RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

LEI GERAL DE PROTEÇÃO DE DADOS E A ATIVIDADE DE INTELIGÊNCIA EM SEGURANÇA PÚBLICA: UMA ANÁLISE PROFÍCUA ENTRE A PRIVACIDADE INDIVIDUAL E A SEGURANÇA COLETIVA

BRAZIL'S GENERAL DATA PROTECTION LAW AND INTELLIGENCE ACTIVITY IN PUBLIC SECURITY: AN IN-DEPTH ANALYSIS OF INDIVIDUAL PRIVACY AND COLLECTIVE SECURITY

LEY GENERAL DE PROTECCIÓN DE DATOS DE BRASIL Y LA ACTIVIDAD DE INTELIGENCIA EN SEGURIDAD PÚBLICA: UN ANÁLISIS PROVECHOSO ENTRE LA PRIVACIDAD INDIVIDUAL Y LA SEGURIDAD COLECTIVA

Rafael Di Lorenzo Costa[1]

e5105813
https://doi.org/10.47820/recima21.v5i10.5813

PUBLICADO: 10/2024

RESUMO

Este artigo visa colaborar com a necessária discussão sobre os conflitos entre a Lei Geral de Proteção de Dados (LGPD) brasileira e a atividade de inteligência em segurança pública (ISP), abordando o delicado equilíbrio entre a privacidade da população e a segurança pública. O estudo revisa publicações, decisões judiciais, matérias jornalísticas e legislações vigentes em âmbito local e internacional, explorando como a LGPD pode impactar as práticas de segurança pública considerando a necessária utilização de dados pessoais para atividade de ISP. Por meio de uma pesquisa qualitativa baseada em análise documental e bibliográfica, os resultados mostram que ainda há grande controvérsia a ser trabalhada referente a essa temática considerando os conflitos entre os direitos individuais e a necessidade de proteção da coletividade. É apresentado o caso do estado do Paraná e sua preocupação com a adequação e *compliance*, bem como sugestões capazes de aprimorar a atividade de ISP, com especial menção à atividade de ISP da Polícia Militar do Paraná em razão do seu considerável efetivo. Conclui-se que há elevada importância na manutenção de um debate aprofundado sobre a composição entre privacidade e segurança no contexto da inteligência em segurança pública, integrando todos os atores estatais e da sociedade civil, considerando que é um tema em desenvolvimento e com rápida e constante evolução.

PALAVRAS-CHAVE: Privacidade. Segurança pública. Atividade de Inteligência. Lei Geral de Proteção de Dados.

ABSTRACT

This article aims to contribute to the necessary discussion on the conflicts between Brazil's General Data Protection Law (LGPD) and public security intelligence (ISP) activities, addressing the delicate balance between population privacy and public safety. The study reviews publications, court decisions, journalistic articles, and existing local and international legislation, exploring how the LGPD can impact public security practices considering the necessary use of personal data for ISP activity. Through qualitative research based on documentary and bibliographic analysis, the results show that there is still significant controversy to be addressed regarding this topic, considering the conflicts between individual rights and the need to protect the collective. The case of the State of Paraná is presented, with its concern for adequacy and compliance, as well as suggestions that could improve ISP activities, with particular mention of the ISP activity of the Paraná State Military Police due to its considerable work force. It is concluded that there is great importance in maintaining an in-depth debate on the balance between privacy and security in the context of public security intelligence, integrating all state and civil society actors, considering that it is a developing and rapidly evolving subject.

KEYWORDS: *Privacy. Public security. Intelligence activity. General Data Protection Law.*

[1] Policial militar do Estado do Paraná, com formação superior em Comunicação Institucional pela Universidade Federal do Paraná (UFPR) e pós graduado em Inteligência Policial e Penitenciária e Análise Criminal.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

RESUMEN

Este artículo tiene como objetivo contribuir a la necesaria discusión sobre los conflictos entre la Ley General de Protección de Datos (LGPD) de Brasil y la actividad de inteligencia en seguridad pública (ISP), abordando el delicado equilibrio entre la privacidad de la población y la seguridad pública. El estudio revisa publicaciones, decisiones judiciales, artículos periodísticos y legislaciones vigentes a nivel local e internacional, explorando como la LGPD puede impactar las prácticas de seguridad pública considerando el uso necesario de datos personales para las actividades de ISP. A través de una investigación cualitativa basada en análisis documental y bibliográfico, los resultados muestran que aún existe una gran controversia por abordar en torno a este tema, considerando los conflictos entre los derechos individuales y la necesidad de protección del colectivo. Se presenta el caso del Estado de Paraná y su preocupación por la adecuación y el cumplimiento, así como sugerencias que podrían mejorar las actividades de ISP, con especial mención a la actividad de ISP de la Policía Militar de Paraná debido a su considerable fuerza. Se concluye que es de gran importancia mantener un debate profundo sobre la composición entre la privacidad y la seguridad en el contexto de la inteligencia en seguridad pública, integrando a todos los actores estatales y de la sociedad civil, considerando que es un tema en desarrollo y de rápida y constante evolución.

PALABRAS CLAVE*: Privacidad. Seguridad pública. Actividad de inteligencia. Ley General de Protección de Datos.*

INTRODUÇÃO

O direito à privacidade está consagrado em vários instrumentos internacionais de direitos humanos, como a Declaração Universal dos Direitos Humanos (ONU, 1948) e o Pacto Internacional sobre Direitos Civis e Políticos (ONU, 1966), bem como nacionalmente, desde 1988, com a Constituição brasileira que estabelece a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (art. 5º, X). Esses documentos reconhecem que os indivíduos têm o direito de estarem livres de interferências arbitrárias em sua privacidade, família, casa e correspondência. Essa gama de garantias se estende à proteção de dados pessoais, e considerando a realidade em que eles podem facilmente ser coletados, armazenados e mal utilizados tanto por atores estatais quanto não estatais foram editadas ao redor do globo uma gama de legislações de proteção aos dados pessoais.

No Brasil temos a Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709/2018. A legislação elevou a nação a um novo patamar de proteção e privacidade para os dados pessoais no Brasil. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD regula o tratamento de dados pessoais, tanto no setor público quanto no privado, impondo obrigações rigorosas para garantir a segurança, a transparência e o uso adequado dessas informações. Entretanto, a necessidade de proteger a privacidade dos cidadãos precisa ser equilibrada com demandas legítimas de interesse público, como aquelas relacionadas à segurança pública, em especial a atividade de Inteligência de Segurança Pública (ISP).

A ISP é descrita pela Doutrina Nacional de Inteligência de Segurança Pública – DNISP (Brasil, 2014) como o conjunto de ações especializadas voltadas a identificar, monitorar e avaliar ameaças, reais ou potenciais, no âmbito da segurança pública. Seu objetivo é fornecer subsídios aos governos federais e estaduais na tomada de decisões estratégicas em suas políticas de segurança. A ISP apoia diretamente as operações policiais, abrangendo ações de prevenção, repressão, patrulhamento ostensivo e investigação criminal. Além disso, busca proporcionar alertas antecipados a autoridades

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

civis e militares, auxiliando na gestão de crises, prevenção de perturbações graves da ordem pública e ataques-surpresa, bem como no apoio à investigação de delitos.

Nesse contexto, surge um desafio crítico: como conciliar as exigências da LGPD com as atividades de inteligência de segurança pública, que dependem amplamente do acesso e tratamento de dados sensíveis para a prevenção e repressão de crimes? Embora a própria legislação preveja exceções para a segurança pública, o debate sobre os limites dessas exceções e o impacto prático da LGPD sobre as operações de inteligência é crescente e envolve questões legais, éticas e tecnológicas.

Por meio de artigos científicos, matérias jornalísticas, juristas, autores nacionais e internacionais, foram absorvidos a este artigo referenciais teóricos que permitiram a compreensão e decorrente reflexão sobre o tema, permitindo assim chegar a considerações contemporâneas e úteis. Desse modo, a metodologia aplicada foi a pesquisa qualitativa, eminentemente bibliográfica, em que o levantamento ou revisão dos conteúdos direciona o trabalho científico sendo dependente de dedicação, estudo e análise (Sousa *et al.,* 2021, p. 3). Por conseguinte, as fontes escolhidas foram selecionadas primando pertinência com o tema, atualidade das informações disponíveis, credibilidade dos autores e diversidade de perspectivas.

Ainda, considerando a extensão continental do Brasil que implica em diferentes realidades regionais, o estado do Paraná é utilizado como objeto de análise em razão de sua importância regional e pioneirismo na busca da governança, com especial menção à realidade da Polícia Militar Paranaense e seus impactos.

Assim, este artigo pretende equacionar a relação entre a LGPD e a atividade de ISP, analisando o marco legal entre a legislação e a segurança pública, incluindo as exceções já previstas. Serão então expostos os potenciais conflitos com a atividade de inteligência, incluídas aí as ferramentas modernas de uso e guarda de dados (Inteligência artificial e Big Data) de modo a identificar possíveis soluções e práticas que permitam equilibrar o direito à privacidade e à segurança pública.

1. O MARCO LEGAL: LGPD E A SEGURANÇA PÚBLICA

A LGPD foi sancionada em 14 de agosto de 2018 por meio da Lei nº 13.709 e surgiu à luz do crescente debate internacional quanto à necessidade de estabelecer um marco regulatório no tratamento de dados pessoais no Brasil em consonância com as práticas internacionais, como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia.

Por sua vez, o GDPR, predecessor europeu, foi implementado pela União Europeia em 25 de maio de 2018, sendo uma das mais abrangentes e rigorosas sobre o tema. O regulamento estabelece um conjunto unificado de regras para a coleta, armazenamento e tratamento de dados pessoais de indivíduos dentro da União Europeia, aplicando-se a empresas e organizações, independentemente de sua localização, desde que tratem dados de cidadãos europeus.

Há muitas similaridades entre a legislação pátria e a europeia, especialmente no que diz respeito aos princípios de proteção de dados e direitos dos titulares. As diferenças surgem majoritariamente na aplicação prática, severidade das penalidades e algumas especificidades

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

regulatórias. No geral, a versão nacional foi construída como uma tentativa de alinhar o Brasil às melhores práticas internacionais de proteção de dados, enquanto leva em consideração as particularidades do cenário jurídico e econômico do país.

A LGPD entrou efetivamente em vigor apenas em setembro de 2020, com o objetivo de garantir a privacidade e a proteção dos dados pessoais de indivíduos, bem como promover maior segurança jurídica no uso dessas informações, tanto no setor privado quanto no público. Com esse objetivo, logo no art. 6º da Lei nº 13.709/2018 (LGPD) são elencados dez princípios que devem nortear o tratamento de dados pessoais. Destes dez, sete se relacionam diretamente com a ISP:

> Finalidade: Os dados devem ser tratados para fins legítimos, específicos e informados ao titular.
> Adequação: O tratamento dos dados deve ser compatível com as finalidades informadas ao titular.
> Necessidade: A coleta de dados deve se limitar ao mínimo necessário para a realização das finalidades pretendidas.
> Transparência: O titular dos dados tem o direito de ser informado de forma clara e acessível sobre o tratamento de seus dados.
> Segurança: Devem ser adotadas medidas para proteger os dados pessoais contra acessos não autorizados e vazamentos.
> Prevenção: É necessário prevenir a ocorrência de danos relacionados ao tratamento de dados.
> Responsabilização e prestação de contas**:** O controlador dos dados deve demonstrar a adoção de medidas eficazes para proteger os dados e cumprir a legislação (art. 6º, I, II, III, VI, VII, VIII, X, da Lei nº 13.709/2018).

Nota-se que esses princípios visam criar um equilíbrio entre a utilização dos dados para fins econômicos e tecnológicos e a preservação dos direitos fundamentais dos indivíduos, como privacidade e liberdade.

Há ainda uma diferenciação importante quanto ao tratamento de dados entre o setor privado e o setor público, conforme estabelece o art. 7º:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
> III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (Lei nº 13.709/2018).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Nota-se que as empresas, além da necessidade de justificar o tratamento de dados pessoais, devem obrigatoriamente possuir o consentimento do titular. Enquanto no setor público o tratamento de dados não depende necessariamente do consentimento do titular, sendo expressa a base legal mais relevante aos órgãos públicos no inciso III, que expressa a permissão de tratamento para o cumprimento de políticas públicas previstas em leis, regulamentos ou para a execução de atividades de interesse público.

Destarte, a execução de políticas públicas é, portanto, uma justificativa central para o tratamento de dados por entes governamentais, expandindo ainda o uso de outras bases, como segurança nacional, consoante é tratado em capítulo específico da lei e que será apresentado adiante.

2. EXCEÇÕES LEGAIS PARA A SEGURANÇA PÚBLICA

Enquanto no setor privado são impostas mais restrições ao uso e tratamento de dados, tendo que ser justificada a coleta e uso de forma transparente, especialmente no que diz respeito ao direito de consentimento, acesso, correção e eliminação de dados frente aos titulares dessas informações, o setor público possui exceções específicas.

O art. 4º da LGPD prevê tratamento de dados por órgãos públicos quando se trata de segurança pública, defesa, segurança do Estado e investigações criminais. Nesses casos, o tratamento de dados pode ocorrer com maior flexibilidade, sem a necessidade de seguir certos princípios aplicáveis ao setor privado, com destaque à obtenção de consentimento, desde que as atividades sejam justificadas pelo interesse público ou pela execução de funções previstas por lei.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> 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;
> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.
> § 2º É vedado o tratamento dos dados a que se refere o inciso III do *caput* deste artigo por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico à autoridade nacional e que deverão observar a limitação imposta no § 4º deste artigo.
> § 3º A autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do *caput* deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais.
> § 4º Em nenhum caso a totalidade dos dados pessoais de banco de dados de que trata o inciso III do *caput* deste artigo poderá ser tratada por pessoa de direito privado, salvo por aquela que possua capital integralmente constituído pelo poder público (Lei nº 13.709/2018).

Destaca-se que, embora haja a exceção prevista, ela é acompanhada de outras determinações visando regular o uso dos dados como destacado nos §§ 1º e 3º do art. 4º e que são mais detalhadas no Capítulo IV da legislação (do tratamento de dados pessoais pelo poder público).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Outrossim, a Autoridade Nacional de Proteção de Dados (ANPD)[1], ciente da importância do tema, produziu um guia orientativo sobre o tratamento de dados pessoais pelo poder público em janeiro de 2022 (versão 1.0) e atualizado em junho de 2023 (versão 2.0).

O guia visa orientar órgãos públicos quanto à aplicação e conformidade à LGPD. Abrangem-se aspectos práticos e legais para garantir que o tratamento de dados pelo setor público seja realizado com respeito aos direitos dos titulares e as bases legais para uso de dados.

A Organização dos Estados Americanos (OEA), da qual o Brasil é membro, também divulgou uma cartilha em 2021 denominada: Princípios Atualizados sobre a Privacidade e a Proteção de Dados Pessoais. Além de apresentar um conteúdo alinhado com a legislação brasileira, é pertinente trazer o que é explanado quanto às exceções à privacidade:

> No entanto, a privacidade não é o único interesse que os Estados membros e seus governos devem ter em conta no campo da compilação, retenção e divulgação de dados. De tempos em tempos, surgirá inevitavelmente a necessidade de levar em conta outras responsabilidades do Estado, levando à limitação dos direitos de privacidade das pessoas.
> Em alguns casos, é possível que as autoridades dos Estados membros da OEA tenham que se afastar destes Princípios ou estabelecer restrições que devem limitar-se àquelas necessárias, adequadas e proporcionais em uma sociedade democrática para salvaguardar a segurança nacional e a segurança pública, a proteção da saúde pública, a administração da justiça, o cumprimento das normas ou outras prerrogativas essenciais da ordem pública, a proteção dos direitos e liberdades e outros objetivos de interesse público geral. Por exemplo, ao responder às ameaças representadas pela criminalidade internacional, terrorismo e corrupção, bem como a certas violações graves dos direitos humanos, as autoridades competentes dos Estados membros da OEA já tomaram providências especiais para a cooperação internacional na detecção, investigação, punição e prevenção de delitos penais (OEA, 2021, p. 83).

Em suma, com esse exemplo, reforça-se, agora em âmbito internacional, o reconhecimento da excepcionalidade aplicável à Inteligência de Segurança Pública (ISP).

Outra exceção aplicada à atividade de inteligência pode ser localizada na Lei Federal nº 12.527/2011, também conhecida como Lei de Acesso à Informação (LAI). A Lei disciplina o direito insculpido no art. 5º, XXXIII, da Constituição Federal de 1988:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (BRASIL, 1988).

Em síntese, a LAI promove a regulação das garantias do direito ao acesso à informação, disciplinando regras, recursos, abarcando o tratamento de informações pessoais e responsabilidade dos agentes públicos em conformidade com os princípios básicos da administração. Estabelece ainda vedações às restrições às informações necessárias à tutela judicial ou administrativa de direitos

[1] Autarquia criada pela LGPD dotada de autonomia técnica e decisória conforme art. 55-A.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

fundamentais ou que impliquem violação a direitos humanos, com preponderância do acesso público, de modo a incentivar a participação popular (Almeida *et al.,* 2014, p. 9-13).

O Ministro da Suprema Corte Gilmar Ferreira Mendes explana didaticamente a relação entre democracia, informação e princípio da publicidade, segundo o qual:

> está ligado ao direito de informação e ao dever de transparência do Estado, em conexão direta com o princípio democrático, e pode ser considerado na perspectiva do direito à informação (e de acesso à informação) como garantia de participação e controle social dos cidadãos (a partir das disposições relacionadas no art. 5º, CF/88), bem como (2) na perspectiva da atuação da Administração Pública em sentido amplo (a partir dos princípios determinados no art. 37, *caput*, e artigos seguintes da CF/88) (Mendes, 2012).

Então, reconhecida a importância da segurança pública e da atividade de inteligência, a norma também regula as restrições a esse direito de informação tutelado. O Capítulo IV da LAI trata das restrições ao acesso à informação:

> Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:
> I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;
> II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;
> III - pôr em risco a vida, a segurança ou a saúde da população;
> IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;
> V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;
> VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;
> VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou
> VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.
> Art. 24. A informação em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, poderá ser classificada como ultrassecreta, secreta ou reservada (Lei nº 12.527/2011).

Assim, fica evidente a comunicação entre ambas, a LGPD e a LAI, no sentido de reconhecer a validade e importância do tratamento de dados e informações pelo sistema de inteligência de segurança pública. Essa comunicação, no entanto, não impede a existência de potenciais conflitos.

3. CONFLITOS POTENCIAIS ENTRE A LGPD E A INTELIGÊNCIA DE SEGURANÇA PÚBLICA (ISP)

A tensão entre privacidade e segurança é um tema central no debate contemporâneo sobre o uso de dados por forças de segurança e operações de inteligência. Esse dilema ocorre porque a coleta e o monitoramento de dados, muitas vezes necessários para prevenir crimes e ameaças à segurança nacional, podem invadir a privacidade dos cidadãos e comprometer direitos fundamentais.

Para equacionar os conflitos de princípios constitucionais, Luciano Pires de Morais (2017) explana que é feita uma ponderação de interesses, colocando-se os dois princípios em choque em uma

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

espécie de balança imaginária, acrescentando ainda que “normas de direitos fundamentais devem ser mantidas, de forma a não se eliminar nenhuma delas do texto da Constituição, operando-se, apenas, uma harmonização de interesses no concreto”. Ainda:

> Complementa Stum que “princípios que se chocam produzem conflito, não implicando a eliminação do sistema, justamente porque nesse caso trata-se do conteúdo de uma norma e não do espaço ocupado por ela”, de modo que a solução deve ser encontrada através de métodos que visem ao equilíbrio entre os princípios conflitantes, utilizando-se, assim, de outros princípios, como os da proporcionalidade, da razoabilidade e da necessidade, pois tal solução não obedece a uma ordem hierárquica pré-estabelecida de valores constitucionais. As normas constitucionais possuem o mesmo valor quando em abstrato, a ocorrência de um caso concreto é que põe em evidência o conflito (Morais, 2017).

A atividade de ISP está escorada no dever do Estado de prover a Segurança Pública conforme art. 144 da carta magna (Brasil, 1988) e para isso muitas vezes depende da coleta massiva de dados, incluindo comunicações eletrônicas, registros financeiros e informações pessoais. Contudo, legislações nacionais e internacionais – como visto anteriormente – impõem restrições e contrapesos a essas coletas. Embora haja regulamentações que permitam aos sistemas de inteligência de segurança pública o acesso e obtenção de informações pertinentes, elas conflitam em momentos de emergência e de necessário dinamismo em razão de barreiras legais e burocráticas impostas.

As barreiras legais e procedimentais por vezes podem retardar o processo de obtenção de informações críticas em ações de inteligência, especialmente em situações de emergência. Quando dados sensíveis são protegidos de forma rigorosa, o acesso rápido e em larga escala por parte de agências de inteligência pode ser restringido, o que pode impactar atuação contra o crime organizado e outras ameaças de alta gravidade, a exemplo das ações de domínio de cidades e novo cangaço[2].

Noutro giro, a inovação da tecnologia muitas vezes avança mais rapidamente que a regulamentação de novas ferramentas tecnológicas, de modo que as novidades frequentemente entram em conflito com legislações de privacidade e órgãos ou representantes da sociedade civil organizada, criando um dilema sobre o quanto pode ou deve ser permitido.

Um exemplo palpitante desse conflito é observado nos casos das ferramentas de reconhecimento facial, que, embora tenham um potencial extremamente útil à segurança pública, sofrem constante aversão. Para ilustrar essa oposição expõe-se o caso do Metrô de São Paulo.

Em 2022 a Companhia do Metropolitano de São Paulo – Metrô, empresa responsável pela operação e expansão do sistema metroviário da região metropolitana de São Paulo/SP, iniciou uma licitação para implantação de um Sistema de Monitoramento Eletrônico (SME) em algumas estações de sua rede de transporte coletivo. Essa iniciativa logo foi alvo de uma Ação Civil Pública (ACP) ajuizada pela Defensoria Pública do Estado de São Paulo, Defensoria Pública da União, IDEC – Instituto Brasileiro de Defesa do Consumidor, INTERVOZES – Coletivo Brasil de Comunicação Social, e ONG Artigo 19 Brasil.

[2] O domínio de cidades é uma nova modalidade dos crimes ao patrimônio, considerado uma evolução dos roubos conhecidos como novo cangaço. Distingue-se por exercer o controle sobre cidades por um período de horas, paralisando suas forças de segurança, obstruindo entradas e saídas (OSTRONOFF, 2023).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Na referida ACP os autores alegaram que o edital de licitação – mesmo sem mencionar explicitamente – busca a implantação de um sistema de reconhecimento facial capaz de monitorar todos os usuários do Metrô, armazenando e compartilhando dados biométricos por meio de um *software* privado que poderia ainda se integrar a outros sistemas de vigilância. Argumenta-se quanto à ilegalidade e desproporcionalidade da medida por não haver consentimento expresso dos usuários para o tratamento de seus dados biométricos, nem transparência quanto aos riscos envolvidos. Alegaram por fim que não teriam sido descritas medidas de proteção e mitigação de riscos, violando a LGPD, o Código de Defesa dos Usuários de Serviços Públicos e o Código de Defesa do Consumidor, além de favorecer a discriminação racial (Autos nº 1010667-97.2022.8.26.0053 6ª Vara de Fazenda Pública – Tribunal de Justiça Estado de São Paulo).

Tamanha é a complexidade do tema que a ação ainda transcorre sem solução na justiça paulista. No próprio Acórdão que denegou o pedido de liminar para suspensão da licitação combatida, não houve consenso, tendo a relatora do recurso sido voto vencido, embora sua preocupação tenha sido devidamente registrada na peça decisória:

> Elegante e zelosa como é do seu proceder, ponderou a nobre relatora sorteada sua preocupação, no âmbito internacional e interno, co'a possibilidade de utilização para além das finalidades iniciais desse novo sistema de vídeo-vigilância, notadamente diante da falta de regulamentação e formas de controle, assim embasando em alentado voto sua proposta de não provimento ao recurso.
> Tenho, todavia, que o sistema processual nos indica outra vertente segura a ser considerada no desate deste agravo de instrumento (Agravo de Instrumento nº 2079077-58.2022.8.26.0000 da 5ª Câmara de Direito Público do Tribunal de Justiça de São Paulo).

O exemplo citado ainda demonstra que não há como deixar de refletir sobre os dilemas éticos no tratamento de dados sensíveis pelas forças de segurança. A vigilância constante ou coleta massiva de dados pode ser vista como uma forma de abuso de poder. A capacidade de monitorar pessoas pode levar a um controle social que interfere nas liberdades civis e nos direitos fundamentais, levando ao uso desproporcional do aparato estatal.

Sabe-se também que doutrinariamente a ISP ocorre sob sigilo, o que pode dificultar a responsabilização de abusos. Outro dilema ético surge quando os cidadãos não sabem quais informações estão sendo coletadas ou como estão sendo usadas, violando o princípio da transparência.

Não há como deixar de mencionar também o risco de vazamentos de informações sensíveis. Forças de segurança que tratam dados pessoais e de inteligência têm a obrigação ética de protegê-los contra-ataques cibernéticos, mas nem sempre isso acontece de maneira eficaz, expondo indivíduos e organizações a riscos.

Em suma, o desafio central reside em encontrar o equilíbrio entre a necessidade de proteger a sociedade de ameaças reais e preservar os direitos individuais, como o direito à privacidade. Ao criar políticas de segurança e regulamentações de proteção de dados, é fundamental considerar o impacto ético, promovendo transparência, responsabilização e controle democrático sobre as atividades de coleta de dados realizadas por forças de segurança, ainda mais em uma era que se abre à Inteligência Artificial e ao grande conjunto de dados disponíveis (Big Data).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

4. INTELIGÊNCIA ARTIFICIAL, BIG DATA E O USO DE DADOS NA SEGURANÇA PÚBLICA

A Inteligência Artificial (IA) e o Big Data[3] têm revolucionado o tratamento de dados e as atividades de inteligência, apresentando diversas oportunidades e, em igual medida, desafios, com especial impacto na segurança pública. Essas ferramentas permitem a coleta, processamento e análise de grandes volumes de dados com velocidade e exatidão sem precedentes, potencializando a capacidade de assessoramento ágil, eficiente e oportuno aos tomadores de decisão, além da capacidade de permitir atuação imediata quando da detecção de incidentes, crimes e ameaças. Porém, como visto, o uso dessas ferramentas também evoca questões regulatórias e éticas, além de desafios técnicos e operacionais que precisam ser adequadamente gerenciados.

No âmbito de ISP, a IA tem potencial para identificar ameaças, prever comportamentos e, inclusive, automatizar processos investigatórios. Sistemas de reconhecimento facial e análise de vídeo em tempo real, como mencionado anteriormente, podem ajudar a identificar suspeitos ou prever a ocorrência de crimes em áreas específicas. Além disso, uma IA pode ser projetada para identificar padrões em atividades como lavagem de dinheiro e auxiliar no combate ao terrorismo e ao crime organizado.

Noutro giro, o Big Data apresenta o desafio às organizações de inteligência que por vezes se deparem com volumes massivos de informações geradas por diferentes fontes, como vídeos de segurança, comunicações telemáticas, transações financeiras e dados de degravação de aparelhos eletrônicos no curso de investigações. Assim, a capacidade de análise massiva é essencial para detectar tendências, responder rapidamente a ameaças em tempo real e instruir inquéritos em curso com informações pertinentes.

Essas relações são bem trabalhadas pelo Major do Exército Brasileiro Igor Leonardo Ventapane Freitas em sua publicação “A Inteligência Artificial como ferramenta para a atividade de Inteligência no combate ao terrorismo”, em que assevera a possibilidade de utilização da IA e Big Data na atividade de inteligência no combate ao terrorismo e outras ameaças. Ele detalha como a IA pode ser utilizada para identificar suspeitos por meio de redes e bancos de dados de imagens, analisando características faciais e em investigações, por meio do processamento de linguagem natural (NLP), com o Big Data facilitando a análise de grandes volumes de dados, como interceptações telefônicas, ajudando a detectar palavras-chave. Menciona ainda a mineração de dados on-line para identificação de padrões de comportamento até aplicação de tecnologias preditivas que podem antecipar desastres naturais (Freitas, 2022, p. 32-40).

Ressalta-se que o governo brasileiro não está alheio à importância da IA e Big Data. Ainda em 2019 já eram anunciados investimentos em ferramentas de Big Data e IA tendo o Ministério da Justiça e Segurança Pública declarado a entrega de quatro ferramentas: Sinesp Big Data, Sinesp Geointeligência, Sinesp Tempo Real e o Sinesp Busca. O investimento inicial anunciado foi de 32

[3] Big Data é um conceito que descreve conjuntos de dados que excedem o tamanho que pode ser gerenciado por ferramentas tradicionais. É definido por três Vs: variedade, volume e velocidade (ORACLE, 2024).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

milhões de reais em "infraestrutura digital com objetivo de facilitar a integração e análise de grandes volumes de dados na segurança pública. O Big Data e Inteligência Artificial serão constantemente aprimorados com novas soluções e recursos de tecnologias sem nenhum custo para os estados" (Brasil; Ministério Da Justiça, 2019).

5. BOAS PRÁTICAS E GOVERNANÇA DE DADOS NA SEGURANÇA PÚBLICA DO PARANÁ

Os conflitos principiológicos, as normas legais e as expansões tecnológicas exercem impacto direto ou indireto na segurança pública de modo que se gera uma necessidade urgente de adoção de boas práticas de governança e *compliance*, especialmente em relação ao tratamento de dados pessoais. Com a promulgação da LGPD, a responsabilidade do Estado e das forças de segurança sobre o uso e a proteção de informações pessoais ficou ainda mais evidente. Além de exigir maior transparência, a lei impõe a criação de políticas internas, programas de capacitação e a implementação de protocolos que garantam o uso seguro e legal dos dados.

O estado do Paraná, por meio da Controladoria Geral do Estado (CGE-PR), em se tratando de administração pública no Brasil, foi pioneiro ao buscar a implementação de um Programa Estadual de Integridade e *Compliance* que envolve concepção, implementação e monitoramento de políticas, procedimentos e práticas em torno do respeito à moralidade e eficiência administrativa. O programa paranaense "é uma ferramenta de gestão, que tem como base a ética e a integridade. A palavra *compliance* significa estar em conformidade ou agir de acordo com leis, normas e regulamentos. Uma das finalidades do programa é promover uma cultura baseada na honestidade" (CGE-PR, s.d.).

Dentro desse escopo se inclui a conformidade à LGPD, razão pela qual já em abril de 2020 a CGE produziu a "Cartilha LGPD", que detalha as determinações e efeitos da legislação; em dezembro de 2020 editou o Decreto Estadual nº 6.474/2020 que regulamentou a LGPD no âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo do Estado do Paraná, e em junho de 2022 foi editada a Resolução CGE nº 36/2022 que instituiu a Política de Privacidade de Dados Pessoais no Âmbito da Controladoria Geral do Estado do Paraná. Ainda nesse sentido, e indicando a preocupação e aprimoramento constantes do Paraná, em fevereiro de 2024 foram publicados pela CGE o "Manual de Implementação da LGPD", "Cartilha de Boas Práticas no Tratamento de Dados Pessoais" e "Plano de Respostas a Incidentes de Segurança".

Essas ações do governo paranaense criam uma estrutura clara de tratamento e responsabilidades no âmbito do executivo estadual a quem estão subordinados os órgãos de segurança pública do estado, como as Polícias Militar (PMPR) e Civil (PCPR). Isso permite governança de dados, envolvendo a implementação de um conjunto de políticas, procedimentos e ferramentas que garantam a conformidade com leis como a LGPD, promovendo transparência, segurança e responsabilidade no tratamento das informações.

Por sua vez a Polícia Militar do Paraná (PMPR), órgão de segurança com efetivo mais numeroso do estado, por meio da Portaria do Comando-Geral nº 221/2022 implementou o Núcleo de

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

Integridade e *Compliance* Setorial da Polícia Militar do Paraná (NICS/PMPR) e lá destinou um capítulo para o tratamento de dados pessoais:

> CAPÍTULO III
> DO TRATAMENTO DOS DADOS PESSOAIS
> Art. 7º O NICS/PMPR terá um Encarregado pelo Tratamento de Dados Pessoais, designado por ato do Comandante-Geral da Corporação, conforme inciso I, do art. 8º do Decreto Estadual nº 6.474, de 14 de dezembro de 2020, e terá as seguintes atribuições:
> I – auxiliar a PMPR a adaptar seus processos de acordo com a LGPD, incluindo a responsabilidade quanto à orientação e aplicação de boas práticas e governança;
> II – trabalhar de forma integrada com o controlador e com os operadores dos dados, considerando a necessidade de um monitoramento regular e sistemático das atividades destes;
> III – estar facilmente acessível quando necessária a sua interveniência;
> IV – receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> V – receber comunicações da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e adotar providências;
> VI – orientar os militares estaduais, servidores e os contratados da Corporação a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
> VII – auxiliar o controlador a apresentar Relatório de Impacto de Proteção aos Dados Pessoais, quando solicitado;
> VIII – receber comunicações e atender a normas complementares da Autoridade Nacional de Proteção de Dados Pessoais (ANPD);
> IX – informar à Agência Nacional de Proteção de Dados Pessoais (ANPD) e aos titulares dos dados eventuais incidentes de privacidade, observadas a Política Nacional de Proteção de Dados Pessoais e da Privacidade e as orientações da CGE;
> X – executar outras atribuições definidas em normas complementares (Portaria CG nº 221/2022, PMPR).

Isto posto, é essencial aos atores da segurança pública, em especial aqueles da instituição mais numerosa (PMPR), a ciência da relevância da sua atividade e da importância de agirem em harmonia com a LGPD e demais normas aplicáveis, tanto a nível federal como estadual e institucional. Deste modo, é possível trabalhar os conflitos potenciais entre a LGPD e a Inteligência de Segurança Pública.

Verifica-se que uma das maiores preocupações com relação ao tratamento de dados pela segurança pública costuma ser a violação da privacidade dos cidadãos. O principal modo de mitigar essa resistência é com atuação profissionalizada, ética e responsável. Falhas de segurança ou exposição de condutas impróprias dos agentes do estado afetam frontalmente as ações que permitem a obtenção, armazenamento e tratamento de dados úteis à atividade de ISP. Relembre-se, no caso do Metrô de São Paulo, que a preocupação com o tratamento das imagens de reconhecimento facial gerou forte resistência à implementação da medida.

Relevante manter devotada atenção aos princípios insculpidos na LGPD (art. 6º) e a partir dali buscar a adoção de políticas de minimização de uso de dados como prática fundamental. Isso significa que as forças de segurança devem limitar a coleta de dados ao mínimo necessário para o cumprimento de suas funções. Isso evita a coleta excessiva de informações pessoais e mitiga os riscos associados ao vazamento ou uso indevido de dados. Outra prática relevante é o estabelecimento de ciclos claros de retenção de dados, determinando por quanto tempo as informações serão armazenadas antes de serem excluídas ou anonimizadas.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

A comunicação clara sobre esses processos reforça a confiança entre a sociedade e as forças de segurança. Nesse sentido, é possível verificar que o estado do Paraná busca as melhores práticas de atendimento à LGPD e *compliance*, o que fortalece colateralmente a atuação da ISP, em razão da validação da credibilidade estatal.

6. CONSIDERAÇÕES

Como visto, a pertinência, relativa novidade e complexidade mantêm o tema em constante discussão na sociedade. A era da informação, ou era da tecnologia como é conhecido o momento civilizacional atual, apresenta como um dos seus grandes desafios em nível de políticas públicas o equilíbrio entre a proteção de dados pessoais e a segurança pública. De um lado, o uso de tecnologias modernas de inteligência artificial e big data fortalece a capacidade das agências de inteligência de segurança pública em prever, prevenir e combater crimes, proporcionando elevada eficiência na proteção dos cidadãos. Por outro prisma, o uso intensivo de dados pessoais eleva as preocupações quanto à privacidade e o risco de abusos, como vigilância excessiva e violações de direitos fundamentais. Encontrar esse equilíbrio é uma tarefa que ainda mantém grande controvérsia, nas esferas de discussão pública, jurídica e legislativa.

É pertinente que as polícias estaduais, importantes membros da ISP, busquem autorregulações e procedimentos para se enquadrar e se adiantar aos constantes debates sociais. Três conjuntos de ações podem auxiliar as atividades de ISP.

Inicialmente, o fortalecimento da supervisão sobre o tratamento de dados pelas forças de segurança é essencial. Isso pode ser alcançado por meio da criação de uma política de tratamento de dados pessoais no âmbito dos sistemas de inteligência estaduais, a cargo de suas seções de Contrainteligência[4] nos moldes da Resolução CGE/PR nº 36/2022, respeitadas as peculiaridades da atividade com a criação de subseções de *compliance* dentro da ISP.

Em continuidade, a implementação de medidas tecnológicas capazes de identificar o uso inadequado dos bancos de dados de acesso restrito a disposição dos agentes de inteligência favoreceria seu fortalecimento e sua capacidade correcional. Medidas simples como gatilhos sistêmicos que informassem a um controlador designado quando um agente de inteligência ou qualquer agente público subordinado, mas com acesso a sistemas, fizesse um número anormal de consultas, o que poderia indicar uso indevido ou comprometimento das credenciais. Ou seja, utilizar a IA também em ações de defesa da ISP e seus ativos.

Em terceiro lugar, o aprimoramento da transparência de resultados é fundamental. Ações de comunicação por meio dos órgãos de segurança com informações claras sobre os resultados práticos decorrentes do processamento e armazenamento de dados e informações pelas atividades de ISP em conformidade com as normas legais. Um exemplo é a publicização de *cases* de sucesso que tiveram

[4] A Contrainteligência é a atividade que objetiva prevenir, detectar, obstruir e neutralizar a Inteligência adversa e as ações que constituam ameaça à salvaguarda de dados, conhecimentos, pessoas, áreas e instalações de interesse da sociedade e do Estado (ABIN, 2021).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

atuação da atividade de inteligência, tal como a operação da inteligência da PMPR que impediu um roubo a duas agências bancárias no município de Três Barras em 2021[5]. Isso eleva a percepção positiva da sociedade, diminuindo as resistências à utilização dos dados.

Essas ações são apenas algumas das possibilidades em um vasto universo de variáveis e discussões que toda a sociedade, seus representantes e suas instituições devem manter. Elas são especialmente aplicáveis aos Sistemas de Inteligência Paranaenses em razão da maturidade das normativas do poder executivo do estado nesse tema. Ressalta-se ainda que as implicações atuais e futuras no contexto da LGPD e atividade de ISP incluem desafios constantes considerando o desenvolvimento ininterrupto de tecnologias emergentes e mais sofisticadas, que exigirão regulamentações dinâmicas e em constante evolução.

Relevante mencionar que embora a realidade paranaense tenha sido privilegiada nesta análise, as ações poderiam ser replicadas em todos os entes federativos, considerada a unidade legislativa federal em que todos os órgãos de governança locais devem se subsidiar.

Por fim, não é intenção deste artigo, nem seria possível, apresentar uma solução definitiva para a dicotomia entre privacidade individual e a segurança coletiva, mas, sim, apresentar uma análise do contexto geral capaz colaborar com a discussão premente sobre um tema de relevante repercussão social e importância para as forças de segurança. Espera-se aprimorar o debate quanto ao equilíbrio delicado entre a proteção dos dados dos cidadãos e as necessidades legítimas das atividades de inteligência em segurança pública, mantendo-se os princípios democráticos e o estado de direito em especial pela ótica dos agentes de ISP.

REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. **Contrainteligência**. Brasilia: ABIN, 2021. Disponível em: https://www.gov.br/abin/ptbr/assuntos/inteligenciaecontrainteligencia/CI#:~:text=A%20Contrainteliq%C3%AAncia%20%C3%A9%20a%20atividade,da%20sociedade%20e%20do%20Estado. Acesso em: 10 out. 2024.

ALMEIDA, H. de; LEHFELD, L. de S.; GUEDES, M. B. **Comentários à Lei de Acesso à Informação**. Santa Cruz do Sul: Essere nel mondo, 2014. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/Livro%20%20Coment%C3%A1rios%20%C3%A0%20lei%20acesso.pdf. Acesso em: 10 out. 2024.

ANPD – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo**: Tratamento de dados pessoais pelo Poder Público. Brasília: ANPD, Versão 2.0, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 10 out. 2024.

[5] "A quadrilha que tentou assaltar um banco em Três Barras do Paraná (PR) já era monitorada pela Inteligência da Polícia Militar desde julho deste ano. Os suspeitos ficaram visados pelas autoridades após realizarem roubos em agências de outros municípios paranaenses, como Campo Bonito, São Carlos do Ivaí e Mariluz e estariam planejando a nova ação há cerca de dois meses" (UOL, 2021).

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

BRASIL – Ministério da Justiça e Segurança Pública. **Ministério entrega aos estados primeiras ferramentas de Big Data e Inteligência Artificial para combater a criminalidade**. 2019. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-1566331890.72. Acesso em: 10 out. 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 out. 2024.

BRASIL. **Doutrina Nacional de Inteligência de Segurança Pública (DNISP)**. 4. ed. rev. e atual. Brasília: Senasp, 2014.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação (LAI). Brasília, DF: Presidência da República, 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 10 out. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 out. 2024.

CONTROLADORIA GERAL DO ESTADO DO PARANÁ. **Cartilha de boas práticas no tratamento de dados pessoais**. Curitiba: CGE-PR, 2024. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/202402/boas%20pr%C3%A1ticas.pdf. Acesso em: 10 out. 2024.

CONTROLADORIA GERAL DO ESTADO DO PARANÁ. **Cartilha LGPD**. Curitiba: CGE-PR, 2020. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/2021-07/cartilha_LGPD.pdf. Acesso em: 10 out. 2024.

CONTROLADORIA GERAL DO ESTADO DO PARANÁ. **Manual de implementação da LGPD**: orientações e procedimentos. Curitiba: CGE-PR, 2024. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/202402/manual%20implementa%C3%A7%C3%A3o%20lgpd.pdf. Acesso em: 10 out. 2024.

CONTROLADORIA GERAL DO ESTADO DO PARANÁ. **Plano de respostas a incidentes de segurança**. Curitiba: CGE-PR, 2024. Guia. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/202402/guia%20incidentes.pdf. Acesso em: 10 out. 2024.

CONTROLADORIA GERAL DO ESTADO DO PARANÁ. **Programa estadual de integridade e compliance**. s.d. Disponível em: https://www.cge.pr.gov.br/Pagina/Programa-Estadual-de-Integridade-e-Compliance. Acesso em: 10 out. 2024.

CONTROLADORIA GERAL DO ESTADO DO PARANÁ. **Resolução nº 36, de 6 de junho de 2022**. Institui a política de privacidade de dados pessoais no âmbito da Controladoria-Geral do Estado. Curitiba, PR: CGE-R. Disponível em: https://www.cge.pr.gov.br/sites/default/arquivos_restritos/files/documento/202206/privacidadededadospessoaiscge.pdf. Acesso em: 10 out. 2024.

FREITAS, I. L. V. **A Inteligência Artificial como ferramenta para a atividade de Inteligência no combate ao terrorismo**. Rio de Janeiro: Escola de Comando e Estado Maior do Exército Escola Marechal Castello Branco, 2022. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/11878/1/MO%206702%20%20IGOR%20Leonardo%20VENTAPANE%20Freitas.pdf. Acesso em: 10 out. 2024.

MENDES, G. F.; BRANCO, P. G. G. **Curso de direito constitucional**. 7. ed. São Paulo: Saraiva, 2012.

MORAIS, L. P. de. Informação versus privacidade: quando direitos fundamentais entram em rota de colisão. **Revista Jus Navigandi**, Teresina, ano 22, n. 5125, 13 jul. 2017. Disponível em:

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

https://www.jusbrasil.com.br/artigos/informacao-versus-privacidade-quando-direitos-fundamentais-entram-em-rota-de-colisao/476189434. Acesso em: 10 out. 2024.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. [S. l.]: ONU, 1948. Disponível em: https://brasil.un.org/sites/default/files/2020-09/por.pdf. Acesso em: 10 out. 2024.

ONU – ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Pacto Internacional sobre Direitos Civis e Políticos**. [S. l.]: ONU, 1966. Disponível em: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights. Acesso em: 10 out. 2024.

ORACLE. **What is Big Data?**. [S. l.]: Oracle, s. d. Disponível em: https://www.oracle.com/big-data/what-is-big-data/. Acesso em: 10 out. 2024.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS – OEA. **Princípios atualizados sobre a privacidade e a proteção de dados pessoais**. [S. l.]: Comissão Interamericana de Direitos Humanos, 2021. Disponível em: https://www.oas.org/en/sla/iajc/docs/Publicacion_Principios_Atualizados_sobre_a_Privacidade_e_a_Protecao_de_Dados_Pessoais_2021.pdf. Acesso em: 10 out. 2024.

OSTRONOFF, L. J. **Domínio de cidades, guerra assimétrica e a privatização da segurança**. São Paulo: UFABC/NEV-USP, 2023. Disponível em: https://www.encontro2023.anpocs.org.br/arquivo/downloadpublic?q=YToyOntzOjY6InBhcmFtcyI7czozNToiYToxOntzOjEwOiJJRF9BUlFVSVZPIjtzOjQ6Ijc3NzMiO30iO3M6MToiaCI7czozMjoiZGE5N2EyZjczMDdiMTFkMDI1YTAwZGJjNTE5MmM5OTciO30%3D. Acesso em: 10 out. 2024.

PARANÁ. **Decreto Estadual nº 6.474, de 14 de dezembro de 2020**. Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), no âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo do Estado do Paraná. Curitiba, PR: Governo do Estado. Disponível em: https://www.legislacao.pr.gov.br/legislacao/pesquisarAto.do?action=exibir&codAto=244066&indice=1&totalRegistros=7&dt=10.4.2021.16.2.39.662. Acesso em: 10 out. 2024.

PARANÁ. Polícia Militar. Comando-Geral. **Portaria do Comando-Geral nº 221, de 9 de março de 2022**. Implementa o Núcleo de Integridade e Compliance Setorial (NICS) na Polícia Militar do Paraná, definindo sua estrutura e regulando suas atribuições. Curitiba: Polícia Militar, 2022.

SÃO PAULO. Tribunal de Justiça**. Ação Civil Pública nº 1010667-97.2022.8.26.0053**. 6ª Vara de Fazenda Pública. Requerente: Defensoria Pública do Estado de São Paulo. Requerido: COMPANHIA DO METROPOLITANO DE SÃO PAULO – METRÔ, 6ª Vara de Fazenda Pública, 3 mar. 2022. Disponível em: https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=1H000LRDS0000&processo.foro=53&processo.numero=1010667-97.2022.8.26.0053. Acesso em: 10 out. 2024.

SÃO PAULO. Tribunal de Justiça. **Agravo de Instrumento nº 2079077-58.2022.8.26.0000**. 5ª Câmara de Direito Público. Agravante: Companhia do Metropolitano de São Paulo – Metrô. Agravado: Defensoria Pública do Estado de São Paulo, Relator: Des. Maria Laura Tavares, 23 nov. 2023. Disponível em: https://esaj.tjsp.jus.br/cposg/show.do?processo.codigo=RI006UUYC0000. Acesso em: 10 out. 2024.

SOUSA, A. S. de; OLIVEIRA, G. S. de; ALVES, L. H. A pesquisa bibliográfica: princípios e fundamentos. **Cadernos da Fucamp**, Campinas, v. 20, n. 43, p. 64-83, 2021. Disponível em: https://revistas.fucamp.edu.br/index.php/cadernos/article/view/2336/1441. Acesso em: 10 out. 2024.

UNIÃO EUROPEIA. **General Data Protection Regulation (GDPR)**. [S. l.]: União Europeia-UE, 2018. Disponível em: https://gdpr.eu/tag/gdpr/. Acesso em: 10 out. 2024.

RECIMA21 - REVISTA CIENTÍFICA MULTIDISCIPLINAR
ISSN 2675-6218

UNIVERSO ONLINE – UOL. PR: Grupo de ação em Três Barras já tinha assaltado bancos em 3 municípios. **Universo Online – UOL**, 2021. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2021/11/05/quadrilha-que-assaltou-banco-no-parana-era-monitorada-ha-3-meses.htm. Acesso em: 10 out. 2024.