ARTIGO

AS NOVAS TECNOLOGIAS E A SEGURANÇA PÚBLICA: UM CASAMENTO COMPLEXO E PROMISSOR

Recebido em: 15/05/2023
Aceito em: 13/06/2023

Bruno de Lima Silva[1]
Marcio Luiz da Costa Limeira[2]

RESUMO: A segurança pública é um tema de relevância internacional e, no Brasil, é um direito garantido pela Constituição Federal de 1988. Por isso, os gestores da área buscam constantemente alternativas para controlar e combater a criminalidade, tornando as atividades policiais mais eficazes. Este artigo tem como propósito analisar a viabilidade da utilização de alguns tipos de novas tecnologias na segurança pública, com ênfase nos impactos no controle da criminalidade. A pesquisa emprega o método dedutivo, incluindo uma análise descritiva e uma revisão bibliográfica de fontes nacionais e estrangeiras. Observa-se no Brasil diversas iniciativas, tanto em âmbito federal quanto estadual, relacionadas ao uso de novas tecnologias, como o videomonitoramento e sistemas de identificação de veículos. No entanto, a implementação de Inteligência Artificial (IA) e Big Data mostra-se desafiadora em escala nacional. O país enfrenta um grande obstáculo ao buscar a colaboração entre a União e os Estados para a criação de bancos de dados de alcance nacional, visando a mineração, análise e perfilamento de informações. Em relação às pesquisas sobre policiamento preditivo/inteligente, nota-se que esse tema ainda é incipiente no Brasil. De acordo com dados da Coordenação de Aperfeiçoamento de Pessoal de

1 Capitão da Brigada Militar. Mestre em Direito Público pela UNISNOS. Especialista em Direito Penal e Processo Penal pela FMP/RS. Bacharel em Direito pela FEEVALE.

2 Major da Brigada Militar. Mestre em Administração/Pesquisa Operacional pela UFRGS. Especialista Segurança Pública pela PUCRS, em Direito do Estado pela UNIRITTER e Gestão Pública pela UERGS. Bacharel em Direito pela UFRGS.

Nível Superior (CAPES), foram encontradas apenas quatro pesquisas específicas sobre o assunto. Foi constatado que as novas tecnologias oferecem diversas vantagens para o trabalho policial, porém, é crucial considerar pontos sensíveis, especialmente no que diz respeito à Lei de Proteção de Dados Pessoais e aos conceitos de intimidade e privacidade. Entretanto, ainda há um longo caminho a percorrer, exigindo uma cooperação nacional para investimentos em recursos humanos, materiais e tecnológicos. Somente assim será possível extrair o melhor resultado das novas tecnologias na segurança pública, promovendo o bem-estar social dos brasileiros.

Palavras-chave: Dados. Novas Tecnologias. Policiamento Preditivo. Segurança Pública.

ABSTRACT: Public security is an internationally relevant issue, and in Brazil, it is a right guaranteed by the Federal Constitution of 1988. Therefore, professionals in the field constantly seek alternatives to control and combat crime, making police activities more effective. This article aims to analyze the feasibility of using certain types of new technologies in public security, with an emphasis on their impact on crime control. The research employs the deductive method, including a descriptive analysis and a bibliographic review of both national and foreign sources. In Brazil, various initiatives related to the use of new technologies, such as video monitoring and vehicle identification systems, can be observed at both federal and state levels. However, the implementation of Artificial Intelligence (AI) and Big Data proves to be challenging on a national scale. The country faces a significant obstacle in seeking collaboration between the Union and the States for the creation of nationally scoped databases, aiming for the mining, analysis, and profiling of information. Regarding research on predictive policing, it is noted that this topic is still in its early stages in

Brazil. According to data from the Coordination for the Improvement of Higher Education Personnel (CAPES), only four specific studies on the subject were found. It was found that new technologies offer several advantages for police work; however, it is crucial to consider sensitive points, especially regarding the Personal Data Protection Law and the concepts of intimacy and privacy. However, there is still a long way to go, requiring national cooperation for investments in human, material, and technological resources. Only then will it be possible to extract the best results from new technologies in public security, promoting the social well-being of Brazilians.

Keywords: Data. New Technologies. Predictive Policing. Public Safety.

INTRODUÇÃO

A sociedade atual tem testemunhado avanços tecnológicos que têm transformado significativamente a forma como vivemos, interagimos e nos organizamos. Essas inovações também têm impactado diretamente a segurança pública, proporcionando às forças de ordem novas ferramentas para combater a criminalidade e proteger os cidadãos. No entanto, esse casamento entre novas tecnologias e segurança pública também traz consigo desafios complexos e preocupações éticas que precisam ser abordados com responsabilidade.

Uma das principais áreas em que as novas tecnologias têm revolucionado a segurança pública é a coleta e análise de dados. Com o crescimento exponencial do armazenamento de informações e o avanço das técnicas de análise de dados, as forças policiais agora têm acesso a uma quantidade impressionante de dados que podem ser usados para prever e prevenir crimes. Por meio do uso de algoritmos e aprendizado de máquina, é possível identificar padrões criminais

e comportamentos suspeitos, direcionando recursos de forma mais eficiente e antecipando potenciais ameaças.

Outra tecnologia emergente com grande potencial para a segurança pública é a Internet das Coisas. Com a interconexão de dispositivos e sistemas, é possível monitorar e controlar espaços urbanos, viabilizando uma melhor resposta a incidentes. Sensores inteligentes podem detectar atividades criminosas, incêndios, vazamentos de gás e outros eventos perigosos em tempo real, permitindo uma ação rápida e precisa por parte das autoridades.

A utilização de câmeras de vigilância também está se tornando cada vez mais comum nas cidades. A tecnologia de reconhecimento facial, por exemplo, pode auxiliar na identificação de suspeitos e na localização de pessoas desaparecidas. No entanto, esse uso intensivo de câmeras também levanta preocupações relacionadas à privacidade e à possível vigilância excessiva por parte do Estado.

Além disso, as redes sociais e a internet em geral têm desempenhado um papel importante na segurança pública. Plataformas online podem ser usadas para disseminar informações em tempo real, alertando a população sobre eventos perigosos e possibilitando uma maior cooperação entre cidadãos e as forças policiais. No entanto, essas mesmas plataformas também podem ser utilizadas para disseminar fake news, espalhar pânico e até mesmo coordenar atividades criminosas.

Apesar de todos esses avanços tecnológicos oferecerem inúmeras vantagens para a segurança pública, é crucial lembrar que a implementação dessas tecnologias deve ser feita com responsabilidade e consideração ética. A privacidade dos cidadãos precisa ser preservada, garantindo que as informações coletadas sejam usadas de forma ética e que os algoritmos não perpetuem vieses ou discriminações existentes.

Assim, o objetivo do presente artigo é analisar a possibilidade de uso de novas tecnologias na área da segurança pública, especialmente,

os impactos no controle da criminalidade. Para tanto a pesquisa utiliza-se do método dedutivo, com análise descritiva e revisão bibliográfica nacional e estrangeira.

OS DADOS E SUA IMPORTÂNCIA PARA A SEGURANÇA PÚBLICA NO CONTROLE DA VIOLÊNCIA – ASPECTOS LEGAIS

No mundo atual os "dados"[3] são a nova riqueza mundial. A internet e as tecnologias digitais já são uma parte inextricável de nossas vidas, transformando a maneira como nos comunicamos, trabalhamos e interagimos com o mundo ao nosso redor. Nessa linha de raciocino surge uma grande rede de múltiplas interações simultâneas a nível global.

A partir da década de 1990, com o advento da internet, surgiram as redes digitais que viabilizaram a disseminação contínua e instantânea de informações, estabelecendo uma hiperconexão entre os usuários. As tecnologias digitais, com foco especial em computadores, software e redes, promoveram uma transformação radical na sociedade e no cenário global de mercado (Schwab, 2016, p. 16-17). O sociólogo Manuel Castells, especialista no estudo da internet, ciberespaço e redes sociais, argumenta que as tecnologias digitais colocam a sociedade global em outro nível de integração através do conceito de "sociedade em rede". Assim explica o autor

> As redes constituem a nova morfologia das sociedades e a difusão da sua lógica modifica substancialmente as operações e os resultados

3 Do latim, data é o plural de datum. Historicamente e em áreas científicas especializadas, termo data, em inglês, é tratado como plural, tend um verbo correspondente no plural, como na frase: "dados fora coletados e classificados". Em se tratando, no entanto de uso moderno não científico, data geralmente não é empregado como um termo plural. Em vez disso, é tratado como um substantivo incontável (mass noun ou uncountable noun), semelhante a uma palavra como informação, levando um verbo correspondente no singular. (EMIDÃO, R. A. M. 2014, p. 71). Já conforme a Lei 13.709/2018 no seu art. 5º **dado pessoal** é considerado "informação relacionada a pessoa natural identificada ou identificável".

> dos processos de produção, experiência, poder e cultura. Embora a organização social, sob a forma de rede, tenha existido noutros tempos e lugares, o novo paradigma da tecnologia da informação fornece as bases materiais para a expansão da sua penetrabilidade em toda a estrutura social (Castells, 2002, p. 607).

A "sociedade em rede" engloba um vasto mundo de interações que abrangem tanto o espaço físico quanto o virtual em todos os aspectos da vida humana, abarcando as áreas da economia, política, lazer, trabalho e social. Essa nova forma de interação por meio das redes provocou dois desafios significativos: a soberania e a liberdade. Assim, nesse novo cenário interativo, inúmeros comportamentos escapam ao controle dos Estados, cuja autoridade tradicionalmente se baseia no conceito territorial. No entanto, para que os Estados estabeleçam novos mecanismos regulatórios, torna-se imperativo compartilhar seu poder (Castells, 2003, p. 145 e 152).

Klaus Schwab (2016, p. 12-13) explica que a Quarta Revolução Industrial, tendo como produto principal determinadas tecnológicas, como: nanotecnologias, a realidade mista (RM), inteligência artificial (IA) e a computação quântica (CQ), biotecnologias, robótica. Essa revolução tem as características: velocidade, impacto sistêmico, amplitude e profundidade.

A nova revolução tecnológica, conforme Schwab (2016) é marcada por três características: velocidade, amplitude/profundidade, e impacto sistêmico. A velocidade é o motor que impulsiona o ritmo exponencial desta revolução, a qual é o "produto de um mundo multifacetado e profundamente interconectado em que vivemos". A amplitude e a profundidade estão intrinsecamente ligadas às transformações na sociedade, nos indivíduos, na economia e nos negócios, tendo como alicerce a revolução digital. No que tange ao impacto sistêmico, esta revolução reconfigura os "sistemas completos entre países e dentro deles, em empresas, indústrias e em toda a sociedade". Deste modo as novas tecnologias prometem/oferecem

infinitas possiblidade de atuação em todas áreas da vida humana, porém existe uma grande incerteza sobre seus riscos e consequências. (Schwab, 2016, p. 12-13).

Quanto ao tema, Stefano Rodotá (2007, p. 66) aponta que a

> "sociedade da informação se especifica, portanto, como 'sociedade dos serviços', com elevada padronização e crescentes vínculos internacionais. Disso decorrem duas consequências: quanto mais os serviços são tecnologicamente sofisticados, mais o indivíduo deixa nas mãos do fornecedor do serviço uma cota relevante de informações pessoais; quanto mais a rede de serviços se alarga, mais crescem as possibilidades de interconexões entre bancos de dados e disseminação internacional das informações coletadas".

Nessa mesma linha de raciocino, Lemos explica que da invasão à garantia do direito à privacidade e à segurança dos dados pessoais, questiona-se quais são os elementos que verdadeiramente representam uma ameaça à liberdade. Segundo o autor, no século XIX, a resposta residia na Lei. No entanto, o autor acrescenta que, no cenário tecnológico contemporâneo, a Lei deixou de ser o único componente que influencia a restrição ou a adaptação da liberdade dos indivíduos, e até mesmo a regulação da sociedade em rede (Lemos, 2005, p.22).

Neste sentido, essa revolução tecnológica trouxe inúmeros avanços em muitas áreas, porém no mesmo ritmo surgiram preocupações crescentes sobre a privacidade e a segurança dos dados pessoais dos indivíduos. Para abordar essas questões, governos de diferentes países têm promulgado leis de proteção de dados, garantindo que as informações pessoais sejam tratadas com respeito e responsabilidade.

A Europa conta com uma construção histórica de mais de cinco décadas, sobre a proteção de dados pessoais, uma evolução gradativa sobre a privacidade, tratamento de dados e transparência. O primeiro dispositivo da Lei do Land de Hesse em 1970, com uma enorme evolução, o Brasil tem a Lei nº 13.709, de 14/08/2018 conhecida

como Lei Geral de Proteção de Dados, LGPD, com a entrada em vigor protraída. É importante registrar a PEC 17/2019, que pretende assegurar o status constitucional à proteção dos dados pessoais (Limberger, 2020, p. 162).

A Europa passou por três etapas no que diz respeito à proteção de dados: a primeira envolveu a introdução da legislação para proteção de dados, exemplificada pela promulgação das primeiras leis, como a do Estado de Hesse, na Alemanha. A segunda fase incluiu a criação de agências de proteção de dados, como a Lei francesa de 1978. A última fase, ocorrida na década de 1990, foi marcada pela implementação de uma legislação unificada. Nesse contexto, surgiu a Diretiva Comunitária 95/46, que estabeleceu diretrizes para a proteção de dados em toda a comunidade europeia (Limberger, 2007, p.79).

Dessa forma, podemos observar a evolução da legislação de proteção de dados na União Europeia. Inicialmente, a Diretiva Comunitária 95/46 estabeleceu as bases para a proteção de dados em toda a comunidade. Em seguida, a Carta Europeia reconheceu o direito à proteção de dados de forma independente, no artigo 8º, desvinculando-o da privacidade mencionada no artigo 7º. Mais recentemente, o Regulamento Geral de Proteção de Dados (RGPD) fortaleceu ainda mais essas diretrizes na Europa, introduzindo inovações significativas. Entre essas inovações, destacam-se as ênfases na prevenção e transparência, conforme estabelecido nos artigos 51 a 59 do RGPD (Limberger, 2019. p. 551-567).

Na perspectiva europeia, a privacidade assume um novo perfil, representando o direito de ter controle sobre nossas informações e de determinar como construímos nossa esfera pessoal - o direito à autodeterminação informativa. Isso é de imensa importância na sociedade da informação, onde a informação é um recurso valioso por si só, uma parte essencial da vida humana. Anteriormente, as informações pessoais eram mantidas sob o domínio dos interessados.

Agora, vivemos em um cenário de informações compartilhadas com uma variedade de indivíduos. O que antes era uma troca de informações através de relações interpessoais (na era da "fofoca") evoluiu para a coleta de dados por meio de transações abstratas (Peixoto, 2018, p. 43).

Passamos de um mundo onde a preocupação se concentrava na divulgação de informações do âmbito privado para um mundo onde o controle sobre as informações que entram se torna cada vez mais crucial. Estamos imersos em uma era em que as tecnologias da informação e comunicação desempenham um papel semelhante ao das "tecnologias poluentes" industriais. Estas tecnologias, por sua vez, contribuíram para a crescente indistinção entre o que é público e o que é privado (Peixoto, 2018, p. 43).

Nos últimos muitos escândalos públicos de nível mundial, chamaram a atenção para a privacidade e governança de dados. Em 2018, os jornais The New York Times dos Estados Unidos e o The Guardian do Reino Unido, veiculara reportagens revelando o vazamento de informações pessoais pela plataforma social Facebook. Havia suspeitas de que isso tivesse influenciado o desfecho das eleições presidenciais de 2016 nos Estados Unidos. A coleta desses dados foi realizada pela empresa Cambridge Analytica, por meio da utilização de aplicativos de avaliação psicológica. A divulgação dessas informações foi realizada por um ex-membro da equipe da referida empresa.

No Brasil, a construção histórica sobre a proteção de dados é bem diferente do que ocorreu na Europa. Um marco importante é a promulgação da Constituição Federal de 1988, a qual garantiu de forma extensiva a proteção ao direito à privacidade e a intimidade, já que o legislador optou em utilizar as expressões vida privada e intimidade, do que privacidade, também não trouxe nenhum conceito para esses dois termos.

Deste modo o art. 5º define que "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". Da mesma forma o inciso XII que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei penal estabelecer para fins de investigação criminal ou instrução processual pena.

Ainda, com relação a proteção constitucional sobre o direito à privacidade e intimidade, pontua o Ministro do Supremo Tribunal Federal Dias Toffoli que, segundo essa normativa, a preservação dos dados pessoais assume a natureza de um direito fundamental. O habeas data, um dispositivo originalmente presente na Constituição, já antecipava, em seus primeiros indícios, a ideia de autonomia informacional do cidadão. Ele garantia, mesmo ao se referir apenas aos registros e aos bancos de dados de entidades governamentais ou de caráter público, que as informações relacionadas ao indivíduo devem estar ao seu alcance (art. 5º, inciso LXXII, a) e ser precisas, podendo ser corrigidas quando necessário (Brasil, 2021, p.45).

Esse rol de direito em relação direta com o conceito de personalidade, sendo que para Maria Helena Diniz (2005, p. 121)

> A personalidade não é um direito, de modo que seria errôneo afirmar que o ser humano tem direito à personalidade. A personalidade é que apoia os direitos e deveres que dela irradiam, é objeto de direito, é o primeiro bem da pessoa, que lhe pertence como primeira utilidade, para que ela possa ser o que é, para sobreviver e se adaptar às condições do ambiente em que se encontra, servindo-lhe de critério para aferir, adquirir e ordenar outros bens.

Portanto, o direito à privacidade e intimidade, são oriundos da própria personalidade humana, ao ponto que na atual sociedade de rede, esse direito pode ser de prestações negativas ou positivas. Para Tatiana Malta Vieira (2007, p. 99) o

> direito à privacidade, na dimensão de uma prestação positiva por parte do Estado, também impõe o debate sobre medidas de segurança a respeito de dados que incidam diretamente na esfera privada dos indivíduos, assumindo caráter preventivo, a fim de se evitar acessos não autorizados a essas informações. A privacidade, nesta dimensão, impõe a "salvaguarda das informações pessoais armazenadas tanto pelo setor público como pelo privado", o que demanda procedimentos aperfeiçoados e atualizados, diante da "constante evolução das tecnologias utilizadas para a coleta, arquivamento, transmissão e interconexão de dados".

O Código Civil de 2002 trouxe algumas inovações quanto a proteção do direito à privacidade e intimidade no bojo do capítulo II "Dos Direitos da Personalidade"[4]. No art. 11 temos a seguinte redação "Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária". Bem como no art. 21 "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma". Para Orlando Gomes Orlando Gomes (1996, p. 130)

> Sob a denominação de direitos da personalidade, compreendem-se os direitos personalíssimos e os direitos essenciais ao desenvolvimento da pessoa humana que a doutrina moderna preconiza e disciplina no corpo do Código Civil como direitos absolutos, desprovidos, porém, da faculdade de disposição. Destinam-se a resguardar a eminente dignidade da pessoa humana, preservando-a dos atentados que pode sofrer por parte dos outros indivíduos.

No ano de 2014, foi promulgada o Marco Civil da Internet, através da Lei Lei nº 12.965, de 23 de abril de 2014[5]. A mencionada

4 Os direitos de personalidade representam garantias constitucionais dos próprios direitos humanos. Gustavo Tepedino (1999, p. 50), leciona que a tutela da personalidade "não pode se conter em setores estanques, de um lado os direitos humanos e de outro as chamadas situações jurídicas de direito privado".

5 De forma complementar a refira lei a União elaboro o decreto 8.771/16 o qual tinha 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

lei estabelece os princípios que orientam a utilização da internet no Brasil, os quais são listados no artigo 3º. Dentre estes, destaca-se o princípio da preservação da privacidade e dos dados pessoais. Ademais, no artigo 7º, são garantidos aos usuários de internet os direitos à inviolabilidade e confidencialidade do tráfego de suas comunicações, bem como à inviolabilidade e confidencialidade das suas comunicações privadas armazenadas, exceto mediante ordem judicial.

O artigo 10º, parágrafo 1º, aborda de maneira específica a proteção dos registros, dados pessoais e comunicações privadas, deixando claro que é possível fornecer dados privados quando solicitados por decisão de um juiz. Além disso, estipula que o responsável pela custódia dos dados é obrigado a disponibilizá-los em caso de requisição judicial.

Em 2018, entrou em vigor a aguardada "Lei de Proteção de Dados Pessoais" (ou LGPD), revogando totalmente o marco civil da internet, cujo propósito é regulamentar o manejo de informações pessoais e estabelecer diretrizes claras para as empresas e instituições que lidam com dados de cidadãos brasileiros. A segurança dos dados pessoais é sempre essencial, especialmente quando se trata de informações sensíveis. É crucial reforçar essa proteção, uma vez que tais dados têm o potencial de gerar situações discriminatórias, o que vai de encontro ao princípio constitucional da igualdade (Limberger, 2007, p.60).

A LGPD marca um importante avanço no âmbito legal do país, proporcionando aos cidadãos um maior controle sobre suas informações e assegurando que seus dados pessoais sejam processados de maneira transparente e segura. Esta legislação abrange um amplo espectro de entidades, incluindo empresas privadas, órgãos governamentais e organizações sem fins lucrativos, impondo a todos

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.

eles a responsabilidade de resguardar os dados pessoais que coletam, armazenam e processam.

A LGPD incorpora diversos aspectos cruciais, entre os quais se destacam: 1. Consentimento explícito (Capitulo II): Agora, as empresas são obrigadas a obter o consentimento expresso dos titulares dos dados antes de coletar qualquer informação pessoal. Esse consentimento deve ser claro, específico e informado, assegurando que os indivíduos tenham pleno conhecimento de como suas informações serão utilizadas; 2. Direitos dos titulares dos dados (Capitulo III): A legislação garante aos cidadãos uma série de direitos sobre seus dados pessoais, tais como o acesso às informações coletadas, a correção de dados imprecisos, a exclusão de informações desnecessárias e a possibilidade de transferir os dados para outros serviços, se assim desejarem; 3. Segurança e proteção de dados (Capitulo IV): A LGPD exige que as organizações implementem medidas de segurança robustas para resguardar os dados pessoais contra acessos não autorizados, vazamentos ou uso indevido; 4. Transferência internacional de dados (Capitulo V): A lei regula a transferência de dados pessoais para países estrangeiros, assegurando que as normas de proteção de dados sejam mantidas mesmo fora das fronteiras nacionais. 5. Responsabilidade e prestação de contas (Capitulo VI): As organizações devem ser transparentes quanto às suas práticas de tratamento de dados e estar prontas para prestar contas em caso de violação da lei.

No ano de 2020 o Executivo Federal elaborou a Medida Provisória nº 954/2020, a qual previa que as empresas que prestam serviços de telefonia fixa e móvel deveriam fornecer ao Instituto Brasileiro de Geografia e Estatística (IBGE) informações relativas aos nomes, números de telefone e endereços de seus clientes, sejam eles indivíduos ou empresas. De acordo com o Executivo, essa norma foi solicitada pelo próprio IBGE com o objetivo de garantir a continuidade de pesquisas que anteriormente eram realizadas por

meio de visitas domiciliares. Essas visitas não podem mais ocorrer devido à pandemia de COVID-19.

Em razão dessa situação, foram propostas ações diretas de inconstitucionalidade (ADIs 6387 – CFOAB; ADI 6388- PSDB; ADI 6389- PSB; ADI 6390 – PSOL e ADI 6393 – PCB). O plenário, em uma sessão realizada por videoconferência, decidiu suspender os efeitos da medida provisória MP 954/2020. Essa MP previa o compartilhamento de informações de usuários de serviços de telecomunicações com o IBGE para a produção de estatísticas oficiais durante a pandemia do novo coronavírus. Por maioria de votos, as medidas cautelares deferidas pela Ministra Rosa Weber em cinco ADIs foram confirmadas para estabelecer que o compartilhamento previsto na MP viola o direito constitucional à intimidade, à vida privada e ao sigilo dos dados. Os argumentos determinantes para a concessão da tutela nessa ação foram: a) a falta de limitação quanto ao escopo da estatística a ser produzida, bem como sua finalidade específica e amplitude; b) o legítimo interesse público no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, levando em conta a necessidade, a adequação e a proporcionalidade da medida; c) a ausência de um mecanismo técnico ou administrativo capaz de proteger os dados pessoais contra acessos não autorizados, vazamentos acidentais ou uso indevido, tanto durante sua transmissão quanto em seu processamento. Essa decisão foi proferida em 17/04/2020 e posteriormente confirmada em plenário em 07/05/2020 (Limberger, 2020, p. 163-164).

O Regulamento Geral de Proteção de Dados (RGPD) consagra o direito fundamental à proteção de dados, conforme estabelecido no artigo 8º da Carta Europeia de Direitos Humanos. Este regulamento se aplica a entidades que possuem um sistema automatizado contendo informações pessoais. No que diz respeito à sua abrangência territorial, o RGPD é válido não apenas dentro da União Europeia, mas também em outros países, mesmo que não sejam membros comunitários.

Isso ocorre quando, devido a alguma relação legal ou comercial, os dados de cidadãos ou empresas estabelecidas na União Europeia são afetados (Limberger, 2018, p. 216).

Dessa forma, o princípio da segurança jurídica é aplicável além das fronteiras europeias, considerando que os dados circulam livremente, sem se limitar às fronteiras nacionais. Outro aspecto crucial diz respeito ao consentimento do indivíduo, conforme estabelecido no artigo 4.11 do RGPD. Ele é definido como toda manifestação de vontade que seja livre, específica, informada e inequívoca, pela qual o indivíduo aceita, seja por meio de uma declaração ou de uma ação claramente afirmativa, o tratamento de dados pessoais relacionados a si (Limberger, 2018, p. 216).

Atualmente, vivemos em um período em que tanto interesses coletivos quanto individuais muitas vezes resultam na violação constante da privacidade dos cidadãos. Ao mesmo tempo, o comportamento singular de cada pessoa dificulta a preservação de uma noção geral de respeito à privacidade. Contudo, sublinhar a importância do direito à privacidade, seja de que forma for expresso, equivale a enaltecer a liberdade, lutar contra a discriminação e salvaguardar as decisões pessoais de cada indivíduo. O respeito pela privacidade é um pilar essencial do exercício da cidadania (CANCELIER, 2017, p. 230).

Deste modo, a sociedade em rede traz consigo uma variedade de implicações relacionadas à governança e à salvaguarda dos dados. Os potenciais perigos do "uso indevido" e da divulgação de informações pessoais são abundantes, contudo, as inovadoras tecnologias de manipulação desses dados também podem proporcionar inúmeras vantagens em diversos aspectos da vida em comunidade. A Segurança Pública é um desses domínios.

NOVAS TECNOLOGIAS: POSSIBILIDADES PARA O FUTURO DA ATUAÇÃO POLICIAL

Na sociedade atual, a Segurança Pública enfrenta muitos desafios, sendo que o avanço tecnológico promete fortalecer a eficiência e a capacidade de resposta das forças policiais. Novidades como o uso de Big Data, inteligência artificial, câmeras de monitoramento, drones, aplicativos moveis e algoritmos voltamos para as necessidades dos órgãos policias são as novas ferramentas para a prevenção de crimes. Ao ponto que nesse capítulo será feira uma análise sobre algumas dessas tecnologias e sua aplicação da Segurança Pública.

BIG DATA

A mineração de dados, um campo da Ciência da Computação que teve seu início por volta de 1980, inicialmente surgiu como uma ferramenta destinada à análise dos dados acumulados por grandes empresas e organizações durante suas operações, resultando em um acúmulo massivo de informações. A análise desses conjuntos de dados poderia revelar informações não aparentes, as quais, uma vez descobertas, poderiam otimizar e potencializar o desempenho da organização. Hoje em dia, com o aumento do fluxo de dados entre computadores, celulares e dispositivos intermediários como tablets, a mineração de dados é amplamente utilizada como técnica para a análise automática de informações e geração de conhecimento. Como o próprio termo sugere, trata-se de extrair os insights contidos nos dados (Serbena,2013, p. 53).

O termo Big Data surgiu no século XXI e teve origem entre astrônomos e geneticistas. Foi cunhado para abordar novas maneiras e ferramentas de analisar grandes conjuntos de dados, devido à limitação da capacidade de memória dos computadores até então, que não permitia o armazenamento de toda a quantidade de informações disponíveis. A expressão "Big Data" é bastante abrangente, muitas

vezes vaga e imprecisa, e pode ser interpretada de diversas maneiras. É frequentemente utilizada em uma variedade de campos de conhecimento e setores da sociedade (Gomes, 2019, p. 23-24).

Atualmente, com o crescimento exponencial de indivíduos e dispositivos conectados à internet, houve um aumento significativo na quantidade de informações geradas e armazenadas diariamente. A prática de capturar, armazenar e analisar dados não é uma novidade na história da humanidade, mas tem evoluído ao longo do progresso tecnológico. Esse ambiente propício para a formação de bases de dados abre espaço para as grandes empresas de tecnologia, conhecidas como Big Techs, cujo principal produto é a utilização do Big Data.

As tecnologias de Big Data estão associadas a conjuntos de dados de grande escala, caracterizados por sua complexidade, diversidade e falta de organização. Esses conjuntos de dados são tão vastos que as técnicas computacionais tradicionais não são adequadas para lidar com seu armazenamento, processamento, compartilhamento e preservação. De fato, eles são tão massivos que não podem ser manipulados por um único computador (Semeler, 2019, p. 115).

O uso do Big Data na área de prevenção e controle na segurança pública é notável. Ele é empregado para analisar de maneira abrangente as dimensões quantitativas do crime, os detalhes temporais e espaciais em que ocorrem, bem como possíveis padrões de evolução ao longo do tempo. Alguns estudiosos têm referido a esse domínio como "big data criminal", cuja importância se destaca principalmente por meio de abordagens inovadoras na prevenção de delitos (Cai; Wang,2020, p.02).

No âmbito internacional, diversos departamentos de polícia nos Estados Unidos têm adotado estratégias de análise de big data para examinar o histórico de crimes passados. Por exemplo, a polícia de Santa Cruz, na Califórnia, tem empregado essa abordagem para identificar tendências e padrões recorrentes ao longo do tempo. Da

mesma forma, em estados como Maryland, tecnologias preditivas são utilizadas para avaliar a probabilidade de reincidência de infratores e para a revisão de liberdade condicional, sendo aplicadas pelos sistemas de justiça. Outro exemplo nos Estados Unidos é o caso da polícia da Carolina do Sul, que recorreu a ferramentas de análise de dados fornecidas pela IBM para examinar padrões de crimes e identificar pontos críticos, visando aprimorar a eficácia das operações policiais. O departamento de polícia de Los Angeles, por sua vez, estabeleceu parcerias com instituições de pesquisa para desenvolver sistemas e softwares capazes de prever áreas de alto risco para a ocorrência de crimes (Amaral, 2023, p. 23)

Na China, o cenário é semelhante. A análise criminal com o uso de big data, conhecida como "policiamento da informação", tem se consolidado como um suporte crucial na região para a prevenção e o controle social na segurança pública. Um exemplo notável é o Departamento de Segurança Pública da polícia de Shandong, onde a implementação da plataforma em nuvem possibilitou a coleta de impressionantes 36,9 bilhões de dados em 2016, totalizando dez petabytes de informação armazenada (Cai; Wang, 2020, p.03).

Dessa forma o Big Data deve servir para facilitar a análise de informações e padrões criminais para realizar a prevenção de delitos, nas palavras de Manning (2003, p. 378)

> Na medida em que a polícia é dependente de informação e precisa confiar no público como sua fonte principal de fornecimento, as formas como a polícia processa, codifica, decodifica e usa a informação são críticas para a compreensão de seu mandato e função. A polícia junta diversos tipos de informações e as usa para diferentes fins, orientando-se por suposições, baseadas no senso comum, a respeito de seu trabalho, de sua atuação principal, e nas expectativas de seu público. A polícia junta informações primárias, ou dados "crus", que então são processadas, no policiamento, para resolver crimes ou encerrar eventos, transformando-se em informações secundárias. Quando processadas duas vezes, juntadas e formatadas, elas podem avançar na organização e tornar-se informações terciárias ou "diretivas". Essas formas da informação e inteligência (informações

> coletadas para antecipar acontecimentos, ao invés de coletadas em resposta a um evento em curso) são percebidas e interagem com as estratégias operacionais da polícia (a alocação de recursos para obter um final preventivo, prospectivo ou reativo).

Então, fontes de dados para a polícia podem ser: informações derivadas de transações econômicas facilitadas por sistemas computacionais; informações obtidas através de dispositivos e locais interconectados à internet, como: a Internet das Coisas (IOT), drones, veículos automatizados, inteligência artificial, repositórios de dados governamentais e empresariais. Também sistemas de vigilância públicos e privados, dispositivos móveis, satélites, e-mail, compras, pesquisas no Google e interações em qualquer tipo de redes sociais como o Facebook (Zuboff, 2017, p. 17-68).

No que diz respeito à implementação da tecnologia de Inteligência Artificial para reconhecimento facial como parte das políticas públicas no Brasil, foram identificados planos e projetos desde os anos 2000. Foi observada uma crescente ênfase na formulação de políticas públicas relacionadas a essa tecnologia, culminando na primeira menção ao reconhecimento facial através de IA no Plano Nacional de Segurança Pública 2018-2028, com o propósito de fiscalização em fronteiras, portos e aeroportos. O estudo também evidenciou um aumento significativo na elaboração de políticas públicas de caráter tecnológico, especialmente após a disponibilização de editais por parte de financiadoras públicas a partir de 2012 (Nascimento Pinheiro Vargas; Matos Ribeiro, 2023, p.19).

No ano de 2019 o Brasil ingressa no uso do Big Data em nível nacional. Com um investimento de R$ 32 milhões de reais, em quatro anos, foram lançados pelo Ministério da Justiça quatro programas governamentais: Sinesp Big Data[6], o Sinesp GeoInteligência[7], o

6 Base dos sistemas da Sinesp, com tecnologias e soluções para execução em larga escala.

7 Georreferenciamento das ocorrências em relação ao tempo e o espaço em que registrada. Será possível, por exemplo, visualizar rotas de policiamento e mapas de

Sinesp Tempo Real[8] e o Big Data Busca[9], introduzidos por meio do "Em Frente Brasil", projeto piloto elaborado para o combate à criminalidade, no Espírito Santo, em Goiás, no Pará, no Paraná e em Pernambuco (Brasil, 2019). Porém, no ano de 2020 eclodiu a pandemia da COVID-19, fenômeno global que impacto diretamente em diversas políticas públicas do Brasil, onde todos os esforços foram feitos para conter a propagação da doença e reforçar a estrutura do sistema de saúde, retardando metas e ações de outras áreas. Igualmente, todos esses programas ainda não entregaram resultados palpáveis.

O quadro 1 abaixo apresenta de forma resumida a área, fonte de dados e técnicas para o tratamento de dados, para comercialização, perfilamento ou agregar valor aos dados.

Quadro 1 – Tratamento de Dados (Fontes e Técnicas)

ÁREA	FONTE DE DADOS	TÉCNICA
Análise/ mineração de textos.	Redes sociais, e-mails, blogs, fóruns on-line, questionários, relatórios, notícias, registros de *call centers.*	*Text summarization, question answering, sentiment analysis.*
Análise de áudio.	Dados de *call centers*, área da saúde.	*Automatic-speech recognition, phonetic-indexing, search.*
Análise de conteúdo de vídeo.	Vídeos de segurança – circuitos internos; geração descentralizada de vídeos – YouTube.	*Server-based/edge-based architecture.*
Análise de redes sociais.	Redes sociais, blogs, microblogs, social, compartilhamento de mídias, sites de respostas/perguntas, wikis.	*Content-based analytics, structure-based analytics – community detection, social influence analysis, link prediction.*

Fonte: Silva Neto; BonacellI; Pacheco, 2021. p.08.

calor com os locais onde mais acontecem crimes e em quais horários.

8 Monitoramento inteligente para rápida intervenção, acompanhamento de ocorrências criminais, detecção por sensores, câmeras de segurança, viaturas e agentes e pessoas com restrição de liberdade que fazem uso de tornozeleiras eletrônicas.

9 Permitirá a busca de informações em boletins de ocorrência de outros estados e municípios, além de pesquisas a dados de pessoas, objetos e documentos.

Assim, um grande desafio no Brasil está relacionado aos bancos de dados. Não existe uma base de dados nacional consolidada e os bancos de dados estaduais em operação enfrentam questões ligadas à qualidade das informações disponíveis. Portanto, dada a vastidão do Brasil, é crucial que haja uma cooperação eficaz entre o governo federal e os estados para estabelecer um banco de dados nacional de alta qualidade, viabilizando a eficaz utilização do Big Data.

INTELIGÊNCIA ARTIFICIAL (IA)

A Inteligência Artificial (IA) é um produto da Quarta Revolução Industrial, essa nova tecnologias trabalha com sistemas operacionais inteligentes, ou seja, sistemas os quais aprendem através dos dados fornecidos pelo usuário e com as experiencias na resolução de problemas concreto.

Para Klaus Schwab (2018, p. 177) a IA está atualmente revolucionando a economia digital e, em breve, irá redefinir a economia do mundo físico. A IA tem como objetivo capacitar as máquinas a navegar no mundo físico e facilitar a interação entre seres humanos e computadores. No futuro, os sistemas de IA serão capazes de lidar com desafios sistêmicos, como a redução das emissões globais de dióxido de carbono e a gestão do tráfego aéreo em escala global, abordando questões complexas que transcendem a capacidade humana. Cientistas indicam que os cenários de ficção científica com sistemas operacionais inteligentes ou assistentes digitais empáticos em breve se tornarão uma realidade.

Nos últimos anos, as pesquisas e investimento na área de IA aumentaram exponencialmente, diante do cenário de mudança grandes empresas globais como: Amazon, Facebook IBM, Google e DeepMind firmaram uma parceria para criar uma plataforma aberta sobre IA buscando beneficiar as pessoas e a sociedade (Schwab, 2018, p. 182).

Atualmente, os métodos mais prevalentes na concepção de máquinas inteligentes consistem em fornecê-las com nossos objetivos desejados e algoritmos, de modo que possam determinar maneiras de atingir tais metas. Uma alternativa seria a programação prévia de comportamentos, no entanto, isso exigiria um esforço mental considerável por parte dos humanos, desviando o foco da verdadeira finalidade da IA. Além disso, tal abordagem é simplesmente inviável, mesmo para tarefas aparentemente simples, como o jogo de xadrez (Schwab, 2018, p. 183)

No mesmo sentido, a área da segurança pública apresenta um enorme campo de atuação para os computadores e sistemas inteligentes através do uso da IA. Os cientistas mais entusiasmados acreditam que os robôs poderão realizar muitas das rotinas policiais básicas. Os sistemas de IA já são utilizados para monitorar o fluxo de informações e dados sendo capaz de emitir alertas para os agentes de segurança para padrões suspeitos.

Em 2016, a polícia de Dallas nos EUA, pela primeira vez na história, a utilizou um robô numa demonstração de força letal. A polícia utilizou um robô-bomba para colocar um dispositivo em sua extensão para que ele detonasse onde o suspeito estava, um atirador solitário o qual já havia matado cinco policiais. Outros robôs já foram implementados na policia especialmente para busca e resgate de vítimas (G1, 2016).

No Brasil, o uso da IA na segurança pública ainda é tímida. No Estado do Paraná em 2022 foi lançado o projeto piloto da "viatura inteligente". Essa viatura está equipada com quatro câmeras projetadas para identificar placas e pessoas, as câmeras de monitoramento estão nas laterais, na frente e uma com visão de 360º. A viatura está atualmente em fase de teste e será utilizada nas operações no Litoral durante o Verão Maior Paraná. O sistema das câmeras é capaz de acessar informações sobre os veículos e pessoas filmadas, como

idade e características físicas, além de emitir alertas sobre indivíduos procurados pela justiça. Além disso, registra a quantidade de pessoas e veículos identificados durante as atividades policiais. (De Freitas, 2023. p. 26944).

Nessa mesma linha o Governo do Estado do Paraná apresentou o projeto Olho Vivo, que tem como objetivo a implantação de câmeras de vigilância em 29 regiões distintas, alcançando assim 65% da população estadual. Essa tecnologia engloba uma série de avanços, incluindo o uso de reconhecimento facial para facilitar a identificação de criminosos, assim como a leitura de placas de veículos. O investimento total no projeto Olho Vivo é de R$ 42 milhões (De Freitas, 2023. p. 26944).

No Estado do Rio Grande do Sul desde o ano de 2017, foi instituído o Sistema de Segurança Integrada com os Municípios (SIM/RS) foi instituído através do Decreto Estadual nº 53.506, de 6 de abril de 2017. Esse sistema foi concebido a partir da necessidade de unir esforços entre instituições federais, estaduais e municipais, assim como a sociedade civil organizada, para combater a violência e a criminalidade no Rio Grande do Sul (Estado do Rio Grande do Sul, 2023).

O SIM se baseia em cinco pilares de integração: prevenção, operações, tecnologia, inteligência e informações, além de ressocialização e sistema penitenciário. Esse sistema permitirá ao Poder Público oferecer um serviço de segurança pública mais eficiente, otimizando tanto recursos humanos quanto materiais, e promovendo o compartilhamento de tecnologias e informações entre os municípios e o Estado (Estado do Rio Grande do Sul, 2023).

Nesse cenário de integração começaram a surgir os Centro Integrado de Operações de Segurança Pública - CIOPS. Esses centros funcionam como o ponto central para o comando e controle de todas as operações de segurança pública não apenas em Santa Maria, mas

também em vários municípios da região central do Rio Grande do Sul. Estes estão sendo conectados de forma tecnológica por meio de sistemas de monitoramento por vídeo e cercamento eletrônico.

De acordo com o termo de cooperação ao SIM/RS a Secretaria de Segurança Pública do Estado do Rio Grande do Sul, define Sistema de videomonitoramento como o: "Sistema que permite a visualização, a gravação e o compartilhamento de imagens em tempo real, obtidas pelas câmeras de vídeo integradas, mediante a utilização de softwares inteligentes" (Estado do Rio Grande do Sul, 2022, p. 03). Na mesma linha, define o Cercamento Eletrônico como: "sistema que permite a leitura de dados, por meio de câmeras de monitoramento, com a utilização de softwares inteligentes, viabilizando a pronta resposta do Estado nas intercorrências que demandem atuação da Segurança Pública e dos agentes de fiscalização" (Estado do Rio Grande do Sul, 2022, p. 03).

A ideia central é distribuir os pontos de entrada e saída do município, é possível estabelecer um sistema de "barreira virtual" ao redor da área municipal. O propósito desse uso é monitorar e regular o fluxo de veículos que entram e saem do município, permitindo a rastreabilidade de ocorrências como roubos de veículos, documentação atrasada, veículos suspeitos e uma variedade de outros tipos de acompanhamento. A eficácia desse sistema aumenta à medida que mais cidades o adotam, possibilitando um monitoramento abrangente. Um exemplo de sucesso na aplicação desse sistema ocorreu no Estado do Rio Grande do Sul, em 2019, quando a Secretaria de Segurança Pública estadual o implementou em 36 municípios e centralizou sua operação na capital (Estado do Rio Grande do Sul, 2019).

Na maioria dos estados brasileiros, existe algum tipo de sistema de vigilância ou monitoramento por vídeo. No entanto, a aplicação de Big Data e Inteligência Artificial ainda está em estágios iniciais. O ponto crucial ainda é a necessidade de integração entre os estados e o

governo federal para obter informações e criar bancos de dados que promovam a cooperação na federação. Após isso, o desafio consiste em utilizar o Big Data em conjunto com uma ferramenta de IA para tornar o trabalho da polícia mais eficaz.

CÂMERAS CORPORAIS (*BORYCAM*)

O uso de câmeras corporais (*Borycam*) não é uma inovação já que é uma realidade em diversos países do mundo como: Reino Unido, França, Itália, Alemanha, Estados Unidos da América e outros. A implementação das Câmeras Corporais pelas forças policiais teve início no Reino Unido por volta de 2005, nos condados de Devon e Cornwall, especialmente na Polícia de Plymouth.

Ao longo dos anos, novas tecnologias foram gradualmente integradas à rotina policial em vários países, visando gerar provas para futuros processos judiciais, diminuir os índices de violência e uso da força, aprimorar a eficiência e reforçar os mecanismos de controle.

No Brasil, a adoção de câmeras corporais é um fenômeno recente e raro, embora seja considerada uma estratégia promissora para diminuir a letalidade causada pelas forças policiais e reforçar a confiança da sociedade. Embora existam poucos estudos científicos sobre o assunto, eles sustentam a ideia de que a incorporação das câmeras corporais na rotina de trabalho dos policiais resulta em uma redução nos incidentes de uso excessivo de força (Maskaly, 2017, p. 675).

Atualmente no Brasil sete estados já utilizaram câmeras corporais nas policias militares sendo eles: Minas Gerais, Pará, Rio de Janeiro, Rio Grande do Norte, Rondônia, Santa Catarina e São Paulo. Outros dez estados sinalizarão que estão na fase de aquisição dos equipamentos.

A partir de 2020, a Polícia Militar do Estado de São Paulo (PMESP) adotou o Programa Olho Vivo, que inclui a incorporação

de câmeras operacionais portáteis (COP) nos uniformes dos policiais. Além da notável redução no emprego da força, a principal motivação da alta cúpula da corporação para implementar esse programa foi a expansão da capacidade operacional, o que fortalece a legitimidade perante a opinião pública e interna (Brasil, 2023, p, 12).

A PMESP atualmente emprega a câmera operacional portátil (COP) "Axon Body 3", fabricada pela empresa norte-americana Axon. Esses dispositivos são utilizados pelos policiais militares de São Paulo na região do peito. Esta disposição corporal difere de outros métodos de transporte adotados por outras forças policiais, como a fixação da COP próxima a um dos ombros ou na região da cabeça, acoplada aos acessórios (chapéus, boinas, quepes, etc.) dos uniformes policiais. Na vivência na PMESP, os agentes não possuem domínio sobre a ativação da COP, já que a gravação se desenrola de maneira contínua e sem interrupções (Brasil, 2023, p, 12).

Diante do cenário nacional existem algumas dificuldades a serem superadas para uma implementação massiva das câmeras corporais. Primeiro o custo e a forma de aquisição dos equipamentos[10], adquirir as câmeras acaba colocando um grande encargo no ente público tanto de manutenção periódica, quanto de troca dos equipamentos. Segundo a gestão das imagens produzidas e a capacidade de armazenamento dos servidores, isso está diretamente ligado à cadeia de custódia das imagens. Em terceiro lugar, é crucial avaliar o tipo de equipamento a ser empregado. Dada a natureza dinâmica das atividades policiais militares, por vezes o equipamento pode não se integrar adequadamente ao uniforme dos policiais, o que resulta em desconforto e, em alguns casos, no mau funcionamento do dispositivo.

10 No Estado de São Paulo após várias estadas da implementação do programa "Olho Vivo" o custo por câmera, considerando os custos com software, é de cerca de R$786,00 e hoje o estado conta com mais de 10 mil equipamentos, a um custo que se aproxima dos R$8.000.000 mensais e pode aumentar conforme o programa for sendo expandido até atingir todos os agentes.

Em quarto lugar, é imperativo promover uma mudança na cultura organizacional de uma parte significativa da tropa da polícia militar, que demonstra certa resistência em adotar esse tipo de equipamento.

Para tentar solucionar esses problemas a PMESP adotou a aquisição através de comodato. Também a PMESP utiliza o Sistema de Gerenciamento, Custódia e Compartilhamento de Evidências Digitais, conhecido como "Evidence". Essa plataforma digital permite a conversão dos dados coletados em informações acessíveis a diversas partes interessadas, tanto dentro da PMESP (incluindo supervisores operacionais, educação policial e corregedoria) quanto fora dela (abrangendo a sociedade civil e outros órgãos ligados ao sistema criminal e ao controle das atividades policiais) (Brasil, 2023, p, 14).

É importante destacar que, ao contrário das experiências anteriores de 2014 e 2016, os dados não são mais armazenados em servidores corporativos, mas sim em um ambiente de nuvem (cloud storage) fornecido pela empresa Axon. Essa mudança apresenta benefícios econômicos significativos, uma vez que o armazenamento em nuvem é mais eficiente em termos de custos do que a aquisição de computadores. Além disso, a utilização da nuvem permite uma capacidade de escalabilidade mais eficaz no armazenamento, o que se torna crucial diante do grande volume de dados gerados pelas Operações de Polícia (Brasil, 2023, p, 14).

Cabanas argumenta que, desde que haja estabelecimento de regras claras sobre o tratamento das gravações, não se poderia alegar uma violação da intimidade. Isso ocorreria porque as gravações seriam mantidas em sigilo e só poderiam ser solicitadas pelas partes envolvidas ou em um processo judicial, proibindo o acesso por parte de terceiros. Dessa forma, estar-se-ia em conformidade com a Lei de Acesso à Informação e a Constituição Federal, sem comprometer o uso das câmeras, na mesma linha ressalta a importância de informar os cidadãos sobre a gravação (Duque, 2017, p. 147).

A principal consideração é que, no futuro, as Câmeras Corporais não apenas terão a função de monitorar as atividades dos agentes governamentais, mas também desempenharão um papel inteligente no contexto da segurança pública. Além disso, câmeras sofisticadas com capacidade de leitura de placas, identificação facial e outros sistemas de alerta serão instrumentos essenciais para apoiar as operações dos agentes de segurança pública, registrando não apenas imagens, mas também áudio das intervenções policiais.

SMART POLICING – POLICIAMENTO PREDITIVO

Diante desse novo cenário nacional a Policia Militar tem um novo desafio, avançar para um policiamento inteligente, ou seja, um policiamento que congregue: tecnologia (Big Data - IA) com rotina policial para ações preditivas no combate à criminalidade. Nos EUA ao longo dos últimos anos vem sendo desenvolvido métodos de Policiamento Preditivo (Predictive Policing) e Policiamento Inteligente (Smart Policing) buscando desenvolver abordagens de policiamento eficazes, com o objetivo de diminuir os índices de criminalidade, enfatizando ações proativas através da aplicação efetiva de informações, aprimorando a avaliação de desempenho e promovendo a inovação (Coldren JR; Huntoon; Medaris, 2013.)

Esses métodos e estratégias têm como principal objetivo antecipar a ação da polícia diante de eventos criminosos, implementando medidas preventivas por meio da utilização de ferramentas analíticas. (Perry, 2013 e Rummens; Hardyns; Pauwels, 2017) Nesse sentido, a principal ideia é identificar locais de risco, ou seja, os locais onde poderão ocorrer os crimes, e por óbvio essa tarefa não é nada fácil.

A capacidade de antecipar ou prognosticar crimes deriva do entendimento de que os delitos não ocorrem de maneira uniforme em termos geográficos, mas sim se concentram em áreas e pontos específicos, conhecidos como "hotspots", devido a fatores que podem

ser elucidados pela interação entre vítima e infrator, bem como pelas oportunidades disponíveis para a prática de crimes (Braga, *et al* 2019; Chainey *et al* 2008; Ratcliffe 2010, e Rummens; Hardyns; Pauwels, 2017).

Essa abordagem, que se concentra na análise de pequenas áreas geográficas com alta incidência de crimes, resultou na formulação da "lei da concentração dos crimes" pela Escola de Criminologia local. Essa lei é fundamentada em pesquisas que revelaram que, em grandes cidades, cerca de 50% dos incidentes ocorrem em aproximadamente 5% da área estudada (Weisburd, 2015).

Desse modo a partir dessas informações o gesto público pode aplicar os recursos de forma eficiente e localizada, tendo um resultado positivo na prevenção de crimes. No Brasil, ainda, existem poucas pesquisas sobre o tema de Policiamento Preditivo/ Policiamento Inteligente. Ao acessar o catálogo de teses e dissertação da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) digitando os caracteres "policiamento inteligente" foram encontradas somente 12 (doze) pesquisas sobre o assunto (Ministério da Educação, 2023). Analisando de forma mais pormenorizada cada pesquisa, foram selecionados 04 (quatro) por estarem diretamente ligadas ao assunto desse artigo.

O quadro 02 abaixo apresenta de forma sistematizada as 04 (quatro) pesquisas selecionadas para análise.

Quadro 2 – Pesquisas sobre policiamento inteligente

AUTOR	INSTITUIÇÃO DE ENSINO	TIPO DA PESQUISA	TITULO	ANO
ARAÚJO JÚNIOR, Adelson Dias de.	Universidade Federal do Rio Grande do Norte	Mestrado	Predspot: predicting crime hotspots with machine learning.	2019
SILVA, Andrio Rodrigo Corrêa	Universidade Federal do Ceara	Mestrado	Predição de localização de crimes em região urbana usando algoritmos de análise de regressão.	2020
LIMEIRA, Marcio Luiz da Costa	Universidade Federal do Rio Grande do Sul	Mestrado	Proposta de Policiamento Inteligente: integrando modelos de localização preditiva e de roteirização eficiente de patrulhas policiais.	2022
SIMÕES JÚNIOR, Moacir Almeida.	Universidade Federal do Rio Grande do Sul	Mestrado	Adoção da estratégia de patrulhamento multiagente para otimização do policiamento preventivo na cidade de Porto Alegre, RS	2023

Fonte: Autor, com base nos dados da plataforma CAPES.

Primeiro um estudo feito na Universidade Federal do Ceará, onde o objetivo do autor era analisar dados criminais e realizar a predição de onde ocorre a o crime de roubo a pessoa relacionado a cidade de Fortaleza, utilizando técnicas de regressão. O autor utilizou como banco de dados a cidade americana Filadélfia, Estados Unidos e a cidade de Fortaleza no Brasil (Silva, 2020, p.15).

As técnicas de regressão empregadas neste estudo apresentaram resultados excelentes na previsão de crimes. Ao contrário de abordagens como *deep learning* e *boosting*, os métodos de K-*Nearest Neighbor, Random Forest, Extra Trees, Decision Tree* e *Bagging* não demandaram

uma grande quantidade de parâmetros para o treinamento, o que possibilitou mais tempo dedicado à modelagem dos dados em si, em detrimento do treinamento dos modelos. Os resultados obtidos evidenciaram a viabilidade de alguns desses métodos na construção de modelos preditivos aplicáveis a situações reais (Silva, 2020, p. 94).

A análise dos dados criminais revelou padrões relacionados principalmente a horários e dias da semana em que os crimes ocorreram. Esses padrões proporcionam a oportunidade de implementar estratégias de patrulhamento mais eficientes em áreas específicas, por exemplo. No entanto, é importante ressaltar que, apesar das acuradas predições alcançadas pelo modelo, é fundamental manter uma regularidade na coleta de novos dados, pois os padrões de crimes tendem a evoluir ao longo do tempo (Silva, 2020, p. 94).

Outro estudo, feito na Universidade Federal do Rio Grande do Norte, onde o objetivo do autor era melhorar nossa estrutura de previsão proposta anteriormente através de mapeamento alternativo do crime e abordagens de engenharia de recursos, e fornecer uma implementação de código aberto que os analistas policiais podem usar para implantar sistemas preditivos mais eficazes policiamentos (Araújo Júnior, 2019, p. 15).

Segundo o autor, foram identificados alguns desafios para a implantação de sistemas preditivos na segurança pública. O primeiro desafio era encontrar um estudo que apresente de maneira clara e transparente as etapas de processamento envolvidas na criação de futuros focos de crime, ao mesmo tempo que demonstre sua eficácia em comparação com estratégias tradicionais. Em segundo lugar, as ferramentas que sustentam tais estudos são geralmente proprietárias, o que torna a reprodução dos resultados uma tarefa árdua. Em terceiro lugar, a partir da literatura existente, é complicado avaliar como a escolha de um método específico de mapeamento do crime ou

algoritmo de aprendizado de máquina influencia o desempenho preditivo (Araújo Júnior, 2019, p.70).

Na pesquisa citada, utilizou dois métodos de mapeamento do crime, KGrid e KDE, juntamente com dois algoritmos de aprendizado de máquina, *Random Forest e Gradient Boosting*, em comparação a um método de linha de base baseado em uma única agregação autoregressiva. (Araújo Júnior, 2019, p.70).

O estudo também realizou a comparação entre duas cidades, Natal no Brasil e Boston nos Estados Unidos, analisando doze cenários de crimes a partir de conjuntos de dados disponíveis. Em cada cenário de crime, foram aplicados quatro modelos: *KGrid-RF, KGrid-GB, KDE-RF e KDE-GB*, juntamente com um modelo de linha de base. Os resultados apontaram que o modelo KDE-GB apresentou o melhor desempenho em todos os cenários de crime ($p < 0,001$), com uma média de PRRMSE de 3,123 (Araújo Júnior, 2019, p.71).

Além disso, é importante mencionar que os cenários de crime tinham diferentes tamanhos de amostras, o que nos permitiu identificar outros padrões nos resultados. Observou-se que os modelos baseados em KDE demonstraram resultados promissores nos cenários de crime com amostras reduzidas. Constatou-se, também, que à medida que o tamanho das amostras aumentava, o desempenho dos modelos baseados em KDE e KGrid tendia a se aproximar (Araújo Júnior, 2019, p.71).

A terceira pesquisa, realizada na Universidade Federal do Rio Grande do Sul, o autor buscou propor um modelo de policiamento inteligente integrado utilizando modelos de localização preditiva de patrulhas policiais e roteirização, a partir de uma abordagem heurística eficiente. (Limeira, 2022, p. 13).

O autor apresenta um Modelo de Previsão para a Localização e Roteamento de Patrulhas, que foi validado usando dados reais. Este modelo representa uma inovação no contexto do policiamento

inteligente, oferecendo a perspectiva de aplicação prática para aprimorar a gestão de operações policiais. A proposta engloba todo o ciclo do policiamento inteligente preditivo, começando com a coleta de dados, seguida de análises preditivas para planejar operações policiais. Espera-se que, com a implementação dessas operações, haja uma redução nos índices de criminalidade, criando assim um ambiente de atuação proativa em áreas de alto risco, mesmo quando recursos são limitados (Limeira, 2022, p. 86).

O modelo utilizou o método *Risk Terrain Modeling* (RTM) para a definição de locais de atuação, considerando o crime de homicídios, em região do município de Porto Alegre. O método, diferente dos hotspots, que considera a incidência anterior do crime analisado, avalia outros fatores que possam interferir para a incidência do delito observado. No caso foram utilizados: zonas de atuação de gangues e tráfico de drogas, locais de violência interpessoal e de conflitos violentos cotidianos, pontos de incidência de homicídios, lugares de ocorrências de arma de fogo e áreas de vulnerabilidade (Limeira, 2022, p. 85).

Assim, considerando dados dos anos de 2020 a 2021, realizou-se uma comparação com outros métodos de localização de facilidades, a p-medianas, o problema de localização de máxima cobertura e k-means. A pesquisa demonstrou que o modelo de RTM proposto, para uma predição mensal das áreas de maior risco, apresentou melhores resultados tanto para o modelo de cobertura de 5% da área estudada, quanto para o modelo que considerou o atendimento de 10% da extensão avaliada, atingindo o índice de assertividade de 31% e 43%, respectivamente (Limeira, 2022, 85).

Além disso, o estudo propôs uma modelagem de roteirização para cobertura das zonas de risco, utilizando a metaheurística Busca Tabu, demonstrando excelentes resultados, com a possibilidade de emprego operacional.

A quarta pesquisa também foi desenvolvida na Universidade Federal do Rio Grande do Sul, onde o autor tinha como objetivo formular o problema de roteamento dinâmico de patrulhas policiais, inspirado em estratégia multiagente de policiamento (Simões Júnior, 2023, p. 16).

A utilização de técnicas preditivas, no campo do aprendizado de máquina e aprendizado profundo, pode conduzir a previsões mais precisas sobre os horários e locais em que ocorrem os crimes. A disponibilização de informações de geolocalização dos agentes e de ferramentas de roteamento precisas pode resultar em melhorias em tempo real no atendimento de ocorrências. A coleta de dados mais abrangentes sobre o funcionamento de estabelecimentos privados (como bares, restaurantes e clínicas) e públicos (como parques, hospitais e escolas) pode possibilitar aprimoramentos nas previsões. Além disso, um entendimento mais aprofundado das particularidades do funcionamento do serviço policial certamente permitirá a implementação de restrições que tornem o modelo mais fiel à realidade e capaz de produzir resultados mais eficazes. (Simões Júnior, 2023, p. 84-85).

Com base nos dados temporais e geográficos do espaço analisado, foi possível criar um modelo de previsão que foi utilizado como critério para priorizar a alocação de recursos policiais durante o patrulhamento. Além disso, isso resultou em uma seleção mais precisa dos pontos com maior probabilidade de ocorrência de eventos policiais (áreas críticas). O modelo foi testado e validado utilizando dados reais de ocorrências e recursos operacionais em uma unidade de policiamento ostensivo em Porto Alegre. Os resultados demonstraram que a implementação do modelo pode significativamente aprimorar a distribuição das atividades policiais na região, reduzindo a ociosidade nas áreas críticas e diminuindo o tempo de resposta em casos de ocorrências policiais. Em cenários práticos, sua aplicação pode resultar

em uma redução da criminalidade e em um aumento da sensação de segurança nas comunidades afetadas. É importante ressaltar que a precisão da previsão e o tempo de resposta para atender ocorrências podem ser aprimorados. O modelo de previsão alcançou uma acurácia de 64,85% nos dados de teste e um máximo de 30,76% no processo de validação (Simões Júnior, 2023, p. 84-85).

O policiamento preditivo é uma necessidade da nova sociedade. O Estado, especialmente, a Polícia Militar deve investir recursos humanos, materiais e tecnologia fomentando parcerias públicos privadas para trilhar novas pesquisas sobre o policiamento preditivo/inteligente. Ainda, todos os estudos citados acima demonstram um campo fértil para novas pesquisas sobre o policiamento preditivo/inteligente.

CONSIDERAÇÕES FINAIS

Como exposto, as novas tecnologias têm o potencial de revolucionar a segurança pública, fornecendo às forças policiais ferramentas mais eficientes para combater a criminalidade e proteger a sociedade. No entanto, é imperativo que essas tecnologias sejam implementadas com responsabilidade, ética e transparência, garantindo que os benefícios superem os desafios e preocupações que possam surgir no caminho. Somente assim poderemos aproveitar ao máximo o casamento complexo e promissor entre as novas tecnologias e a segurança pública.

A era da sociedade em rede traz consigo uma diversidade de implicações ligadas à gestão e proteção dos dados. Os riscos potenciais associados ao "uso inadequado" e à divulgação de informações pessoais são abundantes. No entanto, as tecnologias inovadoras de manipulação desses dados também têm o potencial de oferecer inúmeras vantagens em vários aspectos da vida em comunidade. A Segurança Pública é um exemplo proeminente desses domínios.

Novas tecnologias como IA, Big Data, câmeras corporais prometem melhorar a atuação policial em vários aspectos. No Brasil existem diversas ações em nível federal e estadual sobre o uso de novas tecnologias, especialmente, uso do videomonitoramento e sistemas de identificação de veículos.

Ainda falta uma implementação máxima do uso de IA e Big Data. Ainda, o país tem um enorme desafio em realizar uma cooperação entre a União e Estados para construção de bancos de dados de nível nacional para aplicação de mineração, análise e perfilamento de dados. Também algumas pesquisas demonstram as vantagens do denominado policiamento preditivo/inteligente, porém ainda não necessários mais pesquisas e investimentos na temática no país.

Mesmo diante de tempos líquidos, definição acertada por Bauman (2001), uma certeza é que o uso de tecnologias só vai aumentar em todas as áreas do conhecimento, especialmente, na segurança pública, já que segurança é uma demanda global desde no início da formação das primeiras sociedades. O presente artigo analisou algumas novas tecnologias, demonstrando vantagens e dificuldades de suas implementações na área da Segurança Pública no Brasil.

Contudo existe ainda um longo trajeto a ser percorrido, o qual vai precisar de uma cooperação nacional de investimentos humanos, materiais e tecnológicos para conseguir extrair o melhor resultado nas novas tecnologias na segurança publica e gerar bem-estar social para os brasileiros.

REFERÊNCIAS

AMARAL, Thiago Bottino do; VARGAS, Daniel; PRATES, Fernanda (Coords). **SEGURANÇA PÚBLICA NA ERA DO BIG DATA:** Mapeamento e diagnóstico da implementação de novas tecnologias no combate a criminalidade. Rio de Janeiro: FGV Direito Rio, 2023.

ARAÚJO JÚNIOR, Adelson Dias de. **Predspot: predicting crime hotspots with machine learning**. 2019. 85f. Dissertação (Mestrado). Universidade Federal do Rio Grande do Norte, Centro de Ciências Exatas e da Terra, Programa de Pós- Graduação em Sistemas e Computação. Natal, 2019. Disponível em: https://repositorio.ufrn.br/handle/123456789/29155. Acesso em: 15 out. 2023.

BAUMAN, Zygmunt. **Modernidade líquida**. Rio de Janeiro: Jorge Zahar, 2001.

BRAGA, Anthony A.; TURCHAN, Brandon; PAPACHRISTOS, Andrew V.; HUREAU, David M. Hot spots policing of small geographic areas effects on crime. **Campbell Systematic Reviews**, 15 (3), 2019. Disponpivel em: https://onlinelibrary.wiley.com/doi/full/10.1002/cl2.1046. Acesso em: 04 out. 2023.

BRASIL. SUPREMO TRIBUNAL FEDERAL. **RECURSO EXTRAORDINÁRIO 1.010.606 RIO DE JANEIRO. Recurso extraordinário com repercussão geral.** Caso Aída Curi. Direito ao esquecimento. Incompatibilidade com a ordem constitucional. Recurso extraordinário não provido. Relator Ministro Dias Toffoli. Julgado em 11 de novembro de 2011. Brasília: DF. 2021. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=755910773. Acesso: 04 set. 2023.

BRASIL. **FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA**. As câmeras corporais na polícia militar do Estado de São Paulo: processo de implementação e impacto nas mortes de adolescentes. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2023/05/cameras-corporais-pmesp.pdf. Acesso: 05 set. 2023.

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: 1 out. 2023.

CAI, Yijun; LI, Dian; WANG, Yuyue. **Intelligent Crime Prevention and Control Big Data Analysis System Based on Imaging and Capsule Network Model. Neural Processing Letters**. Springer Nature, 30 abr. 2020. Disponível em: https://link.springer.com/article/10.1007/s11063-020-10256-1. Acesso em: 21 set. 2023.

CANCELIER, Mikhail Vieira de Lorenzi. O direito à privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência (Florianópolis)**, p. 213-239, 2017. Disponível em: https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/?format=html. Acesso em: 15 set. 2023.

CASTELLS, Manuel. **A Era da Informação:** Economia, Sociedade e Cultura. A Sociedade em Rede. v. 1. 5. ed. São Paulo: Paz e Terra, 2002.

CASTELLS, Manuel. **A Galáxa da internet: reflexões sobre a internet, os negócios e a sociedade.** Rio de Janeiro: Zahar, 2003.

CHAINEY, Spencer; TOMPSON, Lisa; & UHLIG, Sebastian. The utility of hotspot mapping for predicting spatial patterns of crime. **Security Journal**, 21, (1–2), 4–28, 2008. Disponivel em: https://link.springer.com/article/10.1057/palgrave.sj.8350066. Acesso em: 04 out. 2023.

COLDREN JR, James R.; HUNTOON, Alissa; MEDARIS, Michael. Introducing smart policing: Foundations, principles, and practice. **Police quarterly**, v. 16, n. 3, p. 275-286, 2013. Disponível em: https://

journals.sagepub.com/doi/abs/10.1177/1098611113497042. Acesso em: 06 out. 2023.

DE FREITAS, Michele Caroline dos Santos. A atuação da Polícia Militar do Paraná frente à proteção da mulher em face da violência doméstica mediante o uso da inteligência artificial. **Brazilian Journal of Development**, v. 9, n. 9, p. 26924-26953, 2023. Disponível em: https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/63365. Acesso em: 20 out. 2023.

DINIZ, Maria Helena. **Curso de direito civil brasileiro.** 22. ed. rev. e atual. São Paulo: Saraiva, 2005, v. I.

DUQUE, Robson Cabanas. **A câmera de gravação de vídeo individual como estratégia para o incremento da transparência e legitimidade das ações policiais e afirmação da cultura profissional: uma proposta de sistematização na Polícia Militar do Estado De São Paulo**. 2017. f. 230. Tese (Doutorado em Ciências Policiais de Segurança e Ordem Pública) - Academia De Polícia Militar Do Barro Branco, Polícia Militar do Estado de São Paulo, São Paulo, 2017. p. 147. Disponível em: https://ibsp.org.br/wp-content/uploads/2022/05/Tese-Doutorado-DUQUE-Robson-Cabanas-Body-Cam-CAES-PMESP.pdf. Acesso em: 25 mar. 2023.

EMIDÃO, R. A. M. **Dados, Informação e Conhecimento enquanto elementos de compreensão do universo conceitual da Ciência da Informação**: contribuições teóricas. 2014. 198 f. Dissertação (Mestrado) – Programa de Pós-Graduação em Ciência da Informação, Faculdade de Filosofia e Ciências, Universidade Estadual Paulista – UNESP, Marília, 2014.

ESTADO DO RIO GRANDE DO SUL. Secretária da Segurança Pública. **Conheça o SIM**. Porto Alegre, 2023. Disponível em: https://www.ssp.rs.gov.br/sim. Acesso em: 10 out. 2023.

ESTADO DO RIO GRANDE DO SUL. Secretária da Segurança Pública. **Termo de cooperação do SIM/RS**. Porto Alegre, 2023. p. 03. Disponível em: https://ssp.rs.gov.br/upload/arquivos/201709/06144616-termo-de-cooperacao.pdf. Acesso em: 10 out. 2023.

ESTADO DO RIO GRANDE DO SUL. Secretaria de Segurança Pública. **Cercamento eletrônico e videomonitoramento reforçam Segurança Pública em 36 municípios. Porto Alegre,** 2019. Disponível em: https://estado.rs.gov.br/cercamento-eletronico-e-videomonitoramento-reforcam-segurancapublica-em-36-municipios. Acesso em: 06 de out. de 2023.

G1. **Polícia usou 'robô-bomba' para matar atirador de Dallas. 2016.** Disponível em: https://g1.globo.com/mundo/noticia/2016/07/suspeito-de-ataque-em-dallas-diz-que-queria-matar-gente-branca.html. Acesso em: 06 out. 2023.

GOMES, Orlando. **Introdução ao Direito Civil.** 11. ed., Rio de Janeiro: Forense, 1996.

GOMES, Rodrigo Dias de Pinho. **Big data**: desafios à tutela a pessoa humana na sociedade da informação. Rio de Janeiro: Lumen Juris, 2019.

LEMOS, Ronaldo. **Direito, tecnologia e cultura**. Rio de Janeiro: Editora FGV. 2005.

LIMBERGER, Têmis. A Potencialização da Utilização do Uso da Internet pela Covid-19: A Necessidade de uma Agência Administrativa Independente para Proteção dos Dados Pessoais. In: BRAGATO,

Fernanda Frizzo; STRECK, Lenio Luiz; ROCHA, Leonel Severo (Orgs.) **Constituição, Sistemas Sociais e Hermenêutica.** Anuário do Programa de Pós-Graduação em Direito da Unisinos Mestrado e Doutorado n. 16. Dossiê Temático: Covid-19 e o Direito. São Leopoldo: Karywa, 2020.

LIMBERGER, Têmis. Informação e Internet, o caso do Facebook – um estudo comparado entre o RGPD e a LGPD. In: BRAVO, Álvaro Sánchez (Director). **Democracia, Pluralismo y Derechos Humanos.** Pamplona: Aranzadi, 2019.

LIMBERGER, Têmis. **O direito à intimidade na era da informática:** a necessidade de proteção dos dados pessoais. Porto Alegre: Livraria do Advogado, 2007.

LIMBERGER, Têmis. TRANSPARÊNCIA E ACESSO AOS DADOS E INFORMAÇÕES: O CASO DO "FACEBOOK" – UM ESTUDO COMPARADO ENTRE O RGPD EUROPEU E O MARCO CIVIL DA INTERNET NO BRASIL. In: STRECK, Lenio Luiz; ROCHA, Leonel Severo; ENGELMANN Wilson (Orgs.) **Constituição, Sistemas Sociais e Hermenêutica.** Anuário do Programa de Pós-Graduação em Direito da Unisinos Mestrado e Doutorado n. 14. São Leopoldo: Karywa, 2018.

LIMEIRA, Marcio Luiz da Costa. **Proposta de Policiamento Inteligente:** integrando modelos de localização preditiva e de roteirização eficiente de patrulhas policiais. 2022. 94 f. Dissertação (Mestrado) - Universidade Federal do Rio Grande do Sul, Escola de Administração, Programa de Pós-graduação em Administração, Porto Alegre, RS. 2022. Dísponivel em: https://lume.ufrgs.br/handle/10183/248030. Acesso em: 01 out. 2023.

MANNING, Peter. As Tecnologias de Informação e a Polícia. In: TONRY, Michael; MORRIS, Norval, Org(s). **Policiamento Moderno.** São Paulo: Editorada Universidade de São Paulo, 2003.

MASKALY, Jon et al. The effects of body-worn cameras (BWCs) on police and citizen outcomes: A state-of-the-art review. **Policing: An International Journal of Police Strategies & Management**, v. 40, n. 4, p. 672-688, 2017. p. 675. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/PIJPSM-03-2017-0032/full/html. Acesso: 05 set. 2023.

MINISTÉRIO DA EDUCAÇÃO. Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES. **Catálogo de Teses e Dissertações**. 2023. Disponível em: https://catalogodeteses.capes.gov.br/catalogo-teses/#!/. Acesso em: 20 out. 2023.

NASCIMENTO PINHEIRO VARGAS, Érica; MATOS RIBEIRO, Mônica. A SOCIEDADE DO CONTROLE DIGITAL E A SEGURANÇA PÚBLICA BRASILEIRA. **Direito UNIFACS – Debate Virtual**, n. 277, p. 01-24. 2023. p. 19. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/8297. Acesso em: 08 out. 2023.

PEIXOTO, Erick Lucena Campos; JÚNIOR, Marcos Ehrhardt. Breves notas sobre a ressignificação da privacidade. **Revista Brasileira de Direito Civil**, v. 16, p. 35-35, 2018. Disponível em: https://rbdcivil.emnuvens.com.br/rbdc/article/view/230. Acesso em: 03 set. 2023.

PERRY, Walt L. **Predictive policing:** The role of crime forecasting in law enforcement operations. Rand Corporation, 2013. Disponível em: https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf. Acesso em: 06 out. 2023.

RATCLIFFE, Jerry. Crime Mapping: Spatialand Temporal Challenges. In: Handbook of Quantitative Criminology. In **Handbook of Quantitative Criminology**, 2010.

RODOTÁ, Stefano. **A vida na sociedade da Vigilância**: a privacidade hoje**.** Rio de Janeiro: Renovar, 2007.

RUMMENS, Anneleen; HARDYNS, Wim; PAUWELS, Lieven. The use of predictive analysis in spatiotemporal crime forecasting: Building and testing a model in an urban context. **Applied Geography**, 86, p. 255–261. 2017. Disponivel em: https://www.sciencedirect.com/science/article/abs/pii/S0143622816304957. Acesso em: 04 out. 2023.

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

SCHWAB, Klaus; DAVIS Nicholas**. Aplicando a Quarta Revolução Industrial.** São Paulo: Edipro, 2018.

SEMELER, Alexandre Ribas; PINTO, Adilson Luiz. Os diferentes conceitos de dados de pesquisa na abordagem da biblioteconomia de dados. **Ciência da Informação**, v. 48, n. 1, 2019. Disponível em: https://revista.ibict.br/ciinf/article/view/4461. Acesso em: 03 out. 2023.

SERBENA, Cesar A. Interfaces atuais entre a E-Justiça e a Q-Justiça no Brasil. **Revista de Sociologia e Política**. v. 21, n. 45, pp. 47-56, 2013. Disponível em: https://www.scielo.br/j/rsocp/a/XVhdtKRxSbzrVXqWV5zhqSz/?lang=pt. Acesso em: 21 set. 2023.

SILVA NETO, Victo José da; BONACELLI, Maria Beatriz Machado; PACHECO, Carlos Américo. O sistema tecnológico digital: inteligência artificial, computação em nuvem e Big Data. **Revista Brasileira de Inovação**, v. 19, p. 01-31, 2021. p.08. Disponível em: https://www.

scielo.br/j/rbi/a/bySdpVGyHNkGvYBr5qVgpmh/. Aceso em: 06 out. 2023.

SILVA, Andrio Rodrigo Corrêa. **Predição de localização de crimes em região urbana usando algoritmos de análise de regressão.** 2020. 99f. Mestrado (dissertação) Universidade Federal do Ceará, Programa de Pós-Graduação em Engenheira Elétrica e de Computação, Sobral, 2020. Disponível em: https://repositorio.ufc.br/handle/riufc/56162. Acesso em: 10 out. 2023.

SIMÕES JÚNIOR, Moacir Almeida. **Adoção da estratégia de patrulhamento multiagente para otimização do policiamento preventivo na cidade de Porto Alegre, RS**. 2023. 93f. Mestrado (Dissertação) - Universidade Federal do Rio Grande do Sul, Escola de Administração, Programa de Pós-graduação em Administração, Porto Alegre, RS, 2023. Disponível em: https://lume.ufrgs.br/handle/10183/263224. Acesso em: 04 out. 2023.

TEPEDINO, Gustavo. A tutela da personalidade no Ordenamento Civil-Constitucional Brasileiro. In: TEPEDINO, Gustavo. **Temas de direito civil.** Rio de Janeiro: Renovar, 1999.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação.** Porto Alegre: Sergio Antonio Fabris Editor, 2007.

WEISBURD, David. The law of crime concentration and the criminology of place. **Criminology**, 53, no. 2: 133-157, 2015. Disponivel em: https://onlinelibrary.wiley.com/doi/abs/10.1111/1745-9125.12070. Acesso: 06 out. 2023.

ZUBOFF, S. Big Brother: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, F. et al. (Orgs.). **Tecnologias da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018.