de 2018. Brasília: Senado Federal, 2018.

_____. Lei nº 13.853, de 8 de julho de 2019. Brasília: Senado Federal, 2019.

_____. Lei nº 13.964, de 24 de dezembro de 2019. Brasília: Senado Federal, 2019.

COSTA, Eduarda; REIS, Carolina. Histórico da LGPD penal: o que foi feito até aqui e quais são os próximos passos. Disponível em: <https://lapin.org.br/2021/04/16/lgpd-penal-o-que-foi-feito-ate-aqui-e-quais-sao-os-proximos-passos/>. Acesso em: 15 abr. 2021.

CRIMINAIS. Canal de Ciências. Projeto de lei do novo CPP e as novas tecnologias. Disponível em: <https://canalcienciascriminais.jusbrasil.com.br/artigos/344286169/projeto-de-lei-do-novo-cpp-e-as-novas-tecnologias>. Acesso em: 27 fev. 2021.

LOPES JÚNIOR, Aury. *Direito Processual Penal*. São Paulo: Saraiva, 2020.

MANGETH, Ana; CARNEIRO, Giovana. Caminhos para a proteção de dados pessoais na segurança pública e investigação criminal: lições do Seminário Internacional da Comissão de Juristas. Disponível em: <https://www.orizonbrasil.com.br/politica-de-dados-pessoais.html>. Acesso em: 18 mai. 2021.

MILOGRINI, Ana; TRIVINO, Aline. Por que o Brasil precisa de lei para proteger dados pessoais na esfera penal. Disponível em: <https://www.conjur.com.br/2020-dez-07/opiniao-brasil-lgpd-penal>. Acesso em: 15 abr. 2021.

MOLINA, Lygia; LIMA, Marcelo. Privacidade: riscos e desafios da decisão do STF sobre a MP 954/2020. Disponível em: <https://emporiododireito.com.br/leitura/privacidade-riscos-e-desafios-da-decisao-do-stf-sobre-a-mp-954-2020>. Acesso em: 14 abr. 2021.

ORIZON. Política para manuseio de dados pessoais. Disponível em: <https://www.orizonbrasil.com.br/politica-de-dados-pessoais.html>. Acesso em: 15 abr. 2021.

PRADO, Geraldo. Notas sobre proteção de dados, prova digital e o devido processo penal. Disponível em: <https://www.conjur.com.br/2020-ago-18/geraldo-prado-protecao-dados-prova-digital-devido-processo-penal>. Acesso em: 27 fev. 2021.

QUEIROZ, David. *A Permeabilidade do Processo Penal*. Florianópolis: Empório do Direito, 2017.

SILVA, Fabiana; LIMA, Marcelo. STF reconhece o direito fundamental à proteção de dados pessoais. Disponível em: <https://emporiododireito.com.br/leitura/stf-reconhece-o-direito-fundamental-a-protecao-de-dados-pessoais>. Acesso em: 14 abr. 2021.

SILVEIRA, Ricardo. A importância da LGPD na implementação das empresas. Disponível em: <https://www.lgpdbrasil.com.br/a-importancia-da-lgpd-na-implementacao-das-empresas/>. Acesso em: 15 abr. 2021.

SCHÜNEMANN, Bernd. *Estudos de Direito Penal, Direito Processual Penal e Filosofia do Direito*. São Paulo: Marcial Pons, 2013.

WOHLIN, Claes. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: SHEPPERD, Martin (org.). *Proceedings of the 18th international conference on evaluation and assessment in software engineering*. Londres: Association for Computing Machinery, 2014. p. 1-10.