UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS DA EDUCAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

Luís Flávio Zampronha

O sistema de proteção dos pessoais no âmbito das atividades policiais: prevenção, investigação, detecção ou repressão de infrações penais

Florianópolis
2023

Luís Flávio Zampronha

O sistema de proteção dos pessoais no âmbito das atividades policiais: prevenção, investigação, detecção ou repressão de infrações penais

Dissertação apresentada como requisito parcial para a obtenção do título de Mestre em Ciência da Informação do programa de Pós-Graduação em Ciência da Informação Centro de Ciências da Educação Universidade Federal de Santa Catarina.

Orientador: Prof. Edgar Bisset Alvarez, Dr.

Florianópolis

2023

Zampronha , Luís Flávio
O sistema de proteção dos pessoais no âmbito das atividades policiais : prevenção, investigação, detecção ou repressão de infrações penais / Luís Flávio Zampronha ;orientador, Edgar Bisset Alvarez, 2023.
155 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências da Educação, Programa de Pós-Graduação em Ciência da Informação, Florianópolis, 2023.

Inclui referências.

1. Ciência da Informação. 2. proteção de dados pessoais. 3. atividade policial. 4. vigilância preditiva. 5. big data. I. Alvarez, Edgar Bisset . II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Informação. III. Título.

Luís Flávio Zampronha

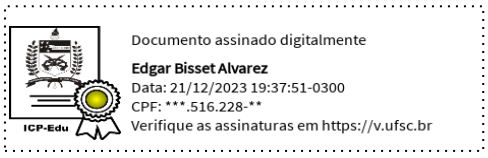
O sistema de proteção dos pessoais no âmbito das atividades policiais: prevenção, investigação, detecção ou repressão de infrações penais

O presente trabalho em nível de Mestrado foi avaliado e aprovado, em 04 de outrubo de 2023, pela banca examinadora composta pelos seguintes membros:

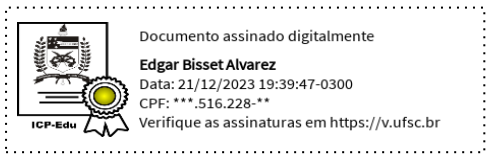
Prof. Enrique Muriel-Torrado, Dr.
Universidade Federal de Santa Catarina – UFSC

Profa. Mirelys Puerta Diaz , Dra.
Universidade de Havana- Examinadora Externa

Certificamos que esta é a versão original e final do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Ciência da Informação.



Prof. Edgar Bisset Alvarez, Dr.
Orientador - UFSC



Prof. Edgar Bisset Alvarez, Dr.
Orientador - UFSC

Florianópolis, 2023.

AGRADECIMENTOS

Para o Professor Edgar Bisset Alvarez, por sua orientação valiosa e apoio inestimável durante esta jornada académica. Muito obrigado!

Aos professores do Programa de Pós-Graduação em Ciência da Informação do Centro de Ciências da Educação, da Universidade Federal de Santa Catarina, por terem aberto as portas deste novo campo de conhecimento aos servidores da Polícia Federal

Para a ANP, por sempre acreditar no valor da educação dos policiais federais.

RESUMO

As polícias precisam gerenciar sistemas de bancos de dados cada vez maiores e mais complexos para conseguir identificar, acessar e extrair evidências criminais ou informações relevantes relacionadas à prevenção de crimes. Ao mesmo tempo, o modelo de ação policial orientada pela inteligência ressalta a importância das informações como principal recurso a ser utilizado pelos órgãos de segurança pública na otimização de suas atividades. Assim, como o exercício do poder de coletar dados e informações é a atividade mais importante realizada pelas polícias, deve-se partir do pressuposto de que toda informação de interesse para os órgãos de segurança pública deve ser preservada, armazenada e principalmente consultada de forma ótima. Por sua vez, a modernização dos aparatos de coleta e análise de dados pessoais, com a profunda transformação dos métodos de enfrentamento do crime a partir da utilização de sistemas de coleta e armazenamento de dados, big data, vigilância preditiva, dentre outras tecnologias cada vez mais invasivas, acarreta limitações aos direitos humanos daqueles que têm seus dados coletados e tratados pelo Estado, como a privacidade e a liberdade informacional. Desse modo, o presente trabalho busca descrever sistemas de tratamento de dados pessoais nas polícias que assegurem um nível adequado de salvaguarda aos direitos fundamentais daqueles que têm seus dados armazenados e tratados pelos órgãos de segurança pública. Para tanto, utiliza-se o modelo adotado pela União Europeia a partir da Diretiva da União Europeia (DUE) nº 680/2016 (Law Enforcement Directive), relativa à proteção dos direitos individuais das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais e execução de sanções penais.

Palavras-chave: proteção de dados pessoais, atividade policial, vigilância preditiva, *big data*.

ABSTRACT

Police agencies need to manage increasingly larger and more complex databases to identify, access, and extract criminal evidence or relevant information related to crime prevention. At the same time, the intelligence-led policing model emphasizes the importance of information as the primary resource to be used by law enforcement agencies in optimizing their activities. Therefore, as the exercise of collecting data and information is the main activity carried out by the police, it must be assumed that all information of interest to law enforcement agencies should be preserved, stored, and, most importantly, accessed optimally. The modernization of data collection and personal data analysis tools, along with the profound transformation of crime-fighting methods using data collection and storage systems, big data, predictive surveillance, among other increasingly invasive technologies, imposes limitations on the human rights of those whose data is collected and processed by the State, particularly privacy and informational freedom. Thus, this work aims to describe personal data processing systems within the scope of law enforcement that ensure an adequate level of protection for the fundamental rights of those whose data is stored and processed by law enforcement agencies. To do so, it mainly relies on the model adopted by the European Union through Directive 2016/680 (Law Enforcement Directive), concerning the protection of the rights of individuals regarding the processing of personal data by competent authorities for the purposes of crime prevention, investigation, detection, or prosecution of criminal offenses and the execution of criminal sanctions.

Keywords: personal data protection, policing, information-led policing, big data.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

CEDH	Corte Europeia de Direitos Humanos
CI	Ciência da Informação
CIA	Agência Central de Inteligência
CJUE	Corte de Justiça da União Europeia
DUDH	Declaração Universal dos Direitos Humanos
DUE	Diretiva da União Europeia
UE	União Europeia
Europol	Agência da União Europeia para a Cooperação Policial
LGPD	Lei Geral de Proteção de Dados
MJSP	Ministério da Justiça e Segurança Pública
NSA	Agência de Segurança Nacional
PNSPDS	Política Nacional de Segurança Pública e Defesa Social
PPGCIN	Programa de Pós-Graduação em Ciência da Informação
RE	Regulamento Europol
RGPD	Regulamento Geral de Proteção de Dados
SINESP	Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas
SOC	Sistemas de Organização do Conhecimento
STF	Supremo Tribunal Federal
SUSP	Sistema Único de Segurança Pública
UFSC	Universidade Federal de Santa Catarina

SUMÁRIO

1. INTRODUÇÃO

A coleta, o armazenamento e a análise de dados e informações representam o núcleo central da atividade policial moderna. Assim, a forma como as polícias administram ou processam seus bancos de dados constitui um tema sempre sujeito a novas abordagens e reflexões. Atualmente as polícias precisam gerenciar sistemas de bancos de dados cada vez maiores e complexos, para conseguirem identificar, acessar e extrair evidências criminais, ou outras informações relevantes e relacionadas à prevenção de crimes. Casos envolvendo muitos *terabytes* de dados associados a um único suspeito estão se tornando frequentes, o que gera um impacto considerável sobre a quantidade de tempo e de recursos que as polícias precisam investir na condução de suas investigações criminais.

Entretanto, ao lado dos desafios enfrentados pelas instituições do sistema de segurança pública, também há novas oportunidades criadas pelas tecnologias. Sistemas informatizados possibilitam a análise de conjuntos de dados volumosos, com o consequente aumento da capacidade das polícias de acessar, cruzar, combinar e correlacionar diferentes fontes de dados e informações. Dados mais concentrados podem aumentar as chances da polícia em encontrar e relacionar evidências de um crime, bem como de elaborar uma linha do tempo de eventos relevantes. Da mesma forma, grandes sistemas de dados e informações podem auxiliar na elaboração do conhecimento sobre crimes e criminosos, melhorando a capacidade das polícias de realizarem análises criminais, visando a identificação de possíveis padrões de condutas ilícitas e áreas de maior potencial de ocorrência de crimes.

Algumas áreas criminais apresentam, por definição, problemas relacionados à coleta e análise de dados. Por exemplo, em investigações de crimes financeiros, com a evasão de divisas de quantias vultosas e fraudes envolvendo criptoativos, torna-se necessário processar milhares de registros de transações bancárias para a identificação das movimentações ilegais de recursos. O mesmo ocorre atualmente nas interceptações de comunicações, com a coleta de inúmeros arquivos telemáticos armazenados em nuvens de aplicativos de comunicação. Assim, hoje em dia é cada vez mais recorrente o desenvolvimento pelas polícias de projetos de *big data*[1], visando a coleta, armazenamento e análise de grandes conjuntos de dados. Este fenômeno foi acompanhado também pelo incremento do poder dos órgãos de investigação criminal de exigir informações, com o acesso a diversos bancos de dados, gerados por organizações públicas e

[1] A maioria dos projetos de "*big data*" envolvem ativos de informações de alto volume, velocidade e/ou variedade, que exigem formas novas e inovadoras de processamento para extração de significados, tomada de decisão aprimorada, *insights* de negócios ou otimização de processos (Gartner, 2023).

privadas. Com dados cada vez mais volumosos e complexos reunidos no contexto das investigações criminais, bem como em ações de prevenção ao crime, a criação de métodos para organizar e gerenciar informações, de forma eficaz e eficiente, não é, portanto, uma escolha. Antes, é uma condição indispensável para que a atuação estatal na área de segurança seja eficiente.

Por outro lado, as modernas técnicas de controle da criminalidade agora vão além das ações policiais reativas tradicionais, quando os órgãos de investigação criminal somente atuam em resposta a crimes específicos, os quais chegam ao seu conhecimento. Atualmente, várias organizações policiais passaram a adotar uma abordagem proativa de enfrentamento ao crime, buscando se antecipar à própria ação criminosa, com base em perspectivas prováveis de sua ocorrência. Essa atividade proativa de prevenção criminal é caracterizada por uma ação policial orientada pela informação, com a utilização de mecanismos de tratamento de dados que possibilitam a identificação de eventos criminosos que estão ocorrendo naquele momento, ou que poderão ocorrer em um futuro imediato, incluso com a utilização de processos automatizados das diversas etapas de análise (ex. sistemas de reconhecimento de imagens).

Um exemplo de ação policial proativa, visando a identificação de um crime futuro ou em andamento, e realizada a partir do cruzamento de dados, é aquela destinada a prevenir e reprimir o tráfico ilícito de drogas em voos comerciais. No enfrentamento de referida modalidade criminosa, as polícias realizam a análise da pré-lista de passageiros, em busca de possíveis traficantes. Estes são conotativamente chamados de “mulas”, ou seja, indivíduos que, conscientemente ou não, transportam drogas em seu corpo ou por meio da ingestão da droga encapsulada, bem como em bagagem, que são despachadas para outros países. No caso brasileiro, as pré-listas de passageiros são repassadas pelas companhias aéreas aos agentes da Polícia Federal, os quais, através do cruzamento com outros bancos de dados, realizam a identificação de passageiros que se encaixam no perfil característico dos últimos casos de “mulas” identificadas enquanto transportavam drogas. Assim, os passageiros selecionados, a partir de determinados critérios, podem ser submetidos a entrevistas policiais e a uma revista pessoal e de bagagem mais detalhada (Silva, 2023).

Do mesmo modo, verificou-se nos anos recentes uma alteração na própria forma de atuação das polícias, com uma mudança em sua filosofia tradicional de atuação como simples agências de manutenção da lei e da ordem. Embora o cumprimento das leis penais seja a sua principal função, as polícias passaram a atuar também no gerenciamento das atividades criminosas. As ações policiais passaram a abordar questões sociais e econômicas mais amplas, como fatores relacionados à criminalidade, que são analisados para a definição das estratégias

mais eficientes de enfrentamento. Pressões políticas e mesmo acadêmicas questionam a capacidade das polícias de prestarem um serviço que atenda às necessidades da sociedade, motivo pelo qual as instituições de segurança pública, com base na concepção de ações orientadas pela informação, têm se engajado cada vez mais na elaboração de análises criminais, visando fornecer à administração uma compreensão real da atividade criminosa e a melhor orientação para enfrentá-la (Fletcher, 2005). Tais análises não lidam apenas com crimes específicos já ocorridos, mas também com a análise de vários tipos de dados, com o objetivo de fornecer aos tomadores de decisão uma compreensão real da atividade criminosa, e a melhor orientação para seu enfrentamento.

Por outro lado, o gerenciamento de imensas massas de dados, no âmbito dos órgãos de segurança pública, passa cada vez mais pela adoção de soluções tecnológicas, com o constante incremento de sistemas de armazenamento e consulta, em termos de capacidade de descrição, classificação e organização da informação (Souza; Almeida; Baracho, 2015). A quantidade de informações, o rápido desenvolvimento computacional e a necessidade de tornar as informações disponíveis a todos os usuários policiais, são os desafios atuais representados pelo crime. Verifica-se que a atividade policial nunca precisou tanto do auxílio da Ciência da Informação para que orquestrar seus esforços de organização dos dados e os seus conhecimentos acumulados. Portanto, com a premissa de que as informações relevantes para a polícia devem ser preservadas, armazenadas e consultadas (Bush, 1945), os princípios da Ciência da Informação são fundamentais neste trabalho.

Além de fornecer argumentos robustos sobre os benefícios e o valor estratégico da informação para as instituições de segurança pública, a Ciência da Informação (CI) oferece uma série de teorias e conceitos que podem ser empregados para o desenvolvimento de sistemas de informação policial. Por exemplo, a aplicação de teorias da CI sobre a organização do conhecimento pode auxiliar na criação de sistemas que categorizam e relacionam informações relevantes, facilitando a recuperação de dados cruciais para a resolução de casos criminais. O uso de sistemas de informação policial também envolve a distinção entre sistemas de bancos de dados, que lidam com a armazenagem estruturada de dados (Navathe; Elmasri, 2010), e dos sistemas de informação, que integram dados e informações em uma abordagem mais ampla e orientada para a tomada de decisões (Lake; Drake, 2014). Do mesmo modo, a distinção clara entre dados, informações e conhecimento é fundamental, para viabilizar a compreensão de como tais conceitos se relacionam. Assim, a CI pode ajudar a definir os limites em que são aplicados os conceitos e os seus diferentes contextos, inclusive em normas que regulamentam o tratamento de informações em sistemas de informação policial, sendo este o tema central da

presente pesquisa.

Não obstante, deve-se reconhecer a legitimidade das preocupações relacionadas ao movimento de expansão do poder do Estado de obter dados pessoais, ou seja, os dados referentes a uma pessoa natural identificada ou identificável (Brasil, 2018b). Este fato foi potencializado pelo desenvolvimento, nos últimos anos, de tecnologias de coleta e armazenamento de informações. As vantagens do uso de *big data* para a maximização da segurança pública, com a consequente promoção do bem-estar geral da população, poderiam justificar a transformação da sociedade em um verdadeiro *big brother,* conforme conceito cunhado pelo jornalista e escritor George Orwell, em seu livro intitulado "1984". Nestes termos, esse trabalho tem como fundamento o reconhecimento da necessidade de que os sistemas de tratamento de dados dos órgãos de investigação criminal, que realizam processos de classificação de pessoas ou de grupos de indivíduos, sigam padrões elevados de proteção aos direitos individuais dos titulares dos dados, ou seja, das pessoas às quais os dados se referem.

Paralelamente, todas as mudanças tecnológicas trazem consigo a necessidade de se assegurar um maior nível de garantia aos direitos fundamentais daqueles que têm os seus dados armazenados e analisados pelo Estado, tais como o direito à privacidade e o direito à liberdade informacional. Torna-se importante, por isso, promover uma maior compreensão dos fluxos de informações existentes nos órgãos de segurança pública e de investigação criminal, com a análise das normas e procedimentos que devem regular o acesso ao conhecimento acumulado pelas polícias e o uso de bancos de dados e informações eficientemente. A partir de reflexões relacionadas à Ciência da Informação, o presente trabalho busca a compatibilidade entre o tratamento de dados realizado por órgãos policiais, e a adoção de padrões elevados de proteção dos direitos individuais dos cidadãos que têm seus dados manipulados pelo Estado.

A promoção da segurança pública e a realização de investigações criminais envolve, de forma geral, a atividade de localização, coleta, produção, recepção, classificação, utilização, transmissão, armazenamento, eliminação, avaliação ou controle de informações de pessoas. Nestes casos, o tratamento de dados pessoais tem como objetivo identificar suspeitos ou criminosos, prevenir a ocorrência de atividades delituosas ou submeter autores de crimes ao poder punitivo do Estado. Deste modo, o tratamento de dados pessoais, em várias das suas formas, representa o ponto central para as atividades policiais de prevenção, investigação, detecção ou repressão de infrações criminais. Por outro lado, a modernização dos aparatos para coleta e análise de dados pessoais, associada à transformação dos métodos de enfrentamento do crime, resulta no uso de tecnologias mais invasivas. De forma evidente, tecnologias de coleta de dados invasivas limitam os direitos individuais dos cidadãos. Por isso, deve-se buscar o

balanceamento entre os benefícios que os sistemas de informação trazem à segurança pública, e a limitação da privacidade e a liberdade informacional daquelas pessoas cujos dados estão sendo coletados e tratados.

Por conta do agravamento do risco de que os órgãos de segurança pública exerçam, de forma abusiva, o poder de coletar informações, os sistemas jurídicos modernos passaram a adotar normas específicas, regulamentando as atividades de tratamento de dados pessoais realizadas no âmbito das instituições de segurança pública. A exigência de normas específicas, regulamentando a atividade policial, é atendida pela legislação brasileira no que diz respeito às investigações criminais, quando a coleta e a análise de dados pessoais buscam ligar determinado indivíduo a um crime específico. Esse seria o caso, por exemplo, do tratamento de dados bancários ou fiscais visando a produção de informações com o objetivo de provar a ocorrência de um crime do delito de corrupção. A atividade policial que visa submeter investigados ao processo judicial é orientada, de forma geral, diretamente pelo Código de Processo Penal e por leis processuais penais esparsas, tal como a Lei nº 9.296/1996, que regulamenta o acesso dos órgãos de investigação a registros de comunicações e dados telemáticos (Brasil, 1996),

Entretanto, o mesmo não pode ser dito em relação às atividades de prevenção e detecção de crimes, bem como no tratamento de dados realizado para o desenvolvimento de análises criminais ou para a formulação de estratégias de atuação policial. Não existe no sistema de segurança pública nacional normas regulamentando o tratamento de dados com o objetivo de prospectar casos criminais, ou mesmo para elaborar novas estratégias de atuação policial. Do mesmo modo, não há no contexto nacional brasileiro uma sistematização das regras relacionadas ao desenvolvimento de sistemas de informação policial que sejam destinados à coleta, armazenamento, processamento e utilização de dados pessoais, bem como o acesso pelas polícias a bancos de dados controlados por organizações públicas ou privadas. Destarte, tendo em vista o incremento das tecnologias de *big data*, torna-se necessário uma maior regulamentação do uso pelas polícias de bancos de dados e de sistemas de informação, tais como os sistemas preditivos automatizados, para a identificação de suspeitos das práticas de crime; sistemas de análise criminal, para a prospecção de crimes e a identificação de alvos específicos; sistemas eletrônicos de vigilância ou sistemas de pesquisa, para minerar dados pessoais em busca de pistas investigativas (p.ex., dados genéticos ou biométricos).

Por outro lado, deve-se também evitar a adoção de uma abordagem estritamente jurídica sobre o tema, uma vez que a simples edição de leis não possuiria a capacidade de promover a criação de sistemas de informação e produção de conhecimento policial. Tal perspectiva foi justamente o enfoque adotado pela Lei nº 13.675/2018, que dispôs sobre a

criação, no âmbito do Ministério da Justiça e Segurança Pública (MJSP), do Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas – SINESP. Segundo a referida lei, o SINESP teria por objetivo, dentre outros, proceder à coleta, análise, atualização, sistematização, integração e interpretação de dados e informações relativos às políticas de segurança pública e de defesa social, inclusive dos bancos de dados de perfil genético e digitais, bem como aqueles relacionados à rastreabilidade de armas e munições.

Entretanto, na referida lei, não foram previstos os fluxos de informação e de cooperação efetiva entre os diversos atores envolvidos, com a definição das tarefas de cada instituição policial integrante do Sistema Único de Segurança Pública (SUSP). Também não foi estabelecida qualquer norma ou princípio relacionado a modelos de organização do conhecimento, a serem adotados no âmbito do SINESP, bem como regras de tratamento de dados pessoais, a serem seguidas pelos usuários do sistema. Por fim, a Lei nº 13.675/2018 teria deixado de definir claramente a finalidade pela qual cada tipo de dado será coletado e armazenado no âmbito do SINESP, bem como o estabelecimento de limitações temporais que possam garantir que os dados sejam conservados apenas durante o período necessário, e em razão de motivos determinados, explícitos e legítimos (Brasil, 2018a).

Assim, verifica-se no contexto nacional uma total inexistência de normas regulamentado o desenvolvimento de sistemas de informação policial, através do estabelecimento de regras próprias que assegurem um nível adequado de proteção aos direitos fundamentais. Estas devem assegurar para as pessoas que terão seus dados armazenados e tratados pelos órgãos de segurança pública a adoção, por exemplo, de medidas técnicas ou organizativas que limitem tratamentos de dados não autorizados ou mesmo ilícitos. A partir desta constatação, esta pesquisa busca justamente identificar, estudar e analisar os sistemas de tratamento de dados pessoais, desenvolvidos no âmbito da atividade policial, que sejam compatíveis com os padrões modernos internacionais de proteção de dados pessoais.

Para tanto, o presente trabalho utilizou como fundamento principal o modelo adotado pela União Europeia a partir da Diretiva da União Europeia (DUE) nº 680/2016 (denominada em inglês como *Law Enforcement Directive*). Esta DUE trata da à proteção dos direitos individuais das pessoas singulares, no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes, para efeitos de prevenção, investigação, detecção ou repressão de infrações penais, e execução de sanções penais, e à livre circulação desses mesmos dados (União Europeia, 2016b). Do mesmo modo, são utilizados os padrões de proteção de dados pessoais adotados pela Agência da União Europeia para a Cooperação Policial, também

denominada Europol[2], notadamente o Regulamento UE nº 794/2016 (União Europeia, 2016c), que garantiu à referida agência europeia um rígido padrão de proteção de dados pessoais relacionados a atividades de detecção, investigação ou repressão de infrações penais.

A escolha dos referidos normativos (documentos), como base para a presente pesquisa, decorre da influência que o modelo normativo europeu já exerce sobre o sistema jurídico do Brasil. O Regulamento UE nº 679/2016, do Parlamento Europeu e do Conselho, denominado Regulamento Geral de Proteção de Dados ou RGPD, relativo à proteção das pessoas singulares no tratamento de dados, (União Europeia, 2016a), foi utilizado como base para a elaboração da Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados brasileira – LGPD (Brasil, 2018b).

Assim, a Diretiva da União Europeia nº 680/2016, juntamente com as demais normas e teorias criadas a partir de sua edição, constitui atualmente o principal parâmetro normativo internacional sobre o tratamento de dados pessoais no âmbito das investigações criminais. Por este motivo, referida DUE constitui o ponto fundamental das reflexões realizadas na presente dissertação. Embora se reconheça a complexidade que envolve qualquer processo de absorção de modelos normativos originados em outros países, tendo em vista a multiplicidade de elementos históricos e ideológicos que caracterizam cada ordenamento jurídico nacional, a mistura de ideias e tradições jurídicas (*cross-fertilization*) representa um fenômeno irresistível. Assim, este trabalho utiliza o sistema europeu de proteção de dados pessoais como substrato para impulsionar a reflexão sobre o tratamento de dados pessoais pelas instituições policiais, fomentando mecanismos de proteção aos direitos individuais dos titulares de tais dados.

Com base no modelo normativo europeu de proteção de dados pessoais, serão descritos e classificados os princípios e regras, que devem nortear os sistemas nacionais de tratamento de dados pessoais no âmbito da segurança pública. A adoção de tais parâmetros normativos faria com que a atividade policial, em sua função primordial de gerenciamento de informações pessoais, passasse a levar em consideração o respeito aos direitos e garantias individuais, notadamente a privacidade e o direito à liberdade informacional dos cidadãos.

Do mesmo modo, tendo em conta os interesses legítimos dos titulares dos dados e da sociedade em geral, o presente trabalho também oferece subsídios para a avaliação dos riscos representados pelos diversos tipos de operações de tratamento de dados, possibilitando o exame

[2]A Europol foi criada por decisão do Conselho Europeu, para atuar como um organismo da União Europeia para apoiar e reforçar a ação das polícias dos Estados Membros, e a sua cooperação mútua em matéria de prevenção e combate à criminalidade organizada, ao terrorismo e a outras formas graves de criminalidade, que afetem dois ou mais países do bloco europeu (União Europeia, 2016b).

do impacto do uso de novas tecnologias policiais na manipulação das diversas categorias de dados pessoais sensíveis. Cada tipo de dado pessoal apresenta um risco específico para os direitos e liberdades fundamentais de seu titular, preocupação que deve estar presente durante todo o ciclo de vida de qualquer sistema de informação policial, com a identificação desde o estágio inicial deste projeto das possíveis armadilhas do ponto de vista da proteção de dados. A partir desta análise, é que poderão ser implementadas medidas que resultem, entre outras coisas, na total transparência acerca da atividade de tratamento de dados pessoais no âmbito policial; bem como no estabelecimento de modelos de sistemas de informação policial, que possam fazer face aos riscos que representam aos direitos individuais.

Ressalta-se, por fim, que o presente trabalho busca distinguir de forma clara os critérios de análise ético-jurídicos em relação ao tratamento de dados pessoais para fins gerais, e aqueles a serem adotados para fins de combate à criminalidade e de garantia da segurança pública. A atividade tratamento de dados pessoais, realizada pelo Estado com o objetivo legítimo de garantir a segurança da sociedade, não pode ser comparada com serviços comerciais *on line*, aplicativos de redes sociais, *marketing* eletrônico, dentre outras atividades realizadas por empresas privadas, que coletam e manipulam grande volume de dados pessoais. Por conseguinte, seria um equívoco não levar em consideração a complexidade do campo da segurança pública, e o tipo de desdobramento e interferência na esfera da privacidade dos indivíduos.

Como em outras atividades realizadas pelas polícias, a coleta de informações e o tratamento de dados pessoais não é algo bom ou mal em si mesmo, não sendo também uma atividade neutra. A legitimidade do tratamento de dado dependerá sempre do contexto sociopolítico e histórico, das razões pelas quais uma tecnologia específica está sendo implementada, e as práticas que caracterizam a implementação de cada sistema de informação (Brakel, 2016).

Desse modo, em razão da natureza, das funções e dos poderes específicos dos órgãos policiais e de segurança pública, torna-se necessário a adoção de regras específicas de tratamento de dados pessoais no âmbito da segurança pública. Visa esse trabalho justamente identificar regras que, ao lado de garantir o respeito aos direitos individuais daqueles que têm os seus dados pessoais tratados pelas instituições policiais, também levem em consideração as necessidades de proteção da sociedade, em face do crime, e da função do Estado, de criar ambientes de convivência social seguros.

1.1. PROBLEMA

O problema que fundamenta a presente dissertação poderia ser resumido à seguinte questão: quais os princípios e regras de proteção de dados pessoais que devem ser incorporados nas especificações de sistemas de organização do conhecimento policial, e nos procedimentos de tratamento de dados para efeitos de prevenção, investigação, detecção ou repressão de infrações penais, a execução de sanções penais e à livre circulação desses dados, principalmente no que diz respeito às atividades executadas por meios computacionais ou de sistemas informatizados?

Tais princípios e regras visam a implementação de medidas que possam minimizar os riscos envolvidos no tratamento de dados pessoais no âmbito das atividades policiais, promovendo uma maior transparência quanto à natureza dos dados coletados e das funções ou finalidades dos tratamentos realizados pelas polícias. Do mesmo modo, um padrão elevado de proteção dos dados pessoais também deve ser observado desde o estágio inicial do desenvolvimento de qualquer sistema de organização do conhecimento policial, identificando as possíveis fragilidades do ponto de vista da proteção de dados pessoais. Os princípios e regras de proteção de dados pessoais constituem a primeira linha de discussão em qualquer projeto, para que se possa estabelecer novas atividades de processamento de dados no âmbito policial.

1.2. JUSTIFICATIVA

A presente pesquisa tem como justificativa central a necessidade de se aprofundarem as discussões em torno do tema da proteção dos dados pessoais no âmbito policial, com base nos princípios e regras estabelecidas na Diretiva UE nº 680/2016. Também há a necessidade de utilização de teorias da Ciência da Informação para a melhor compreensão dos conceitos relacionados à organização do conhecimento e à descrição das diversas etapas do processo de tratamento de dados pelas polícias (entrada, processamento e saída/recuperação).

O uso de sistemas de *big data* por empresas privadas, e instituições de segurança pública e de inteligência se tornou tema corrente após o caso Edward Snowden, o ex-contratado da Agência de Segurança Nacional (NSA) e da Agência Central de Inteligência (CIA), que revelou o uso sistemático de tecnologias de monitoramento eletrônico por agências de inteligência e segurança. Entretanto, não existe em vigor no Brasil nenhuma lei regulamentando o tratamento de dados pessoais realizados no âmbito das polícias, bem como regras para a estruturação de bancos de dados pessoais ou de sistemas de informação policial. Como já

mencionado, a LGPD brasileira não se aplica ao tratamento de dados pessoais relacionados à segurança pública e investigação criminal, tendo sido expressamente estabelecida a necessidade de aprovação de uma lei específica com este enfoque (Art. 4, inciso III, alíneas “a” e “d”, c/c § 1º) (Brasil, 2018b).

A ausência de legislação específica para o tratamento de dados pessoais no âmbito policial pode acarretar diversos riscos para os cidadãos, incluindo questões relacionadas à privacidade, segurança e possíveis abusos. Como exemplo de possíveis riscos relacionados ao tratamento de dados pessoais pelas polícias pode ser citado: i) o vazamento de informações sensíveis, como dados de testemunhas, vítimas e suspeitos, colocando a privacidade ou mesmo segurança dessas pessoas em perigo; ii) o uso indevido de informações pessoais, com a possibilidade do uso inadequado ou para fins não previstos em lei de dados coletadas pelas polícias; iii) monitoramento excessivo, com a possibilidade da realização de ações de vigilância indevidas por agentes públicos, comprometendo a privacidade dos cidadãos sem uma justificativa legal clara.

Desta forma, torna-se necessária a criação de regras específicas sobre o tratamento de dados pessoais no âmbito da investigação criminal e segurança pública, com a descrição dos processos de entrada de dados (coleta), seu processamento (classificação, indexação, catalogação) e saída de informações (consultas). Mesmo que normas formais muitas vezes não consigam acompanhar o ritmo acelerado das inovações tecnológicas, deixando brechas e lacunas significativas na proteção dos direitos dos cidadãos, sempre será necessário tornar transparente os escopos dos tratamentos de dados pessoais realizados pelas polícias, bem como das capacidades tecnológicas de cruzamento e monitoramento eletrônico, como os utilizados pelos órgãos policiais e de segurança pública. Em conjunto, estas são as principais justificativas para a presente pesquisa.

2. OBJETIVOS

2.1. OBJETIVO GERAL

Ao abordar as normas europeias que regulamentam as atividades de tratamento de dados pessoais para efeitos de prevenção, investigação, detecção ou repressão de infrações penais, principalmente aquelas executadas por meio de novas tecnologias ou sistemas informatizados, este trabalho tem por objetivo geral: **analisar os princípios e regras gerais que garantem padrões elevados de proteção e salvaguarda dos direitos individuais dos titulares dos dados**. Tendo em vista que a Lei Geral de Proteção de Dados (LGPD) não se aplica para o tratamento de dados pessoais para fins de segurança pública, e atividades de investigação e prevenção de infrações penais, este trabalho pretende apresentar subsídios para a regulamentação do tema em âmbito nacional.

2.2. OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho consistem em:

a) Analisar os padrões normativos internacionais de proteção e salvaguarda de direitos no tratamento de dados pessoais, realizados por organizações policiais, com ênfase nos dispositivos da Diretiva UE nº 680/2016 e no Regulamento UE nº 794/2016 (Regulamento Europol – RE);
b) Analisar as salvaguardas e mecanismos de mitigação de risco de violação dos direitos dos titulares dos dados;
c) Classificar os tipos de dados pessoais que são produzidos ou coletados pelas polícias;
d) Classificar as categorias de tratamento de dados pessoais realizadas pelos órgãos de segurança pública;
e) Sistematizar, em forma de tabelas, os princípios e normas relacionadas à proteção e à garantia dos direitos e liberdades individuais dos titulares de dados.

A partir desse estudo, serão extraídos os princípios e regras que devem nortear sistemas nacionais de tratamento de dados pessoais na atividade policial, que levem em consideração o respeito aos direitos e garantias dos titulares de dados, notadamente a privacidade e o direito à liberdade informacional. Tais princípios e regras visam auxiliar o desenho de medidas a serem observadas desde o estágio inicial do desenvolvimento de qualquer sistema de organização do conhecimento e tratamento de dados pessoais no âmbito policial. Do mesmo modo, servem

como base para a elaboração de avaliações do impacto de operações de tratamento de dados, criadas a partir de sistemas informatizados a serem utilizados em atividade policiais.

3. METODOLOGIA

3.1. CLASSIFICAÇÃO DA PESQUISA E DEFINIÇÃO DE ESCOPO

Sob a perspectiva metodológica, trata-se de uma pesquisa qualitativa e teórica, que adota a análise documental e de aportes teóricos selecionados. Para alcançar respostas embasadas em evidências, visando o alcance do objetivo geral proposto ao estudo, foi realizada a uma revisão sistemática da literatura sobre vários aspectos do tratamento de dados pessoais, em áreas como: Ciência da Informação, através do repositório BENANCIB, materiais do Programa de Pós-Graduação em Ciência da Informação, da Universidade Federal de Santa Catarina (PPGCIN-UFSC), Google Acadêmico e livros teóricos especializados; Direitos Humanos, por meio de livros especializados; e Ciência Policial, também em livros especializados, Academia Nacional de Polícia e Google Acadêmico. Neste caso, além de pesquisas específicas, relacionadas ao tratamento de dados pessoais pelas polícias, também foram utilizados termos de busca relacionados ao tratamento de dados pessoais de forma ampla, tendo em vista a necessidade de se transpor para o campo policial e da segurança pública vários conceitos utilizados no sistema geral de proteção de dados pessoais.

A presente dissertação busca analisar padrões normativos relacionados ao tratamento de dados pessoais para os fins policiais de prevenção, investigação, detecção ou repressão de infrações criminais e execução de sanções penais, doravante também denominadas, de forma geral, como “atividades policiais”. Em relação ao Brasil, tais atividades incluem o campo de atuação das polícias que possuem atribuições de realizar investigações criminais e funções de polícia judiciária (Polícia Federal e polícias civis dos Estados); bem como das denominadas polícias ostensivas ou administrativas (Polícia Rodoviária Federal, Polícias Militares dos Estado, Polícias Penais e Guardas Municipais), encarregadas do patrulhamento de rodovias, da preservação da ordem pública, da segurança dos estabelecimentos penais e da proteção de bens, serviços e instalações municipais, respectivamente. Parte-se do pressuposto de que não haveria uma contraposição relevante entre as ações policiais de prevenção ao crime e de investigação criminal, que em alguns casos são interdependentes e complementares, motivo pelo qual a DUE nº 680/2016 engloba ambas as atividades.

Esta distinção ganha relevo, entretanto, na parte do trabalho destinada à discussão de um sistema brasileiro de proteção de dados na atividade policial, tendo em vista a lacuna legislativa existente no Brasil em relação ao denominado policiamento ostensivo. Isto porque tanto a Polícia Rodoviária Federal como as Polícias Militares dos Estados desenvolvem e

utilizam sistemas para a coleta, armazenamento e uso de informações policiais, realizando o tratamento de dados pessoais, para identificar indivíduos que estão prestes a cometer uma infração penal ou que acabaram de praticar um crime (situação de flagrância).

Ressalte-se também que este trabalho não tem como objeto de pesquisa a legislação brasileira que regulamenta a investigação criminal, tampouco os meios especiais de produção de provas de modo geral. Entretanto, torna-se necessário abordar os diferentes propósitos pelos quais as polícias realizam atividades de tratamento de dados pessoais, tendo como foco os aspectos relacionados aos principais processos de organização e tratamento de dados realizado cotidianamente no trabalho policial. Do mesmo modo, busca-se descrever os múltiplos procedimentos de coleta e análise de informações realizados pelas polícias, com a compreensão dos diversos tipos de dados pessoais tratados para fins de prevenção, investigação, detecção ou repressão de infrações penais.

A análise documental e a exploração do marco teórico da pesquisa abarcaram o levantamento, a organização e a leitura de artigos científicos e de obras específicas acerca das temáticas centrais deste projeto de pesquisa. Constituem os campos de análise documental:

i) O microssistema legislativo de proteção de dados, notadamente composto pela Diretiva UE nº 680/2016, relativa ao tratamento de dados pessoais para fins de prevenção, investigação, detecção ou repressão de infrações penais e execução de sanções penais, e o Regulamento UE nº 794/2016 (Regulamento Europol);

ii) Referenciais teóricos que fundamentam e justificam o poder do Estado de realizar o tratamento de dados pessoais em atividades policiais, com vistas a demonstrar a necessidade do balanceamento entre os benefícios sociais de segurança pública e os riscos aos direitos individuais representados pela atividade policial de tratamento de dados;

iii) A teoria dos direitos humanos, categoria constitucional que alicerça os direitos fundamentais que sofrem a intervenção estatal pelo tratamento de dados pessoais, a privacidade e o direito à liberdade informacional; e,

iv) Teorias derivadas da Ciência da Informação, principalmente Sistemas de Organização do Conhecimento e Teoria Sistêmica da Informação.

Por sua vez, a análise documental e a consolidação do referencial teórico da pesquisa foram processadas por meio das seguintes etapas:

1) Identificação e seleção dos documentos (normativos legais e decisões judiciais), artigos científicos e obras (livros) pertinentes ao desenvolvimento da pesquisa;

2) Leitura e análise dos constructos teóricos extraídos dos documentos, artigos e obras consultados; e,

3) Sistematização das informações extraídas dos normativos, artigos e obras e apresentação dos resultados por meio de tabelas estruturadas.

3.1.1. Etapa 1 – Critérios de inclusão e exclusão de documentos (normativos legais e decisões judiciais) e aportes teóricos selecionados (artigos científicos e obras pertinentes)

Os cinco objetivos da pesquisa (ver objetivos específicos, subseção 2.2) foram condensadas nos quatro domínios-chave definidos. A estratégia de busca refletiu vários critérios para a inclusão e exclusão na análise documental de normas, decisões e outros materiais selecionados, bem como na seleção dos aportes teóricos representados por artigos, livros e outras publicações. Materiais que atenderam aos seguintes critérios de inclusão foram considerados elegíveis e inclusos na pesquisa:

- Estudos quantitativos ou qualitativos;
- Publicados em sites ou em formato impresso (livros);
- Fornecidos pelos professores do Programa de Pós-Graduação em Ciência da Informação da UFSC (PPGCIN-UFSC), principalmente pelo orientador do presente trabalho, Professor Edgar Bisset;
- Idioma de publicação em inglês, português e espanhol.

Todos os critérios de inclusão de documentos e aportes teóricos acima definidos se aplicam aos quatro domínios da pesquisa. Entretanto, tais domínios-chave também foram submetidos a outros critérios específicos para a definição de sua inclusão como objeto de análise documental e a como aporte teórico de cada domínio.

3.1.1.1. Critérios de inclusão na análise documental e seleção dos aportes teóricos relacionados ao microssistema legislativo europeu de proteção de dados pessoais

Foram selecionadas como subsídio teórico para o presente trabalho as normas adotadas pela União Europeia, principalmente a Diretiva UE nº 680/2016, relativa à proteção dos direitos individuais das pessoas singulares no que diz respeito ao tratamento de dados pessoais para efeitos de prevenção, investigação, detecção ou repressão de infrações penais e execução de sanções penais, e à livre circulação desses dados (União Europeia, 2016b). A escolha das normas da União Europeia como subsídio do presente trabalho ocorre em razão do avanço das discussões sobre o tema nos países do continente, tendo o Parlamento Europeu incluído em sua

agenda legislativa, a partir de 2015, a necessidade da aprovação de novas medidas de proteção dos dados pessoais dos cidadãos de seu território.

Esse pacote legislativo teve por objetivo imediato a criação de limites ao poder econômico das grandes empresas norte-americanas que dominam a indústria da tecnologia da informação, as denominadas *Big Tech*. A aprovação de um pacote de normas, ainda em 2016, visou reformular o sistema europeu de proteção de dados, cujo principal texto aprovado foi Regulamento UE nº 679/2016, denominado Regulamento Geral de Proteção de Dados, ou RGPD (União Europeia, 2016a).

O RGPD da União Europeia foi utilizado como modelo para a Lei brasileira nº 13.709/2018, ou Lei Geral de Proteção de Dados (LGPD), aprovada pelo Congresso Nacional em 18 de agosto de 2018 (Brasil, 2018b). Esta lei foi a responsável por introduzir no sistema jurídico brasileiro o tema da proteção do tratamento de dados pessoais.

A União Europeia também aprovou, no âmbito do pacote de reforma de seu microssistema legislativo de proteção de dados, a referida Diretiva UE nº 680/2016, que se aplica à proteção de dados pessoais no que diz respeito ao tratamento no âmbito as atividades policiais (União Europeia, 2016a). Assim, do mesmo modo que o Regulamento UE nº 679/2016 serviu como texto base à Lei nº 13.709/2018 eu GPD), a Diretiva UE nº 680/2016 (denominada em inglês como *Law Enforcement Directive*) passou a representar o principal referencial teórico para uma possível futura lei brasileira sobre a Proteção de Dados Pessoais para fins de prevenção, investigação, detecção ou repressão de infrações penais e execução de sanções penais, bem como à livre circulação desses dados (Zampronha, 2021), sendo este o motivo principal de sua seleção e inclusão como documento base da presente pesquisa.

Além da seleção da Diretiva UE nº 680/2016 como objeto de análise documental, também foram utilizadas referenciais teóricos publicados por instituições da União Europeia, referentes ao tema da proteção de dados pessoais, tais como:

i. *The Guide to Data Protection in the European Comission* (Comissão Europeia, 2023);
ii. *Practical guide on the use of personal data in the police* (Conselho da Europa, 2018);
iii. *General Data Protection Regulation Compliance Guidelines* (União Europeia, 2023);
iv. Manual da Legislação Europeia sobre Proteção de Dados – Edição de 2018 (Conselho da Europa, 2018).

Tais manuais e guias oferecem informações detalhadas sobre os principais conceitos e definições abordados na presente pesquisa. Por sua vez, para servir como modelo empírico do sistema de informação policial, com padrões adequados de proteção a dados pessoais, foram selecionados as normativas adotadas pela Agência da União Europeia para a Cooperação

Policial, também denominada Europol. A Europol tem como atribuição apoiar as atividades, operações e investigações criminais transfronteiriças entre os países do bloco europeu, com a criação de equipes de investigação conjuntas, e a prestação de suporte operacional, técnico e financeiro.

Do mesmo modo, a Europol fornece informações e apoio em análises criminais, com a elaboração de avaliações de ameaça, análises estratégicas e operacionais e relatórios sobre situações criminais em geral (União Europeia, 2016c). Ao mesmo tempo, devido à exigência de que fossem criados padrões de proteção de dados pessoais, que garantissem aos indivíduos um sistema de proteção efetiva de dados, foi estabelecido pelo Parlamento Europeu uma legislação abrangente e especializada sobre a proteção de dados no âmbito da referida agência policial. Assim, pode-se afirmar que a Europol possui atualmente uma das estruturas de proteção de dados mais consistentes e robustas do mundo no âmbito das agências de aplicação da lei (Europol, 2023).

A peça central da legislação da Europol, sobre o tratamento de dados pessoais, é o Regulamento UE nº 794/2016, ou Regulamento Europol (RE), com enfoque na classificação dos diversos tipos tratamento de dados pessoais de acordo com cada propósito específico: i) investigações criminais; e b) realização de análises criminais (União Europeia, 2016c). Do mesmo modo, foram selecionados para inclusão na presente pesquisas os seguintes documentos e manuais publicados pela Europol: i). *Data Protection at Europol* (Europol, 2012); e ii) *Data Protection Officer. Freedom and Security. Serious crime and terrorism – defending European values* (Europol, 2023). Tais normativas, manuais e guias (*handbook*) fornecem disposições específicas para cada finalidade de processamento de dados (operacional ou estratégica), a forma de acesso a informações pela Europol e mecanismo para troca de informações com Estados membros, países terceiros e organizações internacionais (Conselho da Europa, 2018).

Assim, por terem estabelecido um rígido padrão de proteção de dados pessoais, relacionados a atividades de detecção, investigação ou repressão de infrações penais, tais normas e referenciais teóricos da Europol passaram a ser objeto de análise documental e revisão bibliográfica na presente dissertação. Entretanto, tendo vista a natureza, as funções e as competências específicas da agência policial europeia, as suas regras de proteção de dados pessoais foram criadas sob medida, de modo a atender às necessidades operacionais da Europol como agência de cooperação policial internacional. Desse modo, o presente trabalho buscou selecionar, no âmbito do modelo normativo da Europol, somente as regras e os princípios que podem ser aplicados na atividade policial de uma forma geral.

3.1.1.2. Critérios de inclusão na análise documental e seleção dos aportes teóricos relacionados às justificativas ético-jurídicas do poder do Estado de realizar o tratamento de dados pessoais

Este trabalho parte da perspectiva de que qualquer estudo relacionado à justificativa ético-filosófica do tratamento de dados na investigação criminal e prevenção ao crime deve se apoiar nas mesmas teorias que tentam justificar o poder punitivo do Estado como um todo, cujo cerne cuida precisamente da justificação da intervenção penal estatal no âmbito das liberdades individuais. O problema da justificação do exercício do poder estatal por instituições politicamente organizadas, da capacidade das polícias de restringirem direitos e liberdades dos membros de uma determinada comunidade, constitui-se em um dos temas centrais da própria teoria do Estado como detentor do monopólio organizado da força. Assim, a partir da discussão acerca do poder punitivo do Estado, também podem ser abordadas as questões centrais acerca da legitimação, fundamentação, justificação e função do tratamento de dados pessoais no âmbito da segurança pública.

Em relação à escolha de artigos e livros relacionados ao suporte teórico que justificam a capacidade das instituições policiais de realizarem o tratamento de dados pessoais no âmbito de suas atividades de prevenção e investigação de crimes, a presente pesquisa selecionou e incluiu como referencial a análise do poder punitivo do Estado, como realizada por Luigi Ferrajoli no seu livro "Direito e Razão – Teoria do Garantismo Penal" (Ferrajoli, 2002). A seleção desta obra clássica do Direito Penal decorre da pretensão de se realizar, na presente pesquisa, uma abordagem ético-jurídica dos fundamentos que legitimam o poder do Estado de realizar o tratamento de dados pessoais, notadamente das teorias utilitaristas expostas por Luigi Ferrajoli. Além de analisar as diversas correntes teóricas que justificam o uso da violência pelo Estado, a referida obra também descreve as funções e atividades exercidas pela polícia. O livro de Ferrajoli exerceu, portanto, grande influência no meio jurídico brasileiro e internacional, ao lançar as bases teóricas da corrente do direito penal que passou a ser denominada "Garantismo Penal" (Ferrajoli, 2002).

Por sua vez, a análise das teorias do poder de intervenção do Estado, conforme exposto pelo supracitado autor, indica que a atividade de tratamento de dados para fins de investigação criminal e segurança pública deve possuir os contornos utilitaristas de adequação entre meios e fins. Não se torna possível, desta feita, extrair a sua justificativa de uma base ética retributivista, condicionada por finalidades punitivas, ou seja, como uma pena (retribuição) imposta em razão do dano causado pelo delito cometido por uma pessoa no passado.

Somente as correntes teóricas utilitaristas, ou a ética consequencialista, podem servir para justificar a necessidade do Estado de interferir na esfera da liberdade individual de pessoas isentas de culpa, impondo restrições às liberdades individuais, ainda que sem uma demonstração da existência concreta do crime ou da participação efetiva da pessoa em uma conduta ilícita (Ferrajoli, p. 2002). Neste contexto, o presente trabalho também selecionou alguns estudos acerca de diferentes formas de utilitarismo, inicialmente sistematizada pelo filósofo Jeremy Bentham e posteriormente desenvolvida por John Stuart Mill.

3.1.1.3. Critérios de inclusão da análise documental e seleção dos aportes teóricos relacionados aos direitos humanos (privacidade e o direito à liberdade informacional)

Sequencialmente, foram selecionados como objeto de análise documental do presente trabalho os aportes teóricos que abordam tratamento de dados pessoais, realizados em âmbito policial, sob o enfoque da proteção dos direitos humanos. Este enfoque analisa os efeitos do tratamento de dados pessoais sobre os direitos individuais daqueles que tem seus dados coletados e tratados pelas polícias, notadamente sobre a sua privacidade e a sua liberdade informacional.

Existe uma evidente ampliação da capacidade tecnológica do Estado de realizar o tratamento de dados pessoais, tendo em vista o caráter altamente incriminador dos elementos de prova obtidos por meio das investigações proativas. Assim, seria necessário verificar se as atividades realizadas pelos órgãos policiais são justificadas, efetivamente, pelas circunstâncias do fato, sendo o exame do respeito aos direitos individuais um dos principais contrapontos ao uso abusivo do poder do Estado de tratar dados pessoais. O balanceamento do emprego maciço de técnicas de tratamento de dados somente pode ser obtido com a aplicação de padrões normativos e jurisprudenciais de proteção aos direitos humanos, principalmente àqueles relacionados à proteção do direito à privacidade e à liberdade informacional.

Existem quatro Sistemas Internacionais de Direitos Humanos, sendo um de abrangência universal e três regionais, que são formados por órgãos e mecanismos próprios de monitoramento da aplicação dos tratados e outros normativos de direitos humanos, relativos a cada organização. O sistema de abrangência global, ou universal, denominado Sistema ONU de Direitos Humanos, e envolve todos os países membros da Organização das Nações Unidas (ONU). Por sua vez, os Sistemas Regionais de Direitos Humanos embarcam três continentes: América, Europa e África, os quais constituem, respectivamente, o Sistema Interamericano de Direitos Humanos, o Sistema Europeu de Direitos Humanos e o Sistema Africano de Direitos

Humanos (Schutter, 2010)[3]. Entretanto, o quadro legal europeu de proteção de dados no âmbito policial baseia-se, em grande parte, nos princípios e regras do Sistema Europeu de Direitos Humanos. Estes, por sua vez, e de certo modo, foram materializados na Diretiva UE nº 680/2016 e no Regulamento UE nº 794/2016 (Regulamento Europol – RE).

Assim, foram selecionadas na presente pesquisa para análise documental as decisões proferidas pela Corte Europeia de Direitos Humanos (CEDH), que abordam as principais questões relacionadas ao tratamento de dados no âmbito da atividade policial. Foram igualmente inclusas, como aporte teórico, os artigos e livros que abordam e interpretam as normas e princípios contidos na Convenção Europeia dos Direitos do Homem, principalmente a obra de Olivier de Schutter, intitulada de "*International Human Rights Law*" (Schutter, 2010).

Ressalte-se, por sua vez, que o conjunto de decisões sobre o tema, como proferidos no âmbito do Sistema Interamericano, do qual o Brasil é integrante, é praticamente inexistente. Entretanto, a maior diferenciação entre os dois sistemas – Europeu e Interamericano – é de natureza política. Enquanto o Sistema Europeu de direitos humanos, durante seus quarenta anos de funcionamento, tem geralmente regulamentado países democráticos, que possuem poderes judiciários independentes e governos que observam o estado de direito, a história de grande parte dos países das Américas, desde a década de 1960, tem sido radicalmente diferente, com ditaduras militares e a repressão violenta de opositores políticos.

Do mesmo modo, o Sistema Interamericano engloba uma região que possui grande discrepância econômico-social entre os seus Estados-membros, principalmente entre os Estados Unidos e o Canadá e os demais países latino-americanos. Assim, a leitura dos relatórios anuais e das decisões da CEDH demonstra que o sistema é essencialmente Latino-Americano, com os Estados Unidos e, mais recentemente o Canadá, aparecendo apenas ocasionalmente em petições individuais apresentadas junto à CEDH, com base na Declaração Americana dos Direitos e Deveres do Homem.

No contexto do desenvolvimento de uma jurisprudência, verifica-se o incremento em nível nacional de técnicas de direito comparado, visando identificar as melhores práticas a serem usadas como referência por todos os países. Tal procedimento encoraja os tribunais nacionais a usarem normas internacionais de direitos humanos, para incrementarem suas próprias capacidades de protegerem as liberdades individuais dos cidadãos de seus países.

Passar a considerar a jurisdição global de direitos humanos pode ser atrativo para os

[3] Conforme Schutter, não se pode afirmar sobre a existência de Sistemas de Direitos Humanos no âmbito da Liga Árabe ou do Continente Asiático (Schutter, O. *International Human Rights Law*. Cambridge: Cambridge Press, 2010).

juízes nos países, pois, fazendo isso, ganham legitimidade para interpretar por outros prismas seus normativos nacionais (Schutter, 2010). Cita-se o exemplo de um recurso em tramitação no Supremo Tribunal Federal (STF; Recurso Extraordinário nº 973.837), no qual foi questionada a constitucionalidade da lei que institui o Banco Nacional de Perfil Genético. Neste julgamento, foi ressaltado que a Corte Europeia de Direitos Humanos havia abordado, em diversas oportunidades, a questão da coleta de amostras de DNA para fins de investigação criminal, tendo o STF já utilizado algumas dessas decisões para fundamentar seu entendimento (Supremo Tribunal Federal, 2016)[4].

Assim, pelos objetivos buscados no presenta trabalho, foram selecionadas as decisões da Corte Europeia de Direitos Humanos (CEDH) como o substrato principal da jurisprudência internacional de direitos humanos, relacionada ao tratamento de dados no âmbito das atividades policiais. Com as inúmeras decisões sobre o tema, a CEDH transformou questões abstratas, relacionadas ao direito à privacidade, em um quadro jurídico concreto. Esse robusto conjunto de decisões da CEDH permite a identificação do caminho a ser seguido pelos demais sistemas de direitos humanos e pelos ordenamentos jurídicos nacionais, que elegem a proteção dos direitos humanos com um dos seus objetivos.

O progresso tecnológico levou a um salto quântico na vigilância, interceptação de comunicações e retenção de dados, o que por sua vez resultou em grandes desafios para a proteção de dados pessoais. Assim, desde o julgamento Leander vs. Suécia, de 1987, no qual foi analisado, pela primeira vez, a questão do armazenamento de dados pessoais de um indivíduo, por uma autoridade pública, a jurisprudência dos órgãos da Convenção Europeia nesse campo passou por um desenvolvimento significativo. Foram examinadas pela Corte muitas situações, e questões relacionadas a esse tema foram levantadas. Um amplo espectro de operações envolvendo dados pessoais, como a coleta, armazenamento, uso e divulgação de tais dados, agora é abrangido por uma jurisprudência consolidada da CEDH, que se desenvolveu em consonância com a rápida evolução nas tecnologias de informação e comunicação (CEDH, 2023b).

Tendo em vista o grande volume de decisões da CEDH relacionadas à proteção de dados, as decisões (documentos), pertinentes a cada tema abordado na presente pesquisa, foram selecionadas a partir da plataforma de Compartilhamento de Conhecimento da CEDH (*ECHR Knowledge Sharing platform* – ECHR-KS), ferramenta criada pela Corte com o objetivo de

[4] Foram citadas as seguintes decisões da CEHD: Caso Van der Velden vs. Holanda, nº 29.514/2015; Decisão de 7 de dezembro de 2006; Caso S.e MARPER vs. Reino Unido, Decisão de 4 de dezembro de 2008; Caso Peruzzo e Martens vs. Alemanha (nº 30.562/2004 e nº 30.566/2004); e Decisão de 4 de dezembro de 2008 (STF, 2016).

sistematizar as pesquisas da jurisprudência acerca da Convenção Europeia de Direitos Humanos (CEDH, 2023a). A plataforma ECHR-KS permite o acesso às decisões da CEDH por meio de um artigo da Convenção específico, ou tema transversal determinado, bem como por meio de materiais e *links* de relevância geral para a jurisprudência (CEDH, 2023b). Para o escopo da presente pesquisa, o documento base selecionado foi o *Guide to the Case-Law of the of the European Court of Human Rights – Data Protection*, um guia de jurisprudência que oferece uma visão geral das decisões da CEDH sobre o tema da proteção de dados, organizado por artigo da Convenção e atualizado regularmente (CEDH, 2023b)

3.1.1.4. Critérios de inclusão de na análise documental e seleção dos aportes teóricos relacionados à Ciência da Informação

O tratamento de dados pessoais, para efeitos de detecção, investigação, prevenção e repressão de crimes tipificados em lei, também se relaciona, em grande medida, às manifestações da Ciência da Informação (CI). A gestão de enormes volumes de dados no âmbito dos órgãos de segurança pública tem passado por soluções inovadoras, impulsionadas pelo constante avanço das tecnologias de armazenamento em termos de descrição, classificação e organização da informação. Nesse contexto, a CI pode desempenhar um papel significativo em auxiliar as atividades policiais na organização eficaz dos dados e conhecimentos acumulados, fornecendo argumentos robustos sobre os benefícios do uso de sistemas da organização do conhecimento e do tratamento de dados pessoais, no âmbito das atividades de investigação criminal. Assim, a integração dos princípios da CI nas práticas das agências de segurança pública está alinhada com o cenário contemporâneo orientado por dados, quando informações mais precisas e acessíveis são fundamentais.

A organização de imensas massas de dados, no âmbito dos órgãos de segurança pública, vem passando por novas e criativas soluções. Há o constante incremento de tecnologias de armazenamento de dados e outras possibilidades tecnológicas em termos de descrição, classificação e organização da informação. Ao mesmo tempo, teorias da CI podem contribuir para desenvolvimento de sistemas eficientes, que garantam que aquelas informações críticas permaneçam acessíveis ao longo do tempo. Ao recorrer aos fundamentos teóricos da CI, as instituições policiais podem implementar estratégias sólidas para a preservação, organização e recuperação de dados. Assim, partindo-se da premissa de que se uma informação é importante para a polícia, ela deve ser preservada (Bush, 1945), os fundamentos teóricos da CI também foram aplicados na presente pesquisa.

Pesquisas de diversos campos da CI foram selecionados para o presente trabalho, principalmente dentre os autores inclusos no conteúdo programático do PPGCIN-UFSC. Neste sentido, destacam-se os referenciais teóricos relacionados à “gestão da informação e do conhecimento” e à “organização do conhecimento”, dois conceitos inter-relacionados, mas distintos, que desempenham papéis fundamentais no gerenciamento eficaz dos recursos de informação dos órgãos policiais.

Os referenciais teóricos da gestão da informação são fundamentais na criação das estratégias para lidar com todos os aspectos dos recursos de informação das instituições policiais. Por sua vez, os sistemas de organização do conhecimento (SOC) mostram-se imprescindíveis para a estruturação e a organização técnica dos recursos informacionais das polícias, visando facilitar a recuperação e o uso pelos agentes públicos usuários. Ambos os conceitos são necessários para garantir a utilidade, acessibilidade e preservação das informações policiais em uma variedade de contextos, incluindo as ações de prevenção, investigação criminal e definição de análises estratégicas e táticas.

As teorias da CI também foram selecionadas sobre o enfoque semântico do conhecimento registrado, a partir da consolidação da visão tripartite de dado, informação e conhecimento. Por esta visão, a informação se situa como elemento intermediário entre o conhecimento registrado na mente das pessoas e os dados, sendo estes elementos sem significado em seu estado bruto (Uchôa; Sales, 2023). A relação conceitual entre dado, informação e conhecimento tem reflexo direto na criação de sistemas de proteção dos dados pessoais, pois toda abordagem normativa sobre o tratamento de dados deve necessariamente se utilizar de conceitos e terminologias que são objeto de estudo no âmbito da CI, tais como dado, informação, sistemas de informação e banco de dados.

Essas teorias podem ajudar a compreender como esses conceitos devem ser interpretados, de acordo com os diferentes contextos que envolvem as atividades de prevenção, investigação, detecção ou repressão de infrações penais, e de execução das sanções penais. Assim a CI pode fornecer as bases conceituais e práticas necessárias para garantir que o tratamento de dados pessoais, no âmbito policial, seja conduzido de maneira ética, eficiente e alinhada com os princípios fundamentais de proteção e garantia individual.

Também deve ser ressaltada a inclusão da teoria sistêmica da CI como referencial teórico da pesquisa. Os estudos da teoria sistêmica da informação buscaram determinar e caracterizar os diversos processos necessários para o adequado funcionamento dos sistemas de informação, privilegiando a ideia de ciclo: todo processo sempre representa a saída de alguma entidade, ou *output*, e essa saída vai provocar a formação de novos elementos de entrada, ou

input (Araújo, 2018).

A teoria sistêmica da CI oferece subsídios valiosos para a discussão dos ciclos de produção do conhecimento policial – ou ciclo de inteligência –, um conjunto de fases interconectadas que compõem o processo de requisição, coleta, análise, produção e disseminação de informações e conhecimento, para apoiar as atividades de segurança pública. Por este enfoque, os analistas policiais devem entender o ciclo de inteligência não como único e possivelmente interminável, mas sim como algo mais orgânico. Deve-se compreender que a informação flui em várias direções, e que as etapas do ciclo se refletem sobre si mesmas, em um mecanismo de constante retroalimentação (James, 2016).

Entretanto, além da seleção de correntes teóricas específicas da CI, procurou-se também verificar a presença dos temas principais desta dissertação nas pesquisas da CI realizadas no Brasil. Para verificar como a CI vem incluindo no Brasil o tema da proteção de dados para fins de segurança pública e investigação criminal, bem como seus reflexos sobre os direitos individuais dos titulares dos dados no aspecto dos direitos humanos, foi consultada a Base de Dados do ENANCIB (BENANCIB). Através de uma busca simples pelos principais termos individuais[5], foram encontrados os seguintes resultados (termo/número de hits): “dados” (815 resultados), “pessoais” (46), “proteção” (36), “polícia” (05), “policial” (03), “segurança” (38), “pública” (161) “investigação” (185), “crime” (05), “criminal” (03), “direitos” (51) e “humanos” (60). Não foi possível identificar nenhum artigo diretamente relacionado com os sistemas de proteção de tratamento de dados pessoais no âmbito policial (BENANCIB, 2023).

Por sua vez, foram analisados trabalhos realizados no campo da CI relacionados ao conceito de privacidade. Pelos estudos identificados, verifica-se que no escopo da CI o conceito de privacidade é de difícil definição e carece de maiores discussões, motivo pelo qual o termo vem desencadeando estudos a fim de se encontrar um consenso nas pesquisas (Gristo, Sant´Ana, Segundo). Para alguns autores, privacidade poderia ser definida como o direito do indivíduo de determinarem quando, como e quais informações sobre eles poderão ser divulgadas a outras pessoas ou organizações (Westin, 1967 *apud* Affonso; Oliveira; Sant’Ana, 2017).

Do mesmo modo, também é comum encontrar estudos do campo da CI que tratam da questão da privacidade sob o enfoque da definição de quem é o proprietário do dado, de acordo com a natureza da informação publicada, do meio em que foi obtida e dos controles aplicados, principalmente em relação aos dados fornecidos espontaneamente em diversos locais da web

5 A plataforma do BENANCIB não realiza pesquisa por termos compostos ou expressões como “dados pessoais”, apenas palavras individuais.

(Milagre; Sengundo, 2015). Entretanto, quando a privacidade é tratada pelo prisma da atividade policial, que se caracteriza pela realização do tratamento de dados sem a anuência ou mesmo do conhecimento de seu proprietário ou titular, o tema principal passa a ser o dos limites e das justificativas de poder do Estado para interferir na esfera da vida privada dos cidadãos. Este é o enfoque utilizado no presente trabalho.

3.1.2. Etapa 2 – Leitura e análise dos documentos, artigos e obras selecionados

A segunda etapa da pesquisa, direcionada à realização da análise documental e aplicação do referencial teórico selecionado na pesquisa, foi iniciada com a leitura aprofundada e análise criteriosa dos documentos e referenciais teóricos previamente identificados e selecionados. Trata-se de etapa crucial para a compreensão aprofundada dos elementos que compõem os domínios-chave, que definimos anteriormente, desempenhando um papel fundamental na construção da base conceitual que sustenta a pesquisa. Na análise documental e aplicação do referencial teórico, foi atotado o seguinte processo:

i) *Leitura e familiarização com os documentos selecionados*: processo teve início com a leitura minuciosa e aprofundada dos documentos escolhidos, que englobam normativos legais que tratam do tema, pincipalmente a Diretiva UE nº680/2016 (União Europeia, 2016b); decisões judiciais, notadamente a jurisprudência da CEDH; artigos científicos e demais obras relevantes. O objetivo foi o de alcançar uma compreensão completa do conteúdo de cada documento, contextualizando-os dentro do microssistema legislativo europeu de proteção de dados pessoais;

ii) *Identificação de padrões e relações entre documentos analisados e os aportes teóricos incluídos*: durante a leitura, foram identificadas as conexões entre os documentos e os referenciais teóricos selecionados. Essas ligações foram exploradas em relação ao poder do Estado de realizar o tratamento de dados pessoais em atividades policiais, considerando a necessidade de equilíbrio entre os benefícios da segurança pública e os riscos aos direitos individuais. Do mesmo modo, as teorias derivadas da CI, principalmente os Sistemas de Organização do Conhecimento e a Teoria Sistêmica da Informação, foram utilizadas ao longo de toda pesquisa, sendo sempre verificada a sua relação com as atividades policiais de tratamento de dados;

iii) *Análise crítica e integração teórica*: foi realizada uma análise abrangente dos documentos, considerando diferentes perspectivas e interpretações. A integração dos referenciais teóricos, incluindo as teorias de direitos humanos e os conceitos da Ciência da

Informação, permitiram uma compreensão mais profunda dos temas abordados na pesquisa;

iv) *Identificação de regras e princípios intercambiáveis*: devido à complexidade que envolve qualquer processo de adaptação de modelos normativos, originados em outros países, com a multiplicidade de elementos históricos e ideológicos que caracterizam o microssistema legislativo europeu de proteção de dados pessoais, esta pesquisa buscou selecionar nos documentos e teorias analisadas somente as ideias, conceitos, regras e princípios que podem ser aplicados na atividade policial de uma forma geral e em todos os países.

Os resultados da segunda etapa da pesquisa foram efetivamente incorporados ao capítulo da dissertação dedicado à análise documental e ao referencial teórico (Capítulo 3). Este capítulo pode incluir *insights* sobre o embasamento teórico e normativo das políticas de proteção de dados, a necessidade de se manter o equilíbrio entre segurança pública e direitos individuais, bem como a influência da CI na construção de sistemas de informação e na análise dos dados pessoais em atividades policiais. Em resumo, a segunda etapa da pesquisa envolve uma profunda imersão na leitura, análise crítica e integração dos documentos e referenciais teóricos selecionados. Essa etapa desempenha um papel crucial na estruturação do trabalho, oferecendo uma base sólida que sustentará a análise, a elaboração dos resultados e as discussões posteriores.

3.1.3. Etapa 3 – Sistematização das informações extraídas dos normativos, artigos e obras e apresentação dos resultados por meio de tabelas estruturada

De acordo com os objetivos específicos desta dissertação (ver subseção 2.2), estes consistem em:

a) Analisar os padrões normativos internacionais de proteção e salvaguarda de direitos no tratamento de dados pessoais, realizados por organizações policiais, com ênfase nos dispositivos da Diretiva UE neu680/2016 e no Regulamento UE nº 794/2016 (Regulamento Europol – RE);
b) Analisar as salvaguardas e mecanismos de mitigação de risco de violação dos direitos dos titulares dos dados;
c) Classificar os tipos de dados pessoais que são produzidos ou coletados pelas polícias;
d) Classificar as categorias de tratamento de dados pessoais realizadas pelos órgãos de segurança pública;
e) Sistematizar, em forma de tabelas, os princípios e normas relacionadas à proteção e à garantia dos direitos e liberdades individuais dos titulares de dados.

O primeiro e segundo objetivos indicados consistem, de certo medo, na própria execução da segunda etapa da pesquisa, conforme o processo de análise documental e aplicação do referencial teórico descrito. Os resultados referentes ao terceiro objetivo específico, ou seja, a sistematização dos princípios e normas de proteção de dados pessoais no âmbito das atividades policiais, foram também apresentados no Capítulo 4, referente aos resultados da pesquisa. Para a facilitar a apresentação de tais resultados, com a disposição em tabelas estruturadas dos princípios e regras que devem nortear os sistemas nacionais de tratamento de dados pessoais na atividade policial, foram utilizados os referenciais da teoria sistêmica da Ciência da Informação (Araújo, 2018).

De acordo com as referida corrente teórica, os sistemas de informação passaram a ser pensados a partir da lógica dos processos de entrada (entrada de dados, com a aquisição de itens informacionais, e a seleção destes itens para a composição de determinado acervo); de processamento (os itens informacionais que dão entrada num sistema de informação precisam ser descritos, catalogados, classificados, indexados); e de saída (pelo acesso aos itens informacionais por parte dos usuários, na forma de disseminação, entrega da informação). Assim, na apresentação dos resultados da pesquisa, foi realizada a distinção, por meio de tabelas, dos diversos princípios e normas selecionados, conforme as respectivas fases do tratamento de dados, ou seja: i) regras e princípios de entrada; ii) regras e princípios de processamento; e iii) regras e princípios de saída.

Por fim, tanto o quarto objetivo específico, referente à classificação dos diversos tipos de dados pessoais coletados e armazenados pelas elas polícias, quanto o quinto objetivo, com a classificação das categorias de tratamento dos dados realizados no âmbito da segurança pública, foram objeto de resumo detalhado no capítulo da dissertação referente à apresentação dos resultados (Capítulo 4). Ressalte-se, entretanto, que tais classificações se deram com base na análise documental e na aplicação do marco teórico da pesquisa, consistindo uma das temáticas também exploradas no decorrer do Capítulo 3 (análise documental e referencial teórico).

4. REFERENCIAL TEÓRICO

Para alcançar os objetivos a que se propõe, o referencial teórico deste trabalho está estruturado em quatro partes. A primeira trata dos referenciais teóricos que fundamentam e justificam o poder do Estado de realizar o tratamento de dados pessoais em atividades policiais, com vistas a demonstrar a necessidade do balanceamento entre os benefícios sociais de segurança pública e os riscos aos direitos individuais, que são representados pela atividade policial de tratamento de dados. A segunda parte aborda a origem dos mecanismos de proteção dos dados pessoais, analisando as salvaguardas presentes em regras de proteção da privacidade e da garantia da liberdade informacional. A terceira parte versa sobre os aspectos gerais e conceitos norteadores do sistema de proteção de dados pessoais, abordando o panorama normativo internacional e nacional que versam sobre o tema, notadamente o Regulamento UE nº 679/2016 (RGPD) e a Lei Geral de Proteção de Dados (LGPD). Por fim, a quarta parte do referencial teórico aborda as diversas classes de dados pessoais coletados e armazenados, bem como as diversas finalidades pelas quais as polícias realizam o tratamento de dados pessoais. Esta última parte do trabalho também abordará as principais salvaguardas de mitigação de risco de danos causados aos titulares dos dados, no processo de tratamento realizados pelos órgãos policiais.

4.1. SISTEMA DE PROTEÇÃO DE DADOS PESSOAIS

A sociedade contemporânea está passando por uma profunda integração de tecnologias na vida diária das pessoas, uma transformação que teria sido inimaginável há duas décadas. A tecnologia relacionada à coleta e processamento de dados, informação e sistemas de comunicação contribuem para aprimorar diversos aspectos do cotidiano. Essa evolução dá origem a uma sociedade baseada em informações, na qual praticamente tudo é quantificável, e tanto indivíduos quanto uma ampla variedade de dispositivos eletrônicos permanecem interconectados o tempo todo por meio da internet. Essa rede de conexões e sensores fornece uma quantidade fenomenal de dados, e oferece diversas possibilidades fascinantes que, juntas, são frequentemente chamadas de *big data* (Klous, 2016).

O termo *big data* tem se tornado muito popular nos últimos anos, sendo frequentemente descrito em termos dos 5 V's: Volume, Variedade, Velocidade, Veracidade e Valor. Este termo pode estar associado a valores sociais, sendo utilizado, por exemplo, para reduzir o congestionamento do tráfego por meio da análise inteligente dos movimentos de

smartphones. Do mesmo modo, pode aumentar os rendimentos agrícolas, com base em informações obtidas por meio da varredura de terras agricultáveis, por exemplo, com satélites ou drones.

Por outro lado, o *big data* pode representar uma ferramenta a ser utilizada por empresas que desejam aprender tudo o que há para saber sobre seus clientes para, então, poder vender cada vez mais coisas para eles. De qualquer forma, o *big data* proporcionou a oportunidade para que vários setores da economia fossem organizados de maneira diferente, oferecendo produtos e serviços, e realizando atividades que eram impossíveis até recentemente. Novas empresas causaram mudanças nos mercados ao adotarem abordagens inovadoras para lidar com dados, como pode ser citado o exemplo da Uber. Essencialmente, a empresa Uber não está no negócio de táxis, mas sim no negócio de vender dados de clientes para uma rede de motoristas de táxi, e vice-versa, otimizando a rede de táxis por meio de uma maior inteligência de dados (Klous, 2016).

Ao mesmo tempo, o desenvolvimento de novas tecnologias de coleta e armazenamento de dados pessoais permitiu a realização do tratamento de informações em massa (metadados). Estes podem, por exemplo, direcionar ou induzir o comportamento político de eleitores, com realização de análises preditivas avançadas, a partir da definição do perfil de um indivíduo.

O uso de sistemas de *big data* por empresas privadas contratadas para campanhas eleitorais se tornou tema corrente, devido à revelação do escândalo envolvendo as empresas *Cambrige Analytica* e Facebook, que teriam coletado dados pessoais de milhões de usuários da rede social para o desenvolvimento de um sistema de *microtargeting* comportamental, direcionando conteúdo específico de propaganda política para cada grupo de pessoas que era segmentado, a partir de traços de personalidade em comum. O sistema automatizado da *Cambrige Analytica* foi capaz de descobrir o tipo de anúncio publicitário que levava cada categoria de usuário a se engajar em um determinado tema, desde segurança nacional até a proteção dos animais. Isto permitiu à empresa influenciar os processos eleitorais de diversos países, como no chamado *Brexit*, referendo ocorrido no Reino Unido em 23 de junho de 2016 e que decidiu pelo desligamento da nação do bloco da União Europeia (Kaiser, 2020).

Assim, a partir do reconhecimento da importância de uma legislação clara na área da proteção de dados, diversos países passaram a incluir em suas agendas legislativas a necessidade da aprovação de novas medidas de proteção dos dados pessoais de seus cidadãos. Desde então, a União Europeia tem procurado implementar um novo arcabouço legislativo visando estabelecer regras relativas à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União Europeia, bem

como pelo Estados-Membros no exercício de atividades abrangidas pelas normas relativas à livre circulação desses dados. Por sua vez, o cumprimento dessas regras passou a ser controlado por autoridades independentes, inclusive no que diz respeito ao tratamento de dados pessoais, para fins de prevenção, investigação, detecção ou processamento de uma ofensa criminal, ou de execução de uma sanção penal.

Nesta nova estrutura de proteção de dados pessoais, o principal instrumento criado foi o Regulamento Geral de Proteção de Dados (RGPD; Regulamento nº 679/2016), que reviu o quadro jurídico geral da UE em matéria de proteção de dados pessoais com a criação de novas regras sobre o processamento e recuperação de dados pessoais. Os principais objetivos políticos dessa reforma eram: i) modernizar o ordenamento jurídico da UE em matéria de proteção de dados pessoais, nomeadamente para fazer face aos desafios decorrentes da globalização e da utilização das novas tecnologias; ii) reforçar os direitos dos indivíduos e, ao mesmo tempo, reduzir as formalidades administrativas, para garantir o livre fluxo d dados pessoais dentro e fora da UE; e iii) melhorar a natureza e a coerência das regras da UE em matéria de proteção de dados pessoais, e alcançar uma implementação e aplicação coerentes e efetivas do direito fundamental à proteção de dados pessoais, em todos os domínios de atividade do bloco europeu (União Europeia, 2016a).

Entretanto, RGPD excluiu de seu escopo o tratamento de dados pessoais efetuados pelas autoridades competentes para efeitos de investigação e criminal e segurança pública (União Europeia, 2016a). Entretanto, no âmbito do mesmo pacote de reformas do seu microssistema legislativo de proteção de dados, a União Europeia aprovou a já mencionada Diretiva UE nº 680/2016, um ato jurídico específico, que se aplica à proteção de dados pessoais no que diz respeito ao tratamento para efeitos de prevenção, investigação, detecção ou repressão de infrações criminais, e execução de sanções penais, bem como à livre circulação desses dados (União Europeia, 2016b).

Este normativo foi criado para fazer frente aos avanços tecnológicos que impulsionaram os métodos de coleta e armazenamento de dados pessoais pelas polícias. A exigência a adoção de regras específicas regulamentando o tratamento de dados pessoais pelas polícias tornou-se, assim, um componente básico dos ordenamentos jurídicos que valorizam a proteção dos direitos individuais

A Diretiva UE nº 680/2016 possui escopo significativamente mais restrito daquele mencionado no Regulamento UE nº 679/2016 (RGPD), que procurou estabelecer regras gerais de proteção pessoal, principalmente em relação às empresas privadas de tecnologia da informação. A norma sobre a proteção de dados no âmbito policial reconhece que, caso o

conjunto de direitos especiais atribuídos aos indivíduos pelo RGPD forem exercidos em sua máxima extensão, tais como os direitos à informação sobre a existência de tratamento e o acesso aos dados tratados pelas polícias, esses mesmos direitos podem prejudicar em muito o trabalho da polícia e da justiça criminal (Zampronha, 2021). Assim, em uma redação que permitiu uma flexibilidade em razão ao tipo de tratamento realizado pelas polícias, a referida diretiva europeia buscou estabelecer um claro equilíbrio entre o direito individual à proteção de dados, e os interesses e objetivos dos órgãos de persecução criminal (Hert, Papakonstantinou, 2016).

Assim, a partir do reconhecimento da importância de uma legislação clara na área da proteção de dados, diversos países passaram a incluir em suas agendas legislativas a aprovação de sistemas de proteção dos dados no âmbito policial. Além de estabelecerem as regras relativas à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais pelas instituições, esse novo arcabouço legislativo europeu também alcançou órgãos e organismos policiais da União Europeia, como a Europol e a Frontex[6]. Igualmente, regulamentou as atividades relativas à livre circulação desses dados pessoais entre as polícias dos Estados-Membros da União Europeia.

Por sua vez, o cumprimento dessas regras passou a ser controlado por autoridades independentes, no que diz respeito também ao tratamento de dados pessoais para fins de prevenção, investigação, detecção ou processamento de uma ofensa criminal, ou de execução de uma sanção penal. Uma das implicações deste sistema de proteção sofisticado é que os dados pessoais só podem ser tratados caso tal atividade seja permitida por lei. Desta feita, para garantir clareza jurídica e fiabilidade nesta área sensível, as regras que regem o tratamento de dados devem conter expressões inequívocas e bem definidas, sendo necessário estabelecer claramente os contornos de conceitos como "dados pessoais" e "tratamento de dados".

4.1.1. Dados pessoais

Em termos gerais, pode ser considerado dado pessoal qualquer informação que se refere diretamente a uma pessoa, ou que possa ser usada para determinar sua identidade. Entretanto, em termos jurídico, o Art. 4, §1 do Regulamento Geral de Proteção de Dados da União Europeia apresenta a seguinte definição de dados pessoais:

[6] Agência Europeia da Guarda de Fronteiras e Costeira – FRONTEX, tem o objetivo de apoiar os países da UE e do espaço Schengen na gestão das fronteiras externas da EU, e na luta contra a criminalidade transfronteiras (Frontex, 2023).

> [...] qualquer informação relativa a uma pessoa natural identificada ou identificável (titular dos dados); é considerada identificável uma pessoa natural (pessoa física) que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa natural. (União Europeia, 2016a)

Podem ser citados como exemplos de dados pessoais nomes, datas de nascimento, características físicas, pseudônimos, fotografias, ocupação, endereços (residenciais e/ou trabalho), endereços de e-mail, números de telefone, números de identificação pessoal, entre outros, ou qualquer combinação de tais dados. Por sua vez, seriam exemplos de dados não considerados pessoais o número de registro de empresas e dados anonimizados, ou seja, dados que perderam a possibilidade de serem associados, direta ou indiretamente, a um indivíduo, em razão da utilização de meios técnicos específicos (Europol, 2023).

Verifica-se, assim, que o conceito extraído do RGPD possui três elementos que servem para classificar uma informação como dado pessoal: i) qualquer informação; ii) relacionada a uma pessoa natural; iii) identificada ou identificável. A definição desses elementos, por sua vez, é fundamental para compreensão da amplitude do conceito de dados pessoais. Por exemplo, ao se referir a "pessoa natural" – ou pessoa física – o RGPD declara que dados sobre empresas, que são consideradas "pessoas jurídicas", não são dados pessoais. Do mesmo modo, dados relacionados a pessoas falecidas não são considerados dados pessoais na maioria dos casos sob cobertura da RGPD (União Europeia, 2023).

O RGPD torna o conceito de dados pessoais muito inclusivo ao usar a expressão "qualquer informação". Assim, podem ser definidos como dados pessoais tanto informações "objetivas", como a altura de um indivíduo, quanto informações "subjetivas", como avaliações de perfil. Do mesmo modo, os dados pessoais não estão limitados a nenhum formato específico, podendo incluir dados numéricos, dados gráficos e registros em foto, vídeo ou áudio. Por exemplo, o desenho de uma criança sobre seus parentes, feito como parte de uma avaliação psiquiátrica, para determinar como ela se sente em relação a diferentes membros de sua família, pode ser considerado um dado pessoal, na medida em que essa imagem revela informações relacionadas à criança (sua saúde mental, como avaliado por um psiquiatra) e o comportamento de seus pais (União Europeia, 2023).

Mesmo quando as informações são atribuídas de forma imprecisa a uma pessoa específica, com a reunião de informações que, na realidade, estariam relacionadas a outro indivíduo, ainda assim são consideradas dados pessoais no que se refere ao titular dos dados. Somente se os dados forem imprecisos, a ponto de nenhum indivíduo poder ser identificado, as

informações deixam de ser consideradas dados pessoais. Por exemplo, se alguém se referir ao "homem que mora na Rua Agnaldo Silva, n. 107, que teria adquirido um carro último modelo", quando a Rua Agnaldo Silva termina no número 100, essa informação não pode ser considerada um dado pessoal (União Europeia, 2023).

Entretanto, o Art. 4º do RGPD define como sendo dado pessoal qualquer informação relativa a uma pessoa singular identificada ou identificável. Em sua forma mais básica, pode-se afirmar que, sempre quando um indivíduo é diferenciado dos outros, este indivíduo está sendo identificado. Diferenciar alguém pelo nome é a forma mais básica de identificar uma pessoa. Entretanto, existem milhões de "Marias" no Brasil, não sendo possível distinguir um indivíduo somente com esse dado. Mas ao adicionar outro ponto de dados ao nome, como por exemplo um endereço, passariam a existir informações suficientes para identificar uma pessoa específica. Esses pontos de dados são denominados identificadores (União Europeia, 2023).

Em acréscimo à definição dos tipos de informações que estão incluídas no conceito de dados pessoais, o Art. 4, §1 do RGPD apresenta uma lista de diferentes identificadores, tais como "*um nome, um número de identificação, dados de localização, um identificador eletrônico*". Neste sentido, uma menção especial deve ser feita para os dados biométricos, como impressões digitais, e os genéticos, como o DNA, que também podem ser aplicáveis como identificadores.

Embora a maioria dos identificadores sejam simples, os identificadores eletrônicos, ou *online*, são um pouco mais complexos, motivos pelo qual o RGPD fornece vários exemplos (Considerando N. 30): i) endereços de protocolo de *internet* (IP); ii) identificadores de *cookies*; e iii) outros identificadores, como etiquetas de identificação por radiofrequência (RFID). Os identificadores eletrônicos, de uma forma geral, relacionam-se às ferramentas, aplicativos ou dispositivos informáticos de um indivíduo, como seu computador ou *smartphone*. Assim, qualquer informação que possa identificar um dispositivo específico, como sua impressão digital, pode ser considerada como um identificador eletrônico (União Europeia, 2023).

A abordagem do conceito de dados pessoais, por fim, levanta a seguinte questão: quando uma pessoa é considerada identificável, designadamente por referência a um ou mais fatores, como o nome e o número de identificação? Neste sentido, as normativas europeias buscaram esclarecer que a definição de que uma pessoa "pode ou não ser identificada" é certamente, antes de mais nada, uma questão de meios (Europol, 2012)

> Para determinar se os meios são razoavelmente susceptíveis de serem utilizados para identificar a pessoa singular, devem ser tidos em conta todos os fatores objetivos, tais como os custos e o tempo necessário para a identificação, tendo em consideração a

> tecnologia disponível no momento do processamento e os desenvolvimentos tecnológicos. (Considerando 26 da eu PD nº 679/2016 e Considerando 21 Diretiva UE nº 680/2016).

Desse modo, tais regras estabelecem que um indivíduo não deve ser considerado "identificável" se a identificação exigir uma quantidade excessiva de tempo, custo e mão de obra empregada no tratamento dos dados. Assim, um indivíduo não é considerado como "identificável" se o tratamento dos dados envolver um esforço excessivo, e que não possa ser investido realisticamente na identificação de uma pessoa. Por isso, para definir se uma pessoa "pode ou não ser identificada", conforme definição legal, seria necessário definir o esforço necessário e os meios utilizados para a identificação da referida pessoa (Comissão Europeia, 2023).

Caso os dados pessoais sejam criptografados, ou se forem utilizados pseudônimos para a ocultação de nomes, e mesmo assim permaneçam passíveis de serem decodificados e utilizados na identificação das pessoas relacionadas, eles ainda continuam sendo considerados dados pessoais, se enquadrando no escopo do sistema de proteção da RGPD nº 679/2016. Somente dados pessoais que tenham sido tornados anônimos de forma que o indivíduo não seja mais identificável, não são considerados dados pessoais. Para que os dados sejam verdadeiramente anonimizados, e deixem serem considerados dados pessoais, a anonimização deve ser irreversível (União Europeia, 2023).

Um indivíduo é diretamente identificável se ele puder ser identificado somente com os dados já disponíveis. No exemplo anterior, com o nome e localização, é possível identificar à qual "Maria" determinado dado está se referindo. No entanto, o nome nem sempre seria necessário. Se o nome de Maria não for conhecido, ainda assim ela poderia ser identificada por meio de alguma combinação de fatores físicos, como altura e cor do cabelo. As informações que identificam um indivíduo, mesmo sem um nome associado a ele, podem ser consideradas dados pessoais, se tais informações forem processadas com o objetivo de se descobrir algo sobre esse indivíduo. Igualmente, no caso de o processamento de trais informações tiver algum tipo de impacto ou consequência sobre esse indivíduo (União Europeia, 2023)[7].

Já a identificação indireta significa que a pessoa não pode ser pode identificada por meio das informações que o detentor dos dados possui, sendo necessário acessar outras fontes. Por exemplo, um órgão policial que combina dados de uma empresa com informações de bancos de dados policiais, para realizar a identificação de indivíduos específicos, realiza uma

[7] European Union. General Data Protection: Regulation Compliance Guidelines. Disponível em: https://gdpr.eu/eu-gdpr-personal-data/. Acesso em: nov. 2023.

forma de identificação indireta. Um exemplo simples de informação, que pode ser usada para identificar indiretamente uma pessoa, é o número da placa de um veículo. A polícia pode rapidamente associar o nome de uma pessoa ao número das placas de carros, dados que são coletados e armazenados por determinada empresa de estacionamento, o que levanta discussões sobre o tipo de proteção que deverá incidir sobre tais dados.

Assim, verifica-se que o qualificador "identificável" é muito importante na definição do conceito de dados pessoais, pois métodos de processamento para a identificação de indivíduos que não existem hoje podem ser desenvolvidos no futuro. Isso significa que os dados armazenados por longos períodos devem ser continuamente avaliados e protegidos, garantindo que não possam ser tratados com novas tecnologias, as quais permitiriam a identificação indireta de pessoas de forma indevida, ou sem o respeito às garantias individuais necessárias. Qualquer informação que possa levar à identificação direta ou indireta de um indivíduo provavelmente será considerada dado pessoal (União Europeia, 2016a).

Por fim, devem ser destacados os dados que, por sua natureza especial, são considerados sensíveis e merecem um nível maior de proteção. Seguindo o mesmo parâmetro adotado no Regulamento Geral de Proteção de Dados da União Europeia (RGPD), o Artigo 5º, Cap. II, da LGPD (Brasil, 2018b) classifica como "sensível" os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, bem como dos dados referente à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculado a uma pessoa natural. Segundo as normas da LGPD, o tratamento de dados pessoais sensíveis somente poderá ocorrer em hipóteses específicas, como a execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos (Brasil, 2018b).

4.1.2. Tratamento de dados pessoais

Segundo o Art. 4º, § 2 do Regulamento Geral de Proteção de Dados da União Europeia (RGPD), é considerado tratamento de dados pessoais

> [...] qualquer operação ou conjunto de operações realizadas sobre dados pessoais ou conjuntos de dados pessoais, seja por meios automatizados ou não, tais como coleta, registo, organização, estruturação, estruturação, conservação, adaptação ou alteração, recuperação, consulta, utilização, divulgação por transmissão, disseminação ou qualquer outra forma de disponibilização, comparação, interconexão, limitação, apagamento ou destruição. (União Europeia, 2016a).

Para o RGPD qualquer tipo de ação realizada com dados pessoais é considerado um tratamento. Informações e dados pessoais dos indivíduos são processados em muitos aspectos da vida cotidiana, como por exemplo, abertura de conta bancária, inscrição em uma academia, reserva de voo, emissão de cartão de crédito, registro de cartões de fidelidade em lojas. Do mesmo modo, os próprios indivíduos, em suas atividades cotidianas, processam dados pessoais, quando, por exemplo, criam uma lista de participantes de um evento.

Neste sentido, a Corte de Justiça da União Europeia (CJUE) já decidiu que mesmo a vigilância realizada por CFTV, que envolve a gravação e armazenamento de dados, consiste em um tipo de tratamento automático de dados, que se enquadra no escopo das leis de proteção de dados da União Europeia (União Europeia, 2016a). Assim, devem ser garantidos os mecanismos de proteção contra o tratamento abusivo de dados. Isto porque, se as informações pessoais sobre uma pessoa foram imprecisas, desatualizadas ou divulgadas de forma indevida, o dano causado ao indivíduo pelo tratamento de dados pode ser bastante sério. Uma situação plausível de ocorrência, é que esse indivíduo possa ter um contrato de trabalho injustamente recusado, ao ser confundido com outra pessoa, ou até mesmo se tornar vítima de roubo de identidade.

Organizações ou indivíduos que controlam o conteúdo e o uso de dados pessoais são conhecidos como controladores de dados. De acordo com a LGPD, os indivíduos possuem direitos sobre como seus dados pessoais são utilizados, e os controladores de dados têm responsabilidade sobre como lidam com essas informações. Por exemplo, nada impede que empresas de estacionamento realizem o registro das placas automotivas para fins de controle de acesso e movimentação de clientes, mas esses dados não poderão ser utilizados por essas empresas para se determinar a identidade dos proprietários ou dos usuários dos veículos.

Quando uma pessoa fornece seus dados pessoais a uma organização, empresa ou indivíduo, ela tem o direito de ter mantidos esses dados protegidos e seguros. Aqueles que não respeitam esses direitos podem ser considerados culpados por divulgação não autorizada de informações. De qualquer forma, deve-se levar em consideração a finalidade do tratamento a ser realizado, verificando como os dados estão sendo usados para tomar decisões sobre indivíduos específicos. Uma informação que não se qualifica como dados pessoais para uma organização pode se tornar um dado pessoal para uma organização diferente, em razão do impacto que esses dados podem ter sobre o indivíduo, e de acordo com os motivos pelos quais a organização está processando os dados.

Assim, quando uma organização processa dados, com o único propósito de identificar alguém, tais dados passam a ser, por definição, dados pessoais. Outro exemplo, uma foto de

uma rua nas mãos de um fotógrafo não é um dado pessoal, enquanto essa mesma foto nas mãos de um investigador policial, que está trabalhando para identificar os indivíduos e veículos que estavam presentes naquela rua, em um momento específico, seria considerada como dados pessoais dos indivíduos investigados (União Europeia, 2023).

Segundo a Diretiva 95/46/EC de Proteção de Dados do Conselho da Europa (CoE), o processamento automatizado de dados é definido como operações realizadas com dados pessoais, no todo ou em parte por meios automáticos. Assim, verifica-se que a definição de processamento de dados pessoais reconhece a possibilidade do uso manual dos mesmos, com a realização de operações "não automatizadas". Dessa forma, a legislação da UE se aplica a dados pessoais processados de duas maneiras: i) dados pessoais processados, total ou parcialmente, por meios automatizados (ou informações em formato eletrônico); e ii) dados pessoais processados de maneira não automatizada, que fazem parte de um "sistema de arquivamento", ou registros escritos, em um sistema de arquivamento manual (União Europeia, 2023).

Em termos práticos, tal definição significa que qualquer processamento automatizado de dados pessoais e que envolva o uso de um dispositivo informático, como, por exemplo, um computador pessoal, um dispositivo móvel ou um roteador, pode estar coberto pelas regras de proteção de dados da União Europeia **(**Agência dos Direitos Fundamentais da União Europeia, 2018). Assim, em processo envolvendo o motor de busca *Google Search*, a CJUE declarou que, ao explorar a internet de forma automatizada, constante e sistemática, na busca das informações nela publicadas, o operador de um motor de busca recolhe esses dados, que recupera, registra e organiza posteriormente no âmbito dos seus programas de indexação. Do mesmo modo, este operador conserva as informações nos seus servidores e, se for caso disso, as coloca à disposição dos seus utilizadores, sob a forma de listas de resultados das suas pesquisas. Assim, o CJUE concluiu que tais ações constituem "tratamento", independentemente de o operador do motor de busca efetuar as mesmas operações também com outros tipos de informação, que não são distinguidas dos dados pessoais (Corte de Justiça da União Europeia, 2014b).

Como anteriormente mencionado, a proteção de dados não está limitada a sistemas de tratamento automatizados. Da mesma forma, no próprio tratamento automatizado, podem existir algumas etapas de utilização manual de dados pessoais. Assim, a proteção de dados também se aplica ao tratamento de informações pessoais em sistemas manuais de classificação e consulta. Ou seja, desde que se envolva o conjunto de dados pessoais estruturados, de acordo com critérios específicos de classificação por categorias, permitindo que sejam recuperados e consultados, os sistemas de ficheiros em papel também estão sujeitos às regras de proteção ao tratamento de dados. O motivo dessa ampliação da proteção de dados é que tais sistemas

manuais podem ser estruturados, de modo a permitir a localização das informações pessoais de forma fácil e rápida, possibilitando ao mesmo tempo contornar as restrições impostas pela lei ao tratamento automatizado de dados (Agência dos Direitos Fundamentais da União Europeia, 2018).

4.1.3. Contexto nacional

O novo marco normativo europeu para o tratamento de dados fascinou acadêmicos do Direito, legisladores e jornalistas de várias partes do mundo, tendo em vista as inúmeras novidades que trazia. Dentre estas, o direito ao esquecimento/apagamento, o direito à portabilidade de dados, o direito à limitação de tratamento de dados pessoais, a introdução de conceitos como *privacy by design* (privacidade desde a concepção) e *privacy by default* (privacidade por padrão), além de novas regras para transferência internacional de dados (Zampronha, 2021).

Assim, não tardou para que tais novidades legislativas também aportassem no Brasil, tendo o RGPD UE nº 679/2016 servido como texto base da Lei nº 13.709/2018, a denominada Lei Geral de Proteção de Dados (LGPD). Aprovada pelo Congresso Nacional em 18 de agosto de 2018, a LGPD introduziu o tema da proteção do tratamento de dados pessoais no sistema jurídico brasileiro (Brasil, 2018b).

Ao definir dado pessoal como sendo toda informação relacionada à pessoa natural, identificada ou identificável, a LGPD utilizou os mesmos elementos do conceito apresentado no Regulamento Geral de Proteção de Dados (RGPD) – Regulamento UE nº 679/2016. Do mesmo modo, outras definições e conceitos do RGPD passaram a fazer parte do ordenamento jurídico brasileiro, tais como (Brasil, 2018, n.p.):

i. *Dado pessoal sensível:* dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural);
ii. *Dado anonimizado*: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
iii. *Titular do dado*: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
iv. *Controlador*: pessoa natural ou jurídica, de direito público ou privado, a quem

competem as decisões referentes ao tratamento de dados pessoais;

v. *Operador*: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

vi. *Autoridade nacional*: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.

Do mesmo modo, o conceito de tratamento de dados pessoais, apresentado na LGPD, possui a mesma abrangência daquele adotado pelo RGPD da União Europeia, compreendendo toda operação realizada com dados pessoais, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (Brasil, 2018b). Em suma, tanto para a normativa europeia quanto para a LGPD brasileira, qualquer tipo de ação realizada sobre os dados pessoais é considerado um tratamento.

Ainda seguindo um paralelo com o RGPD europeu, a LGPD também excluiu de seu escopo o tratamento de dados pessoais relacionados à segurança pública e à investigação criminal, estabelecendo expressamente a necessidade de aprovação de lei específica (Art. 4º, caput, inciso III, alínea “a” e “d”, c/c § 1º). Entretanto, diferentemente do que ocorreu na União Europeia que concomitantemente ao RGPD aprovou a Diretiva UE nº 680/206 (União Europeia, 2016b), o parlamento brasileiro ainda não aprovou um ato jurídico específico que se aplique à proteção de dados pessoais, no que diz respeito ao tratamento para efeitos de prevenção, investigação, detecção ou repressão de infrações criminais, e execução de sanções penais, bem como à livre circulação desses dados. Em outros termos, o Brasil ainda não dispõe de uma legislação sistematizada sobre a proteção contra o tratamento de dados pessoais no âmbito das atividades policiais, bem como não existe uma padronização clara das normas relacionadas ao desenvolvimento de bancos de dados e sistemas de informação policiais. Esses sistemas são essenciais para a coleta, armazenamento, processamento e utilização de dados pessoais, que podem ser originados tanto pelas próprias instituições policiais quanto por organizações públicas ou privadas.

É importante ressaltar que as poucas leis que existem atualmente no Brasil não conseguem abranger, de forma adequada, a complexidade atual das tecnologias de coleta e tratamento de dados utilizados pelos organismos policiais, deixando vácuos significativos na proteção dos direitos dos cidadãos. Este seria o caso da Lei nº 13.675/2018, que criou a denominada Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e institui o Sistema Único de Segurança Pública (SUSP), com a finalidade de preservação da ordem por

meio de atuação conjunta, coordenada, sistêmica e integrada dos órgãos de segurança pública brasileiros. Segundo a referida lei, o SUSP possui como órgão central o Ministério da Justiça e Segurança Pública (MESP), e é integrado pelos órgãos de que trata o Art. 144 da Constituição Federal – nominalmente, Polícia Federal, Polícia Rodoviária Federal, Polícias Civis e Polícias Militares dos Estados, Polícias Penais e Guardas Municipais – e pelos demais integrantes estratégicos e operacionais, que atuarão nos limites de suas competências, de forma cooperativa, sistêmica e harmônica (Brasil, 2018a).

O Artigo 7º da Lei nº 13.675/2018 define que a PNSP será implementada por estratégias que garantam o diagnóstico dos problemas de criminalidade a serem enfrentados, a excelência técnica dos órgãos policiais, a avaliação continuada dos resultados e a garantia da regularidade orçamentária, para execução de planos e programas de segurança pública. Por sua vez, a Seção II da referida lei elenca princípios da PNSPDS que estariam diretamente relacionados à criação de sistemas de informação policial, tais como a necessidade de conferir publicidade às informações policiais não sigilosas (inciso XI) e a promoção da produção de conhecimento sobre segurança pública (inciso incisos XI e XII do Art. 4º) (Brasil, 2018, n.p.).

Do mesmo modo, a PNSPDS teria dentre seus objetivos (Seção IV), dentre outros, o de estimular a produção e a publicação de estudos e diagnósticos para a formulação e a avaliação de políticas de segurança, bem como integrar e compartilhar as informações de diversos órgãos policiais nacionais (Artigo 6º, incisos VI e X). Tais objetivos estão vinculados a um modelo de atuação policial orientada pela informação, indicando que a PNSP reconhece a importância da criação de sistemas de organização da informação policial e a elaboração de análises criminais para a orientação da atividade policial no país (Brasil, 2018a).

Além de elencar princípios e objetivos, a Lei nº 13.675/2018 também menciona a criação do Sistema Nacional de Informações de Segurança Pública, Prisionais, de Rastreabilidade de Armas e Munições, de Material Genético, de Digitais e de Drogas (SINESP), um banco de dados de informações policiais administrados pelo Ministério da Justiça e da Segurança Pública, e disponibilizado aos diversos órgãos integrantes do SUSP.

O SINESP teria por objetivo, dentre outros, proceder à coleta, análise, atualização, sistematização, integração e interpretação de dados e informações relativos às políticas de segurança pública e defesa social. Fariam parte do SINESP os bancos de dados de perfil genético e digitais, bem aqueles relacionados à rastreabilidade de armas e munições (Artigos 35 e 36).

Com base nas informações disponibilizadas em um banco de dados nacional sobre crimes e criminosos, o Ministério da Justiça e Segurança Pública (MJSP) poderia conduzir

operações ostensivas, investigativas, de inteligência ou mistas, que seriam combinadas, planejadas e desencadeadas em equipe, contando com a participação de órgãos integrantes do SUSP (Artigo 10, § 2º). Assim, pela descrição contida na Lei nº 13.675/2018 (Brasil, 2018a), o funcionamento do SINESP envolveria necessariamente o tratamento de dados pessoais, sendo o esboço de um possível sistema de organização do conhecimento policial.

Entretanto, verifica-se que a Lei nº 13.675/2018 se apresenta, em grande parte, como uma declaração geral de princípios, diretrizes e objetivos, possuindo um enfoque bastante semelhante ao daquele adotado no Projeto Segurança Pública para o Brasil, elaborado ainda em 2001. Não foram previstos os fluxos de informação e cooperação efetiva entre os diversos atores envolvidos, com a definição das tarefas de cada instituição policial integrante do SUSP. Embora os objetivos da lei somente possam ser alcançados por meio do tratamento de dados pessoais, também não foram estabelecidas quaisquer regras de proteção de dados pessoais a serem seguidas pelos controladores e usuários do banco de dados, bem como normas ou princípio relacionados a modelos de organização do conhecimento, a serem, por sua vez, adotados no âmbito do SINESP.

A Lei nº 13.675/2018 teria deixado de definir claramente a finalidade pela qual cada tipo de dado deve ser coletado e armazenado no âmbito do SINESP, com o estabelecimento de limitações temporais, que possam garantir que os dados sejam conservados apenas durante o período necessário e em razão de motivos determinados, explícitos e legítimos. Assim, verifica-se no contexto nacional uma total carência de normas regulamentado o desenvolvimento de sistemas de informação policial, inexistindo regras para assegurar um nível adequado de proteção aos direitos fundamentais das pessoas que terão seus dados armazenados e tratados pelos órgãos de segurança pública, incluindo as medidas técnicas ou organizativas que limitem os tratamentos de dados não autorizados ou mesmo ilícitos.

Entretanto, deve ser ressaltado que qualquer abordagem normativa sobre o tratamento de dados deve necessariamente utilizar-se de temas e ideias amplamente debatidos nos estudos realizados no âmbito da CI, como as teorias que abordam a definição de dado e a sua distinção dos conceitos de informação e conhecimento, bem como as diversas abordagens relacionadas à gestão da informação e dos sistemas de organização do conhecimento. Essas teorias podem ajudar a compreensão de como esses conceitos se relacionam, e como podem ser aplicados em diferentes contextos, incluindo aqueles do tratamento de informações em sistemas de informação policial. Assim a CI pode fornecer as bases teóricas e práticas necessárias para garantir que o tratamento de dados pessoais seja conduzido de maneira ética, eficiente e alinhada com os princípios fundamentais de proteção e garantia individual.

4.2. A APROXIMAÇÃO ENTRE A CIÊNCIA DA INFORMAÇÃO E A ATIVIDADE POLICIAL

A relação entre a Ciência da Informação e a atividade policial pode ser ilustrada por J. Edgar Hoover (1895-1972), umas das figuras mais influentes e controversas da história do *Federal Bureau of Investigation* (FBI), a Polícia Federal estadunidense. Ele serviu como diretor do FBI por quase cinco décadas, de 1924 até a sua morte em 1972, sendo o diretor mais longevo e poderoso da agência. Entretanto, antes de se tornar o diretor icônico do FBI, J. Edgar Hoover, durante sua juventude e início da carreira, trabalhou na Biblioteca do Congresso em Washington, considerada a maior dos Estados Unidos, e que buscava conservar um exemplar de todos os livros publicados no país. Essa grande biblioteca poderia transmitir a sensação de que todo o conhecimento estava ao alcance da mão, se a pessoa soubesse onde buscá-lo (Winer, 2012).

A Biblioteca do Congresso contava com seu próprio sistema de classificação, e Hoover aprendeu sua complexidade como catalogador, ganhando dinheiro para pagar a universidade arquivando e recuperando informações. Em 1917, Hoover deixou a Biblioteca e conseguiu um emprego como escriturário no Departamento de Justiça dos EUA, onde sua história se tornou mais conhecida (Winer, 2012).

A experiência de Hoover como bibliotecário e a sua organização inovadora do conhecimento, muitas vezes, foram creditadas por influenciarem a criação do próprio sistema de gerenciamento de conhecimento do FB (*FBI Files*). O sistema de arquivamento que Hoover ajudou a arquitetar tornou-se conhecido por sua eficiência e, ao longo dos anos, serviu de fonte para livros, notícias e filmes. Entretanto, o sistema de arquivamento do FBI não utilizou o modelo de arquivamento da Biblioteca do Congresso, tendo sido baseado no tipo de caso que o arquivo cobre (FBI, 2023).

Cada arquivo é designado por um número de classificação como, por exemplo, casos de sequestro começam com o número 7, enquanto casos de espionagem com o número 65. No entanto, a metodologia de Hoover teve um impacto significativo em como o sistema de arquivamento do FBI foi usado e adaptado, tendo o próprio ex-diretor do FBI declarado que o seu trabalho na biblioteca havia lhe ensinado o "[...] *valor da coleta de material. Isso me deu uma base excelente para o meu trabalho no FBI, onde foi necessário reunir informações e evidências*" (FBI, 2023).

Essa capacidade de sintetizar informações foi fundamental quando Hoover, ao assumir como diretor assistente, supervisionou a reforma dos arquivos do FBI, que estavam em

desordem após várias reestruturações organizacionais. Nesta reforma, Hoover utilizou algo antigo, o sistema do Departamento de Justiça, e o misturou com algo novo, a indexação dos arquivos à medida em que estes eram criados. Ao mesmo tempo, ele utilizou algo emprestado da Biblioteca do Congresso: a ideia de extensas referências cruzadas dentro dos índices de cartões que davam acesso ao conteúdo dos arquivos do FBI (FBI, 2023).

Cada referência cruzada apontava para o arquivo original, e permitia a comparação de informações em todos os arquivos. Assim, um agente ou funcionário poderia encontrar o nome de uma pessoa, um evento, um local ou qualquer outra coisa, mesmo que estivesse espalhado por dezenas de arquivos diferentes na Sede da agência, na capital estadunidense, e nos escritórios de campo do FBI. Ao final, o trabalho de Hoover na Biblioteca ajudou o FBI a criar um sistema de arquivamento que, em comparação com outros da época, era muito avançado. Embora a carreira de Hoover tenha tomado um caminho diferente ao final, sendo considerado o artífice da espionagem interna e maior adversário dos movimentos civis nos Estados Unidos, sua experiência em bibliotecas e a sua compreensão da importância da organização e do acesso a informações influenciaram uma abordagem rigorosa em relação à coleta, análise e uso de dados durante sua liderança na agência de investigação (FBI, 2023).

Em uma área que exige informações ao alcance das mãos, e a capacidade de saber tudo o que está disponível sobre crimes e criminosos, a CI é crucial em qualquer modelo de tratamento de dados no âmbito da atividade policial. Como ocorre no campo de conhecimento relacionado à CI, a polícia está sempre preocupada com a origem, coleção, organização, armazenamento, recuperação, interpretação, transmissão, transformação, e utilização da informação sobre atividades criminosas. Por sua vez, dentre as preocupações dos órgãos de segurança pública, também pode ser considerado o uso de códigos para a transmissão eficiente da mensagem, além do estudo do processamento e de técnicas aplicadas aos computadores e seus sistemas de programação. Desse modo, qualquer estratégia moderna de atuação das instituições de segurança pública deve buscar abordagem interdisciplinar da CI, tais como matemática, ciência da computação, artes gráficas, comunicação, biblioteconomia, administração e outros campos científicos semelhantes (Borko, 1968).

A atividade policial é focada na localização, coleta, organização, armazenamento, recuperação, interpretação, transmissão, transformação, e utilização de dados pessoais (de diferentes tipos de informações, relacionadas às atividades criminosas). Por outro lado, a CI, como como campo específico de conhecimento, oferece percepções e métodos visando o aprimoramento da eficiência na gestão de dados de aplicação policial. Levando em consideração o fundamento de que toda informação importante para as organizações deve ser

preservada e utilizada da maneira mais eficiente possível (Bush, 1945), as teorias da CI tornam-se cada vez mais relevantes no âmbito da segurança pública. Isso ocorre porque a informação não possui somente a utilidade imediata, mas também possui relevância futura potencial, seja em investigações, análises ou processos de tomada de decisão.

O ponto de partida da CI é a percepção da importância da informação e do tratamento de dados como recurso dentro das organizações. Sendo um campo especialmente sensível às exigências de eficácia e eficiência em relação aos vários recursos organizacionais disponíveis no mundo, esta área sofreu os efeitos da chamada "explosão da informação". Embora a informação seja compreendida, cada vez mais, como um recurso importante para as organizações, instituições e empresas, o seu excesso também se constitui um problema.

Os problemas relacionados ao excesso de informações ocorrem tanto em termos de uso, devido à dificuldade de se encontrar a informação que se quer em um universo muito amplo; quanto dos entraves à sua circulação, para garantir que ela chegue a todos os setores que dela precisam, em vez de ficar estocada em um único ponto. Do mesmo modo, o excesso de informações gera problemas também em relação ao seu volume físico, devido à necessidade de se dispor de locais cada vez maiores para armazená-la. Assim, as primeiras reflexões sobre a gestão da informação policial devem incidir sobre sua natureza física, com a realização de projetos de pesquisa visando reduzir o excesso, otimizar a circulação, identificar com precisão as necessárias e descartar as inúteis ou redundantes (Araújo, 2014).

Devido ao grande volume de dados que coletam, e de informações que são produzidas, as instituições policiais utilizam "memórias artificiais" (Bush, 1945). Estas memórias artificiais têm o intuito de permitirem a recuperação, transmissão e armazenamento de todo conhecimento que primeiramente surge na mente do policial, viabilizando a realização de um registro que pode ser compartilhado e acessado por outras pessoas.

O ponto central para a produção de informações de qualidade é a capacidade das polícias de acessarem dados de plataformas distintas, reunindo a mais ampla gama de fontes relevantes de informação. Em uma abordagem holística, a gestão da informação policial deve levar em consideração as pessoas, as políticas de segurança pública, os processos, os dados e a tecnologia de apoio, a fim de garantir que, no âmbito policial, a informação certa seja acessada pela pessoa certa no momento certo (Fletcher, 2000).

Identificar e descrever com precisão os problemas de segurança pública enfrentados pelas polícias é o primeiro passo para se encontrar as melhores soluções, sendo necessário a existência de instrumentos para armazenar, ordenar e acessar os dados e informações com eficiência e rapidez. Assim, existe uma relação direta entre a atividade policial, em sua busca

constante de informações sobre crimes e criminosos, e a CI. Esta, segundo Harold Borko, é a "disciplina que investiga as propriedades e o comportamento informacional, as forças que governam os fluxos de informação, e os significados do processamento da informação, visando à acessibilidade e a usabilidade ótima" (Borko, 1968, p. 3). Ao organizar as estruturas conceituais próprias do campo policial, formulando representações esquematizadas do conhecimento policial acumulado, a CI pode auxiliar na navegação pela busca de dados e informações relevantes, atuando na construção de uma ponte entre os recursos informacionais e o usuário policial (Sanches, 2017).

Existe uma diferença essencial entre simples motores de busca, que são operados sobre arquivos das instituições policiais, e os sistemas de informação construídos a partir de fundamentos teóricos da CI. Motores de busca podem representar uma tecnologia impressionante, sendo que sua importância como ferramenta para encontrar documentos e informações relevantes dentre de uma instituição policial não pode ser subestimada. No entanto, tais motores de busca também possuem suas limitações (Hjørland, 2021).

Quando um usuário faz uma pesquisa em determinado sistema como o Google, normalmente digita algumas palavras e estuda a primeira parte da lista de resultados. Este sistema resulta na recuperação de um conjunto de documentos, em resposta a uma entrada de pesquisa, denominado "transformação de consulta", o que implica ao usuário a obrigação de conhecer as palavras (ou outros símbolos) que correspondem às palavras (símbolos) nos documentos que deseja recuperar. Isso coloca um problema teórico, pois parece ser impossível selecionar termos de documentos que você não conhece; pois se você já os conhecesse, não estaria fazendo uma busca por assunto (Hjørland, 2021)[8].

Assim, para que uma pessoa possa realizar sua pesquisa em documentos desconhecidos, ela terá que se basear em conceitos utilizados em determinado contexto, com o estabelecimento de conceitos, categorizações e classificações. Desse modo, a atividade policial orientada pela informação deve se utilizar as teorias da CI, para auxiliar seus esforços de organização dos bancos de dados policiais, de modo a tornar disponível a melhor informação e da forma mais eficiente.

O exercício do poder de coletar, armazenar e analisar dados e informações constitui o cerne das instituições policiais, sendo desejável a sua relação entre com as diversas correntes

[8] O problema de conhecer termos de busca relevantes é menor, obviamente, porque uma busca inicial pode fornecer *hits* contendo outras palavras em potencial para a pesquisa, mecanismo relacionado às tecnologias conhecidas como "expansão de consulta", e que geralmente depende parcialmente de sistemas de organização do conhecimento para identificar sinônimos, termos mais restritos etc. Isso significa que as pesquisas interativas solucionam parcialmente o problema de identificar termos de pesquisa relevantes (Hjørland, 2021).

teóricas da CI. Devido a essa relação evidente, torna-se bastante interessante a utilização dos conceitos desenvolvidos pela CI na análise e compreensão da atividade de tratamento de dados realizada no âmbito policial. Entretanto, no discurso científico, os conceitos teóricos não são elementos verdadeiros ou falsos, bem como o vislumbre de um elemento da realidade já definido de antemão, sendo constructos projetados para atender uma determinada necessidade da melhor maneira possível (Hjørland; Capurro, 2007). As definições elaboradas no âmbito da CI para termos como dado, informação e conhecimento são, portanto, fundamentais para a identificação dos elementos constitutivos da atividade policial de tratamento de dados.

4.2.1. Dado, informação e conhecimento

Dentro do campo da CI, existem várias correntes teóricas que abordam a distinção entre dados, informações e conhecimento. Essas teorias ajudam a compreender como esses conceitos se relacionam e são aplicados em diferentes contextos, podendo ser bastante úteis na definição dos termos utilizados em normas de proteção de dados pessoais, bem como no desenho de sistema de informação e organização do conhecimento policial. Como referência de um estudo nesta área, pode ser citada a teoria de Nonaka e Takeuchi, que aborda a interação entre o conhecimento tácito – aquele incorporado nas experiências individuais – e o conhecimento explícito – formalizado e documentado.

Para os referidos autores, o processo de conversão entre esses tipos de conhecimento é fundamental para a geração e aplicação do conhecimento organizacional. Do mesmo modo, o denominado "Funil do Conhecimento" é frequentemente utilizado, para descrever a ideia de que o processo de aprendizado e aquisição de conhecimento começa com uma ampla gama de informações, a parte mais larga do funil; e conforme o aprendizado avança, o conhecimento se torna mais específico e refinado, representando a parte mais estreita do funil (Ceballos; Arias, 2018, p. 674).

Essa metáfora do funil é comumente usada para representar a forma como as pessoas assimilam informações e adquirem conhecimento, passando por diferentes níveis de compreensão e especialização à medida que avançam em seus estudos ou experiências. Os itens de dados se referem a uma descrição elementar de coisas, eventos, atividades e transações, que são registradas, classificadas e armazenadas, mas não são organizadas para transmitir qualquer significado específico (Rainer; Prince; Cegielski, 2013). Os itens de dados podem ser números, letras, figuras, sons e imagens, bem como coleções de números (por exemplo, 3,11, 2,96, 3,95, 1,99, 2.08) e caracteres (por exemplo, B, A, C, A, B, D, F, C).

Figura 1 – O funil do conhecimento.

Fonte: Ceballos e Arias (2018, p. 674).

Entretanto, tais dados devem representar fatos conhecidos, que podem ser registados, possuindo um significado implícito (Navathe; Elmasri, 2010). Dados também podem ser fluxos de fatos brutos, que representam eventos ocorridos nas organizações ou no ambiente físico, antes de terem sido organizados de uma forma que as pessoas possam compreender e usar (Laudon, 2014), como o registro de imagens coletadas em sistemas de CFTV.

Por sua vez, informações, em seu conceito mais básico, são dados moldados de uma forma que passam a ter significado e valor para o destinatário (Laudon, 2014); ou seja, são dados organizados de modo útil para os seres humanos (Rainer, Prince, Cegielski, 2013). Entretanto, o impacto da tecnologia da informação nas ciências naturais e sociais, especialmente, tornou esta noção quotidiana de informação num conceito altamente controverso, tendo a CI utilizado este termo em diversas perspectivas teóricas diferentes (Hjørland, Capurro, 2007). Buckland identificou três principais usos da palavra informação em pesquisas da CI:

i) Informação-como-processo (*becoming informed*): a informação é o ato de informar, a comunicação do conhecimento ou a notícia de algum fato ou ocorrência;

ii) Informação-como-conhecimento (*knowledge*): informação é aquilo que é o destinatário recebe da "informação-como-processo", o conhecimento comunicado relativo a algum fato particular, assunto ou evento;

iii) Informação-como-coisa (*data, document*): informação se refere a objetos, como dados e documentos, que são identificados como informativos por terem a propriedade de

proporcionar conhecimento de algo (Araújo, 2018, p. 72-73).

A partir desses três usos da palavra informação, Buckland percebe a existência de duas distinções: i) a informação às vezes é percebida como entidade, e outras vezes como processo; ii) a informação algumas vezes é percebida como algo tangível, ou também como algo intangível. Com base nessa distinção, Buckland apresenta uma quarta definição de informação, o processamento da informação, que significa o tratamento, o manuseio e a obtenção de novas formas ou versões da informação-como-coisa (Araújo, 2018, p. 72-73).

Conforme Buckland, a principal característica da "informação-com-conhecimento" é a sua intangibilidade; ou seja, não se pode tocá-la ou medi-la de forma direta, pois conhecimento, crença e opinião são pessoais, subjetivos e conceituais. Entretanto, para serem comunicadas, as informações como conhecimento devem ser expressas, descritas ou representadas em alguma forma física, como um registro, texto ou comunicação, sendo convertida em uma “informação-como-coisa” (Buckland, 1991, p. 351-360). Resumidamente, o esquema de Buckland pode ser representado conforme a Figura 2.

Figura 2 – Representação do quadro de conceitos de informação de Buckland.

	INTANGIBLE	TANGIBLE
ENTITY 2.	Information-as-knowledge Knowledge	3. Information-as-thing Data, document
PROCESS 1.	Information-as-process Becoming informed	4. Information processing Data processing

Fonte: Buckland (1991) apud Araújo (2018).

Importante notar que a informação, na atividade policial, pode ser também definida por três enfoques distintos, conforme modelo criado por Buckland: i) como um objeto, ou seja, um documento com conteúdo informativo a ser utilizado na atividade policial; ii) como um processo, através de um fluxo das etapas de requisição/demanda, produção, avaliação e difusão para seu destinatário; e, iii) como conhecimento, em forma da ampliação da compreensão pelos policias dos fatos relacionados a crimes e criminosos (Moreira; Muriel-Torrado, 2019, p. 16). Por esta abordagem, o conceito de "informação-como-coisa” é de interesse especial em relação aos sistemas policiais de tratamento de dados, porque, em última análise, os mecanismos de armazenamento e recuperação de informação lidam com a informação apenas neste sentido.

Por sua vez, a definição do conceito de informação foi discutida por Capurro ao longo de quase três décadas, com a busca das raízes históricas e da forma do uso deste termo em diferentes períodos. O autor representou uma visão da informação dividida nos paradigmas físico, cognitivo e social (Moreira; Muriel-Torrado, 2019, p. 14-15).

Pelo paradigma físico, a informação é um objeto, algo material, que um emissor transmite a um receptor. Este conceito de informação na CI é mais restrito, e está vinculado à sua dimensão física, sendo estudado somente a partir de uma perspectiva quantitativa e positivista. Já o modelo cognitivo relaciona informação a conhecimento, ou seja, a informação estaria associada à interação entre aquilo que existe materialmente (dados ou documentos) e aquilo que está na mente dos sujeitos (conhecimento), sendo seu estudo relacionado à identificação de significados e interpretações. Por fim, o paradigma social estaria voltado para a constituição social dos processos informacionais, buscando inserir o usuário nos seus contextos concretos de vida e atuação. Por esta visão, apenas a existência de um conhecimento compartilhado entre diferentes atores faz com que algo seja reconhecido como informação (Araújo, 2018).

Tanto o Regulamento UE n° 679/2016 (RGPD) quanto a Lei nº 13.709/2018 (LGPD) se referem ao termo "dado" em seu conceito básico, como sendo apenas números, caracteres, figuras, sons e imagens em estado bruto e com significado apenas implícito (Navathe, Elmasri, 2010). Como mencionado, as “informações-como-conhecimento”, para serem comunicadas, são expressas, descritas ou representadas em alguma forma física, como um registro, texto ou comunicação, sendo convertida em uma “informação-como-coisa”. Assim, no contexto das normas estudadas, o termo “dado” também englobaria as informações, aqueles dados que foram processados e moldados, de forma a se tornarem compreensíveis e relevantes para a tomada de decisões e ações específicas. Isto porque, antes se serem apenas resultados do processamento, tais informações podem ser submetidas a subsequentes tratamentos para a geração de novos conhecimentos. Assim, ao lidar com a proteção e garantias individuais, essa ampla interpretação do termo “dado” reflete a importância de considerar a natureza do tratamento de dados no atual estágio tecnológico de empresas e instituições públicas.

Neste ponto, torna-se necessário também analisar o próprio conceito de “conhecimento” na CI. Segundo Adriana Suárez Sánches, enquanto a informação é um dado que alguém pode encontrar, ler, rever, assimilar e utilizar, para acrescentar à percepção de mundo do destinatário, o conhecimento é um conjunto de saberes que somente podem ser alojados na mente humana e do qual são feitas representações materializadas (Sanches, 2017, p. 1-18). Desta feita, o conhecimento – que constitui um recurso importante para as

organizações – não é aquele que existe materialmente, mas sim, o que ainda não existe como entidade física, que está somente na mente das pessoas que pertencem à organização (Araújo, 2014). Em uma adaptação ao tema deste trabalho, não basta aos órgãos policiais gerirem seus recursos informacionais, sendo preciso também criar as condições propícias para transformá-los em conhecimentos preservados, armazenados e, principalmente, que possam ser consultados de forma ágil.

Do mesmo modo, todo o conhecimento abstrato formado na mente do policial, para se manifestar, requer sua transformação em dados ordenados, sendo a informação o substituto físico deste conhecimento. Assim, para melhorar a eficácia na realização de análises e investigações criminais, as organizações policiais devem estruturar suas bases de dados, de forma a permitir o uso mais eficiente da informação coletada ou produzida no dia a dia da atividade policial. Somente com a criação de sistemas de gerenciamento de dados e informações, com o uso de tecnologias da informação, torna-se possível transformar o vasto conhecimento que as polícias acumulam sobre a realidade criminal do país em conhecimentos, que sejam preservados, armazenados e principalmente consultados de forma eficiente.

4.2.2. Banco de dados, sistemas de gerenciamento de banco de dados e sistemas de informação

Segundo Buckland, o conceito de "processamento da informação" seria representado pelo tratamento, manuseio de itens de dados para a obtenção de novas versões da "informação-como-coisa" (Araújo, 2018, p. 24-25). Embora tanto o Regulamento UE n° 679/2016 (RGPD), na tradução da União Europeia para português (União Europeia, 2018a), quanto a Lei nº 13.709/2018 (LGPD) tenham utilizado o termo "tratamento" de dados, pode-se afirmar que "tratamento" e "processamento" são aqui expressões equivalentes.

Por sua vez, a análise dos conceitos relacionados aos processos que atuam sobre dados possibilitaria uma melhor interpretação das normas de proteção de dados pessoais, viabilizando sua adaptação a casos concretos. Desse modo, torna-se necessário para a presente pesquisa uma melhor compreensão do modo de funcionamento dos sistemas de processamento, ou tratamento, de dados.

Sistemas de banco de dados, bases de dados e sistemas de informação são elementos comuns na vida moderna, sendo que a maioria das pessoas se depara com atividades diárias que envolvem algum tipo de interação com uma base de dados. Por exemplo, ao visitarmos um

banco para efetuar depósitos ou saques, ao fazermos uma reserva de hotel ou passagem aérea, ao acessarmos um catálogo eletrônico de biblioteca para buscar informações bibliográficas, ou ao adquirirmos produtos pela internet, necessariamente existe a interação entre pessoas e programas de computador, que acessam bases de dados.

Essas interações representam exemplos de aplicações tradicionais de bases de dados, onde a maior parte das informações armazenadas e acessadas assume forma textual ou numérica. Entretanto, nos últimos tempos, progressos tecnológicos têm conduzido a outras aplicações de sistemas de base de dados. Graças à tecnologia de mídia digital, se tornou possível armazenar imagens, arquivos de áudio e fluxos de vídeo de forma digital. Tais tipos de arquivos estão rapidamente se tornando um componente fundamental de bases de dados multimídia. Sistemas de informações geográficas (*Geographic Information Systems – GIS*), por exemplo, têm a capacidade de armazenar e analisar mapas, dados meteorológicos e imagens de satélite.

Em muitas organizações, sistemas de processamento analítico online *(Online Analytical Processing - OLAP*) são utilizados para extrair e analisar informações úteis a partir de grandes bases de dados, com a finalidade de embasar decisões estratégicas. Além disso, técnicas de busca em bases de dados estão sendo aplicadas à *World Wide Web,* com o intuito de aprimorar a pesquisa por informações necessárias para os usuários que navegam na internet (Navathe; Elmasri, 2010).

Ao mesmo tempo, o uso pelas polícias de tecnologias de bancos de dados tem tido um impacto considerável no cotidiano da atividade policial. É justo dizer que os bancos de dados desempenham um papel crucial em todas as áreas da atividade policial onde os computadores são empregados, abrangendo consulta de pessoas, registro de ocorrências, investigações criminais, controle migratório, registros de armas, emissão documentos, interceptação telefônicas e telemáticas, extração de dados de dispositivos eletrônicos, perícias criminais, dentre outras áreas. Como exemplo, o Plano Diretor de Tecnologia de Informação e Comunicação (PDTIC 2020/2021) da Polícia Federal, cita a existência de 51 sistemas corporativos em produção, quatro em implementação e cinco em desenvolvimento, fora aqueles já existentes na instituição (Polícia Federal, 2020). Assim, o termo "banco de dados" (*database*) é tão comumente empregado no âmbito policial, que seria importante a sua melhor definição. Em uma conceituação inicial ampla, “banco de dados” seria uma coleção de dados que possuem algum tipo de informação (Silberschatz; Korth; Sudarshan, 2011), ou uma coleção de dados interconectados (Navathe; Elmasri, 2010).

Por exemplo, se uma pessoa registrar os nomes, números de telefone e endereços das pessoas que ele conhece em uma agenda indexada ou os tenha armazenado em um disco rígido,

usando um computador pessoal e *software* como o Microsoft Access ou Excel, essa coleção de dados, que são relacionados e possuem um significado implícito, constitui um banco de dados. Embora essa definição de dados seja muito abrangente[9], o uso comum do termo "banco de dados" geralmente é mais restrito, devendo possuir certas características implícitas. Assim, um banco de dados precisa refletir algum aspecto do mundo real, às vezes chamado de minimundo, universo de discurso (UoD) ou ambiente externo (Navathe, Elmasri, 2010)..

Neste sentido, alterações no minimundo devem ser refletidas no banco de dados. Ao mesmo tempo, um banco de dados é uma coleção logicamente coesa de dados, com um significado intrínseco. Uma coleção aleatória de dados não pode ser adequadamente referida como um banco de dados. Por fim, um banco de dados deve ser projetado, construído e preenchido com dados com um propósito determinado. Ou seja, o banco de dados deve ser destinado a um grupo de usuários específicos, e conter algumas aplicações preconcebidas nas quais esses usuários têm interesse (Navathe, Elmasri, 2010).

Os usuários de uma base de dados podem realizar transações comerciais (p.ex., um cliente compra uma câmera) ou informar eventos que podem ocorrer (p.ex., um funcionário tem um filho), o que faz com que as informações na base de dados se alterem. Para que uma base de dados seja precisa e confiável, ela deve ser um reflexo fiel do “minimundo”, ou do ambiente externo, que ela representa, devendo qualquer alteração ser refletida na base de dados o mais rápido possível.

Por sua vez, uma base de dados pode variar em tamanho e complexidade. Retomando, a lista de nomes e endereços mencionada anteriormente pode consistir em apenas algumas centenas de registros, cada um com uma estrutura simples. Por outro lado, o catálogo informatizado de uma grande biblioteca pode conter meio milhão de entradas, organizadas em diferentes categorias – pelo sobrenome do autor principal, por assunto, por título do livro –, sendo cada categoria organizada alfabeticamente. Essa imensa quantidade de informações deve ser organizada e gerenciada, para que os usuários possam buscar, recuperar e atualizar os dados conforme necessário (Navathe, Elmasri, 2010).

As bases de dados devem possuir fontes das quais os dados são derivados, um certo grau de interação com eventos no mundo real e determinado público, que esteja ativamente interessado em seu conteúdo. Por sua vez, as bases de dados podem ser geradas e mantidas manualmente, ou podem ser informatizadas. Em uma aplicação, o catálogo de fichas de

[9] Por este conceito amplo, retomando o exemplo dado, a coleção de palavras que compõem uma página de livro-texto poderia ser considerada como dados interligados e, consequentemente, como um banco de dados (Navathe, Elmasri, 2010).

biblioteca é uma base de dados que pode ser criada e mantida manualmente. Já as bases de dados informatizadas podem ser criadas e mantidas por um grupo de programas de aplicação, escritos especificamente para essa tarefa, ou por um sistema de gerenciamento de banco de dados.

Ressalte-se, assim, que este trabalho tem como objeto de atenção as bases de dados complexas e informatizadas, utilizadas no âmbito policial, tendo em vista que são esses sistemas que representam os maiores riscos às liberdades individuais dos titulares de dados e, por esse mesmo motivo, constituem o principal foco de atenção do sistema europeu de proteção de dados pessoais abordados nesta pesquisa. No entanto, para melhor compreender os fundamentos da tecnologia de dados (*database technology*), torna-se necessário abordar também o conceito de "sistema gerenciamento banco de dados" (*database management system - DBMS*), ou simplesmente, sistema de banco de dados. Este conceito se refere a uma coleção de dados inter-relacionados e a um conjunto de programas, que permitem aos usuários acessarem e modificarem esses dados. Um dos principais objetivos de um sistema de banco de dados é fornecer aos usuários uma visão abstrata dos dados, com a ocultação de certos detalhes sobre como estes são armazenados e mantidos, os chamados metadados (Silberschatz, Korth, Sudarshan, 2011).

Os sistemas de gerenciamento de banco de dados (*DBMS*) permitem ao usuário criar e manter um banco de dados, através de *softwares* que facilitam os processos de definição, construção, manipulação e compartilhamento de bancos de dados entre vários usuários e aplicativos. A "definição" de um banco de dados envolve a especificação dos tipos de dados, estruturas e restrições dos dados a serem nele armazenados. Por sua vez, a "construção" do banco de dados é o processo de armazenar os dados, em um meio de armazenamento controlado pelo sistema. Já a "manipulação" de um banco de dados inclui funções, como realizar consultas para obter dados específicos, atualizar informações para refletir as mudanças no ambiente em questão (minimundo) e gerar relatórios a partir dos dados armazenados. Por fim, compartilhar uma base de dados permite que vários usuários e programas a acessem simultaneamente (Navathe, Elmasri, 2010).

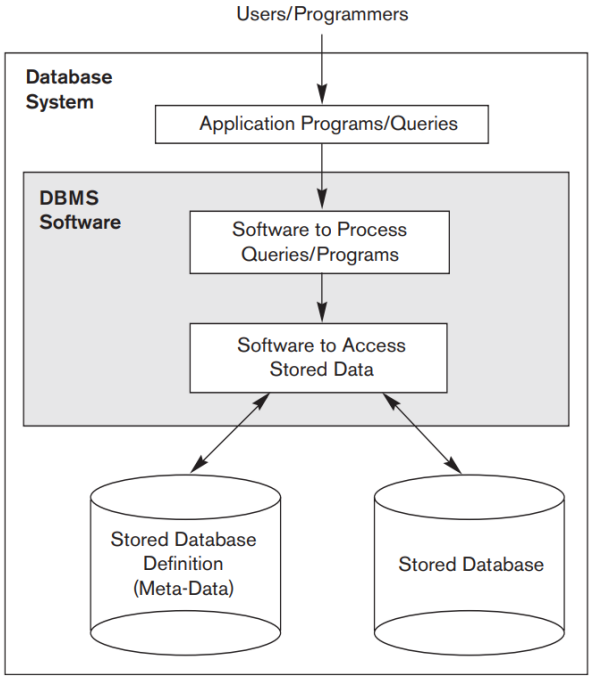
Sistemas de banco de dados são projetados (*database designs*) para gerenciamento de grandes volumes de informações que não existem isoladamente. Tais sistemas fazem parte do funcionamento de organizações ou empresas, cujo produto pode ser informações provenientes do banco de dados, bem como algum produto ou serviço, para o qual o banco de dados desempenha apenas um papel de apoio.

Assim, *database designs* envolve principalmente o projeto de um ambiente completo

de dados (minimundo), que atenda às necessidades da organização, requerendo a atenção a um conjunto amplo de questões. De um modo geral, um programa de aplicação acessa a base de dados enviando consultas (*queries*) ou solicitações (*requests*) de dados ao DBMS (*database management system*). Uma consulta (*query*) normalmente resulta na recuperação de dados e, por sua vez, uma requisição/transação (*transaction*) leva à leitura ou a inserção de dados na base (Silberschatz; Korth; Sudarshan, 2011). .

Adicionalmente, outras funções importantes fornecidas pelo DBMS incluem proteger e manter a base de dados ao longo do tempo, preservando o sistema contra o mau funcionamento de *hardware* ou s*oftware,* e garantindo proteção de segurança contra um acesso não autorizado ou malicioso. Uma base de dados complexa pode ter um ciclo de vida de muitos anos, portanto, o DBMS deve ser projetado de modo a manter um sistema de base de dados flexível, permitindo sua evolução conforme os requisitos mudem ao longo do tempo (Navathe; Elmasri, 2010). A Figura 3 ilustra alguns dos conceitos discutidos neste tópico.

Figura 3 – Modelo simplificado de sistema de gerenciamento de banco de dados.



Fonte: Navathe e Elmasri (2010, p. 7).

Por sua vez, existe também a distinção entre sistemas de banco de dados e sistemas de informação, conceitos que desempenham papel crucial na compreensão de como os dados são coletados, processados e utilizados para a tomada de decisões em diversos contextos. Enquanto ambos os tipos de sistemas têm um papel fundamental na gestão da informação, por outro lado, abordam diferentes estágios do ciclo de transformação dos dados em conhecimento útil. Essa

distinção se torna especialmente relevante no desenvolvimento de sistemas de informação policial, que desempenham um papel vital na prevenção, investigação, detecção e repressão de infrações criminais, bem como na execução de sanções penais.

Os sistemas de bancos de dados são projetados para armazenarem, organizarem e recuperarem grandes volumes de dados. Eles oferecem uma estrutura eficiente para lidar com informações estruturadas, permitindo o acesso rápido e a recuperação precisa dos dados. No entanto, os sistemas de banco de dados por si só não transformam esses dados em informações significativas: eles são a base sobre a qual os sistemas de informação são construídos.

Um Sistema de Informação (*information system*) pode ser definido tecnicamente como um conjunto de componentes inter-relacionados, que coletam (ou recuperam), processam, armazenam e distribuem informações, para apoiar a tomada de decisões e o controle em uma organização. Os sistemas de informação fornecem informações sobre pessoas, lugares e coisas importantes dentro da organização e no ambiente em que está inserido. Neste caso, informação é delimitada no sentido de dados organizados, de uma forma que as pessoas podem entender.

Para produzir as informações de que as organizações precisam para tomarem decisões, controlarem operações, analisarem problemas e criarem estratégias, produtos ou serviços, um sistema de informação realiza três atividades: entrada (*input*), processamento (*processing*) e saída (*output*). A atividade de entrada está relacionada à captura ou coleta dados brutos, sejam de dentro da organização ou de seu ambiente externo. Já o processamento converte os dados brutos em informações úteis. Por fim, a saída se refere à transferência das informações processadas para as pessoas que as utilizarão, ou para as atividades para as quais serão empregadas. Ao mesmo tempo, os sistemas de informação também exigem *feedback*, que o é resultado enviado aos membros apropriados da organização, para ajudá-los a avaliar ou corrigir o estágio de entrada (Laudon, 2014).

Os sistemas de informação (*information managmeent system* – IMS) têm uma abordagem mais abrangente que os sistemas de gerenciamento banco de dados (*database management system* - *DBMS*). Eles não apenas armazenam e organizam os dados, mas também os processam, analisam e interpretam, para gerarem informações valiosas. Essas informações são essenciais para a tomada de decisões informadas. No contexto policial, os sistemas de informação podem desempenhar um papel vital na coleta e análise de dados relacionados às atividades criminais. Eles não apenas registram eventos e informações, mas também fornecem análises estatísticas, geração de relatórios e previsões, para a orientação das ações das forças policiais.

A diferença entre esses dois tipos de sistemas tem implicações significativas na criação

de sistemas de informação policial. Um sistema de informação policial eficaz deve ser capaz de coletar dados brutos, armazená-los adequadamente em um banco de dados estruturado e, em seguida, transformá-los em informações significativas para os profissionais de segurança pública. Isso envolve a incorporação de ferramentas de análise avançada, recursos de geração de relatórios e de integração de informações de várias fontes, para auxiliar nas atividades de prevenção, investigação, detecção e repressão de crimes. Em suma, a compreensão da distinção entre sistemas de banco de dados e sistemas de informação é fundamental para a concepção e o desenvolvimento de sistemas de informação policial eficazes. Esses sistemas não apenas lidam com dados, mas os transformam em informações úteis, as quais auxiliam as forças de segurança em suas operações diárias e na promoção da justiça.

4.2.3. Sistema de organização do conhecimento

As instituições policiais realizam, necessariamente, atividades relacionadas à reunião, interpretação, recuperação e a apresentação, de dados e informações, sobre crimes e criminosos. Neste sentido, para lidar com as inúmeras modalidades criminosas existentes, as polícias precisam coletar diversos tipos de informações e dados, com origem nas mais variadas fontes, o que leva, ao final, à produção de conhecimento sobre a realidade criminal do país.

Para tanto, torna-se necessário tratar grades volumes de dados para fins de suporte à gestão do crime, ou para a predição de cenários criminais, através da utilização crescente de informação não estruturada, principalmente de cunho textual, para a produção do conhecimento e seu uso de forma útil. Por esse motivo, a organização das informações reunidas e dos conhecimentos produzidos no dia a dia das instituições policiais se constitui como importante e complexa tarefa.

Todo conhecimento abstrato formado na mente do policial, para se manifestar, requer sua transformação em dados ordenados, com o registro físico deste conhecimento na forma de documentos. Entretanto, seria um erro afirmar que os problemas relacionados ao desenvolvimento de sistemas de organização do conhecimento envolveriam apenas questões tecnológicas, os quais seriam solucionados quando o poder computacional e os algoritmos ótimos estivessem disponíveis às instituições policiais (Hjørland, 2021).

Não basta às instituições policiais administrarem os recursos informacionais por meio de sistemas computacionais, concentrando-se somente no desenvolvimento de ferramentas tecnológicas, sendo preciso também gerir o próprio conhecimento que estas produzem. Para tanto, as polícias devem utilizar as ferramentas auxiliares do processo de organização da

informação, tais como aquelas elaboradas no âmbito da Ciência da Informação, com a utilização dos arranjos já aplicados em distintos âmbitos, como arquivos científicos, museus, bibliotecas, dentre outros (Sánchez, 2017).

Diversos componentes da atividade policial possuem relação direta com a criação de Sistemas de Organização do Conhecimento (SOC), que possam permitir a realização da gestão, a análise e a recuperação da melhor informação, e da forma mais eficiente (Souza; Almeida; Baracho, 2015). Para tanto, o ponto de partida para a criação de qualquer SOC está na percepção da importância dos processos de armazenamento e busca da informação como recursos dentro das organizações, com a consequente a criação de sistemas de indexação, busca e classificação desenvolvidos no campo da Ciência da Informação.

Os SOC são um conceito que engloba todos os tipos de mecanismos para organizar a informação e promover a gestão do conhecimento. Constituem-se em modelos com estrutura voltada à exploração de conteúdos mediante termos, associações e atributos. Para que o conhecimento seja comunicado entre os indivíduos, inclusive de uma geração para outra, é necessário que ele possa ser manipulado por meio de uma representação específica, que se materializa em recursos de informação esquematizados. Assim, os SOC são instrumentos que facilitam o encontro de recursos de informação, e a sua recuperação através de indexações e classificações, atuando como mapas semânticos, os quais possibilitam uma orientação comum para futuros usuários, inclusive sistemas informatizados (Sanches, 2017).

Por sua vez, deve ser reconhecido que a representação total do conhecimento policial, com a definição de suas áreas exatamente como elas existem na realidade, não é possível de ser reproduzida em uma ferramenta computacional. Entretanto, o objetivo de um SOC policial deve ser representar, da melhor forma possível, os conhecimentos acumulados pelas instituições, de acordo com os diversos níveis temáticos da segurança pública. Assim, as estratégias de um sistema de organização do conhecimento policial se baseariam em dois propósitos elementares: i) atender às necessidades de usuários policiais individuais ou instituições de modo geral, enfatizando a organização de itens de informação de alta utilidade; ii) prover a organização completa, ou ao máximo nível possível, de toda a informação e conhecimento existente no âmbito dos órgãos de segurança pública (Emygdio, 2021).

Em termos de estrutura, os SOCs são diagramas gráficos e/ou textuais do universo do conhecimento, e em síntese baseados em três aspectos (Sanches, 2017, p. 1-18): i) conceitos como elementos representativos; ii) categorias para estabelecer níveis entre os elementos conceituais; e iii) relações entre as entidades conceituais que formam o conhecimento. Conforme Dahlberg, o conhecimento somente pode se fixar através de elementos de linguagem,

tendo em vista que o homem, desde que foi capaz de falar, emprega conjuntos de símbolos ou palavras para designar os objetos que o circundam, bem como para traduzir pensamentos formulados e os comunicar a seus semelhantes (Dahlberg, 1978).

Por sua vez, com a ajuda dessas linguagens naturais[10], torna-se possível a formulação de enunciados, a partir dos quais são elaborados conceitos individuais, referentes a objetos únicos e presentes no tempo e espaço (um crime específico, uma organização criminosa que atua em referia área etc.); ou conceitos gerais, relacionados a objetos situados fora do tempo (os crimes de colarinho branco em geral, as organizações criminosas de estilo mafioso etc.). Dessa forma, os conceitos são formados a partir da compilação de enunciados verdadeiros a respeito de determinado objeto (Dahlberg, 1978), constituindo ideias que formam o entendimento, expressas em palavras, que permitem descrever, classificar e prever elementos cognoscíveis (Sanches, 2017).

Hjørland (2021) ressalta que os sistemas para organizar documentos e informações envolvem, necessariamente, a organização de conceitos derivados de domínios de conhecimento específicos. Assim, no caso do conhecimento relacionado às atividades policiais, qualquer sistema de organização do conhecimento a ser criado deve ter como ponto de partida os diversos conceitos utilizados no campo de domínio da segurança pública, em grande parte derivados da Ciência do Direito.

Neste sentido, considera-se que tanto as necessidades informacionais, quanto as abordagens tecnológicas de um sistema de organização do conhecimento policial, serão influenciadas pela compreensão e conhecimento prévio dos atores envolvidos em seu desenvolvimento, incluindo-se os profissionais programadores de computador. Assim, seria necessária uma compreensão aprofundada acerca dos contextos social, jurídico e disciplinar das atividades dos órgãos de segurança pública, com a identificação de todas as formas de coleta e das etapas de tratamento dos dados, os quais são gerenciados pelas instituições policiais (Hjørland, 2021).

Os conceitos diferenciam e definem as entidades de um campo de conhecimento, possibilitando, por um lado, a sua existência do ponto de vista da organização do conhecimento, e por outro, a comunicação intrínseca e extrínseca do domínio. Os conceitos são a essência dos SOCs, pois a organização do conhecimento é basicamente a organização destes mesmos conceitos (Sanches, 2017).

---

[102]As linguagens naturais são aquelas utilizadas pelo homem nas necessidades da vida diária. Além da linguagem natural, o homem também criou as chamadas linguagens especiais ou artificiais, tais como a linguagem da matemática, linguagem da lógica, linguagem dos sistemas de classificação etc. (Dahlberg, 1978).

Desse modo, a construção de qualquer sistema de organização do conhecimento, no âmbito da segurança pública, deve envolver a análise conceitual dos diversos objetos abordados pelas polícias, tais como as inúmeras modalidades criminosas existentes no ordenamento jurídico (homicídio, roubo, crimes ambientais, corrupção, lavagem de dinheiro, fraudes eletrônicas etc.); e os inúmeros tipos de atores que praticam tais condutas (criminosos individuais, organizações criminosas de âmbito nacional ou regional, criminalidade internacional, colarinho branco etc.). As respectivas características de cada conceito do domínio policial, bem como da sua relação com outros conceitos que compõem o sistema de justiça criminal, implicam delimitações lexicais e semânticas precisas, que devem ser abordadas a partir de uma perspectiva linguística formal.

O segundo aspecto do SOC, a categorização, consiste na ordenação que é atribuída às pessoas, objetos ou conceitos, tendo por base suas características, atributos, qualidades, traços, entre outros aspectos. Deve-se partir da premissa de que, no mundo real, existem coisas com características comuns, que as permitem serem agrupadas (Sanches, 2017). A categorização constitui, em si, um princípio inerente à própria organização do conhecimento, na medida em que, a partir da identificação de um conjunto de traços comuns (que gera um critério ou uma diferença), é possível reunir coisas semelhantes e separar coisas diferentes. Todo processo de categorização implica a comparação entre as características das coisas, estabelecendo um princípio de ordem que obedece a um conjunto complexo e dinâmico de inferências (Guimarães, 2014).

O terceiro elemento dos SOCs são os relacionamentos, entendidos como associações entre enunciados e conceitos que compõem o domínio, os quais variam de acordo com os vários tipos de sistemas. Por exemplo, uma lista de assuntos não possui relacionamentos, enquanto as ontologias utilizam as relações como elemento substancial para representar um domínio. Desse modo, é fundamental definir que tipo de relacionamento cada sistema estabelece, e determinar como isso impacta na organização ou no resgate das informações que será realizado.

Um SOC pode apresentar relações hierárquicas, ou seja, com a determinação do maior e do menor termo, bem como outros relacionamentos atributivos, o que gera efeitos na recuperação da informação. De acordo com sua estrutura relacional, serão criados sistemas capazes de realizar maiores ou menores inferências, de acordo com as abordagens de consulta feitas pelos usuários, podendo ser consolidadas ferramentas que possibilitam a recuperação de informações por meio de questionamento direto (*query*) ou por navegação (*browsing*) (Sanches, 2017).

O uso de SOC pode ocorrer desde as primeiras atividades de organização dos dados e

informações, coletados em uma investigação criminal específica, até o contexto atual, caracterizado pela atuação policial proativa, com base no tratamento de grandes volumes de dados, e a partir do fornecimento de recursos que satisfaçam as necessidades de informação das instituições policiais. O SOC serve como uma ponte entre as buscas temáticas dos usuários e os materiais do acervo policial, permitindo a identificação de objetos de interesse, que aumentem o conhecimento de investigadores sobre determinada modalidade criminosa. Nesse quadro, sistemas de organização do conhecimento policial, projetados a partir de bases teóricas da CI, poderiam ajudar a evitar, da melhor forma possível, o desperdício de recursos onerosos, como o tempo e os investimentos financeiros, que são empregados no desenvolvimento de sistemas de processamento e armazenamento e nos itens de informação policial.

4.3. TRATAMENTO DE DADOS NO ÂMBITO POLICIAL

Assim como ocorre com a CI, uma ciência interdisciplinar derivada de vários campos relacionados, os órgãos de segurança pública realizam uma série de atividades também de caráter multidisciplinar, com a utilização de referenciais teóricos de diversas áreas ou domínios de conhecimento. Além de lidar com matérias estritamente relacionadas ao direito penal e a outros ramos da ciência jurídica, as polícias também possuem, dentre seus objetos de preocupação, o desenvolvimento de sistemas para a transmissão eficiente das informações e do conhecimento que administram, além do desenvolvimento de técnicas computacionais e códigos de programação relacionados à gestão e à análise dos dados. Isto porque, em sua atividade precípua de produzir conhecimento sobre crimes e criminosos, as polícias precisam coletar diversos tipos de dados, bem como conduzir múltiplos procedimentos de análise e produção de informações e conhecimentos.

A coleta de dados pessoais, em várias das suas formas, constitui o ponto central para a investigação criminal e para as atividades de segurança pública, de um modo geral. O cotidiano das ações realizadas pelas polícias envolve principalmente a reunião, a interpretação, a recuperação e a apresentação de informações sobre crimes e criminosos. Neste ponto, deve ser ressaltado que o principal desafio informacional da atividade policial é justamente o de lidar com a diversidade dos tipos de crimes previstos em lei, que também podem ser praticados de diferentes modos (Roberts *et al.*, 2011). A exemplo, um roubo pode ser praticado individualmente ou em grupo; pode ser fruto de grande planejamento, ou um ato de improviso; pode ser uma questão local, ou uma ação internacional; e pode gerar para o criminoso quantias vultosas ou um pequeno volume de dinheiro. Assim, não é possível descrever o formato,

volume ou o modo de disposição das informações e dados gerados pelas circunstâncias de cada evento criminoso. Alguns delitos produzirão uma grande quantidade de informações, que poderão estar espalhadas por diversos locais, e outros irão gerar pouquíssimos dados, que estarão localizados em um lugar específico (Stelfox, 2009).

Sendo uma atividade baseada na informação, torna-se necessário determinar os diversos tipos de dados pessoais utilizados pelos órgãos policiais, para efeitos de prevenção, investigação, detecção ou repressão de crimes, incluindo-se as ações de repressão e prevenção de ameaças à segurança pública. Do mesmo modo, é preciso definir a importância estratégica das diversas fontes de dados utilizadas pelas polícias, sejam de origem interna quanto aqueles dados fornecidos por órgãos do poder público, organizações não-governamentais, entidades privadas, bem como dados provenientes de fontes acessíveis ao público (fontes abertas). Devem ser estabelecidos os critérios acerca da qualidade e confiabilidade dos dados pessoais, a serem tratados pelas polícias, tomando como referência a sua fonte ou natureza (Araújo, 2014).

A impressão digital, por exemplo, é um tipo de dado vem sendo utilizado pelas polícias ao longo dos anos, com diversos propósitos diferentes. Por sua vez, as técnicas de identificação, coleta, processamento e uso de registros datiloscópicos foi se tornando cada vez mais complexo, conforme foram surgindo novas tecnologias. No final do Século XIX, as impressões digitais começaram a ser usadas com fins burocráticos, para assegurar que uma pessoa era quem ela dizia ser. Isso era feito por meio da coleta de uma imagem da digital da pessoa e feita sua comparação com a impressão que já estava arquivada. Entretanto, rapidamente as polícias perceberam que essa técnica poderia ter uma aplicação na investigação criminal, porque quando o criminoso toca um objeto durante o curso de um evento ele deixa uma impressão de sua digital (Stelfox, 2009).

Ao longo do tempo foram sendo desenvolvidas diversas metodologias de localização e coleta de impressões digitais em locais de interesse para as investigações, que passaram a ser extraídas de uma grande variedade de superfícies, e se tornou uma estratégia de investigação criminal usada em quase todas as polícias do mundo. Mesmo que uma impressão não puder ser comparada com a de uma pessoa já conhecida pela polícia, ela permaneceria sendo um material útil, pois uma vez que um suspeito fosse identificado por outros métodos, seria possível conectá-lo à cena do crime.

Contudo, um banco de dados com impressões digitais não se limita, certamente, à mera coleta dos dados para a investigação policial. Engloba também todo o processo pelo qual a polícia faz uso dos dados coletados, sendo a ação de maior importância a seleção do padrão compatível com a amostra a ser confrontada. Assim, estes recursos de seleção podem ser lentos

na hora de encontrar impressões digitais em um arquivo com cinco milhões delas (Stelfox, 2009). Entretanto, a organização de imensas massas de dados vem passando por novas soluções, com o incremento da capacidade de armazenamento e outras possibilidades tecnológicas em termos de descrição, classificação e organização da informação.

Em um contexto geral, as polícias utilizam o tratamento de dados pessoais como uma ferramenta para dar sentido às relações sociais, transformando dados brutos em informações disponíveis sobre crimes e redes criminosas. Trata-se de um conjunto de processos analíticos direcionados ao fornecimento de informações oportunas e pertinentes, relativas aos padrões de criminalidade e às correlações de tendências. Esse processamento de informações serve como o meio para fornecer *insights,* que podem impulsionar ou apoiar operações e estratégias de investigações policiais, bem como influenciar políticas e decisões governamentais. Encarregados de explicar um problema policial, os analistas procuram primeiro identificar quatro coisas (James, 2016, p. 10):

i. O que já se sabe sobre o objeto de pesquisa;
ii. Onde podem ser encontrados dados para preencher as lacunas de conhecimento;
iii. Como esses dados podem ser obtidos; e
iv. O significado que pode ser inferido deles.

Na maioria das polícias, os policiais que realizam análises de dados recebem o maior e mais avançado tipo treinamento profissional. Normalmente são treinados na operação do ciclo de inteligência, usando uma técnica analítica padrão, e produzindo vários tipos de informação, tais como avaliações estratégicas, avaliações táticas, perfis detalhados de suspeitos ou vítimas, dentre outros. Nestes casos, existe um grande o foco na análise de redes de relacionamento interpessoais de criminosos (*criminal network*), que são centrais para o tratamento de dados no âmbito policial. Na análise de redes criminosas, uma imagem pode valer mais que mil palavras (James, 2016).

O desenvolvimento do tratamento de dados pessoais no âmbito policial, principalmente no contexto de análise redes criminosas, pode ser descrito em termos de gerações de tecnologias. Os sistemas de informação policial podem ser classificados de acordo com sua complexidade e capacidade de análise, pelos tipos de ferramentas desenvolvidas ao longo do tempo. As ferramentas de primeira geração, como Anacapa, contavam com métodos manuais, tabelas e listas de dados brutos, sobre eventos e relacionamentos, que eram utilizadas para criar gráficos de *links* mostrando associação criminosa.

Por sua vez, a análise de redes de segunda geração passou a utilizar softwares como o *i2 Analyst´s Notebook,* e produtos similares como *COPLINK* ou *NetMap*. Tais programas

possuíam a capacidade de gerenciar grandes quantidades de dados e de fornecer análises muito mais complexas dos relacionamentos existentes dentro de uma rede do que poderiam ser obtidas manualmente. Esta segunda geração também é caracterizada pela grande ênfase ao uso de recursos visuais para descrever grupos, indivíduos e as ligações entre eles (James, 2016).

Já as análises de redes sociais de terceira geração baseiam-se em métodos já utilizados pesquisas nas ciências sociais há muitos anos. Segundo John Scott, a moderna análise de redes sociais teve origem a partir da adaptação de vários estudos sociais, como o realizado por um grupo de antropologistas da Universidade de Manchester, que investigaram nos anos 1950 a estrutura das relações comunitárias em sociedades tribais, a partir da análise dos conflitos e das contradições entre os seus membros (Scott, 2000).

A análise de rede sociais pode medir e mapear relacionamentos, e identificar indivíduos significativos dentro da rede (como líderes ou indivíduos que conectam um subgrupo a outros), e que não seriam necessariamente identificados por outros meios. De qualquer forma, as tecnologias que eram descritas como sendo de segunda geração se tornaram parte da chama terceira geração, à medida que as empresas atualizaram e aprimoraram seus *softwares* para fornecer as funcionalidades que os analistas policiais esperavam (James, 2016).

4.3.1. Informações gerenciadas pelas polícias

Conforme Peter Stelfox, as polícias gerenciam dois tipos de dados e informações: i) a informação como conhecimento; e ii) e a informação como dado. O primeiro tipo de informação diz respeito ao conhecimento sobre crimes que é relatado aos órgãos de segurança pública por vítimas, testemunhas, policiais, criminosos ou qualquer pessoa que teve contato indireto com o fato delituoso,. Já a informação como dado é representada por meio de objetos, documentos, imagens, gravações, registros alfabéticos e numéricos, e amostras de materiais, que podem ser submetidos a análises científicas, como DNA e impressões digitais. Ambos os tipos de dados e informações são utilizados pelas polícias para inferir fatos e circunstâncias de interesse para a segurança pública, aumentando o conhecimento de policiais sobre crimes e criminosos (Stelfox, 2009).

A teoria de Stelfox possui um certo paralelo com a distinção realizada por Buckland entre “informação-como-conhecimento” – a comunicação do conhecimento ou a notícia de algum fato ou ocorrência – e a “informação-como-coisa” – representada por objetos com conteúdo informativo (documentos, imagens, gravações, registros e amostras de materiais), que possuem a capacidade de proporcionar o aumento do conhecimento sobre algo. Conforme já

mencionado neste trabalho (subseção 4.2.1), a principal característica da "informação-como-conhecimento" é a sua intangibilidade, ou seja, não se pode tocá-la ou medi-la de forma direta, pois conhecimento, crença e opinião são pessoais, subjetivos e conceituais (Buckland, 2001).

Entretanto, para serem comunicadas, as “informações-como-conhecimento” devem ser expressas, descritas ou representadas em alguma forma física, como um registro, texto ou comunicação, sendo convertida então em uma “informação-como-coisa”. Neste sentido, deve ser ressaltado que os SOC policiais, bem com os sistemas de gerenciamento de bancos de dados, lidam somente com a “informação-como-coisa”. Isto porque, em última análise, os mecanismos de armazenamento, análise, cruzamento e recuperação de informação somente podem atuar com a informações registradas.

As “informações-como-conhecimento” que surgem na mente de policiais, vítimas, testemunhas, suspeitos e peritos, dentre outras pessoas que podem estar em torno do fato criminoso analisado, precisam ser convertidas em uma “informação-como-coisa”. Para tanto, são expressas, descritas, registradas ou representadas, em alguma forma física ou eletrônica, como um registro de texto, vídeo ou áudio, planilhas eletrônicas ou mesmo sistemas *online*.

Da mesma forma, os conhecimentos adquiridos pelos policiais, após o processamento de dados e informações em sistema informatizado, precisam ser também convertidos em novas formas ou versões de uma “informação-como-coisa” (Araújo, 2018), tais como informações policiais, relatórios de inquérito, relatórios de análise, mapas com manchas criminais, laudos periciais, dentre outros. Por sua vez, estes novos conhecimentos, registrados em alguma forma física, são também inseridos como dados no sistema de informação, subsidiando a geração de outras análises, em um ciclo constante de produção de conhecimento policial.

4.3.1.1. Informação como conhecimento.

Um dos principais objetivos do sistema de segurança pública é o de identificar pessoas que possuem conhecimento sobre fatos criminosos, ou que estão de alguma forma relacionados com crimes e criminosos, realizando a gestão da transferência dessa informação para os órgãos policiais. Embora essa atividade envolva o uso de técnicas para localizar vítimas, testemunhas e infratores, além do recrutamento de informantes e o assessoramento de peritos e expertos, que dominam determinado assunto, o gerenciamento da informação como conhecimento é quase totalmente uma questão de comunicação humana. A obtenção pela polícia de conhecimento sobre o crime depende, assim, tanto da transferência da informação por aquele que a detém, de forma voluntária ou não, quanto da capacidade do policial de recebê-la e interpretá-la (Stelfox,

2009).

Mesmo quando vítimas ou testemunhas não possuam informações que liguem um infrator ao ato ilícito, estas geralmente poderão fornecer informações relevantes sobre a ocorrência do crime. Além de serem fontes de informações úteis aos órgãos de segurança pública e investigação criminal, como a hora, a data e o local da ocorrência do crime, vítimas e testemunhas podem oferecer detalhes sobre os métodos utilizados no cometimento do crime. Entretanto, os infratores são as melhores fontes de informações sobre os crimes que eles mesmos cometem, sendo que muitos deles comunicam este conhecimento para membros da família, amigos ou associados, que se transformam em testemunhas ou informantes dos órgãos de segurança pública (Stelfox, 2009). As diversas investigações realizadas com o auxílio de interceptações de comunicações demonstram que o valor dos autores de crimes como fonte de conhecimento para as polícias.

Por sua vez, as polícias também utilizam como fonte de informações as manifestações de experts, peritos ou analistas, cujo treinamento ou experiência permitem que sejam reconhecidos como detentores de opiniões válidas ou legítimas sobre determinado assunto. Ao elaborar sua opinião, o analista se utiliza de técnicas específicas e do conhecimento científico geral, formulando uma explicação que seja considerada objetiva e demonstrada por uma relação de causa e efeito. Entretanto, deve ser ressaltado que, mesmo não sendo aceita como uma evidência em um julgamento, opiniões sobre tendências criminais elaboradas por analistas, com base em fundamentos teóricos, são bastantes úteis nas atividades de segurança pública e de investigação criminal (Stelfox, 2009).

No Brasil, as informações policiais como conhecimento humano são produzidas, de uma forma geral, no denominado inquérito policial. Este é um procedimento policial de instrução preparatória e delimitado temporalmente, que começa com o cometimento do crime e termina com o seu arquivamento, ou com o início de um processo criminal junto ao Poder Judiciário. Com a finalização da investigação, é feita a remessa ao julgador (juiz monocrático ou aos tribunais) de todas as informações e dados reunidos pela polícia sobre o crime, os possíveis autores e todas as circunstâncias do fato investigado. Neste procedimento são registradas as informações prestadas por vítimas, testemunhas, criminosos e peritos, dentre outras fontes humanas, sobre um determinado crime e suas circunstâncias.

É no inquérito policial que são transformados em entidades físicas o conhecimento sobre crimes e criminosos, surgido primeiramente na mente de vítimas, testemunhas, informantes, policiais, peritos e, até mesmo, dos autores do crime. Todo o conhecimento abstrato, formado na mente de pessoas relacionadas ao fato investigado, para se manifestar,

requer sua transformação em dados ordenados e registrados. No âmbito do inquérito policial, a "informação-como-conhecimento" se converte em uma "informação-como-coisa" (Buckland, 2001), através de atos formais, tais como declarações, depoimentos, interrogatórios, informes, informações policiais, gravações, termos circunstanciados, laudos periciais e relatórios, dentre outros instrumentos. Por sua vez, a "informação-como-conhecimento" se transforma em algo tangível por vários meios, como textos, vídeos e áudios, que são registrados em qualquer tipo de mídia de armazenamento. Desse modo, o inquérito policial representa a materialização física de todo o conhecimento humano, produzido pela polícia, sobre as pessoas em torno de determinado crime e as circunstâncias dos fatos investigados.

Os inquéritos policiais reúnem, em sua grande maioria, informações não estruturadas e de cunho textual. Entretanto, com a utilização de sistemas de *big data* e de gerenciamento de dados, é possível transformar o conhecimento acumulado em diversas investigações distintas em informações que possam ser utilizadas de forma eficiente em favor da segurança pública.

Tendo por base o fundamento da CI, de que toda informação de interesse para as organizações deve ser preservada, armazenada e principalmente consultada (Bush, 1945), verifica-se que o próprio acervo de investigações criminais realizadas por determinada instituição policial constitui sua mais importante fonte de informações para a segurança pública. O conhecimento acumulado pelas polícias ao longo do tempo, por meio de inquéritos individualizados, constitui o principal ativo informacional a ser utilizado no enfrentamento de atividades como o tráfico internacional de drogas, crimes ambientais, evasão de divisas, tráfico de pessoas, contrabando, entre outros crimes relacionados à denominada criminalidade organizada. Por meio da análise do acervo, é possível aos órgãos policiais recuperarem informações sobre os principais criminosos já identificados, suas redes de relacionamento, modus operandi, áreas de atuação, cadeias de comércio ilícito, dentre outras. Assim, os dados relacionados, viabilizam análises direcionadas para a seleção de novas investigações e a definição das estratégias policiais mais eficientes.

4.3.1.2. Informação como dado

Enquanto as informações como conhecimento, no âmbito das polícias, possuem origem sempre em fontes humanas, a informação como dado pode derivar de uma grande quantidade de fontes (Stelfox, 2009). Existem várias maneiras pelas quais as instituições policiais obtêm informações pessoais, podendo a lista de fontes incluir diversos tipos de dados e diferentes sistemas de coleta e armazenamento, tais como (Stelfox, 2009, p. 89):

i. Sensores: CFTV, câmeras inteligentes, detecção de atividade incomum, dispositivos de cidade inteligente etc.;
ii. Registos biométricos: impressões digitais, DNA, fotografias;
iii. Sistemas de mapeamento: geolocalização pessoas, fluxo de pedestres, mapas de calor de tráfego etc.;
iv. Registos automatizados de placas veiculares: radares, lombadas eletrônicas, estacionamentos automatizados etc.;
v. Dispositivos móveis: sistemas de navegação de automóveis, telefones celulares;
vi. Serviços eletrônicos públicos e privados: compras *online*, atividades em redes sociais, serviços de e-mail, mensagens instantâneas, governo digital, e-Gov etc.;
vii. Internet das coisas: *wearables*, *smart devices*, sistemas de automação etc.;
viii. Registos de cidadãos e clientes: registos financeiros, registos de nomes de passageiros, registos criminais, registos de veículos, informações fiscais, informações de pagamento etc.).

Todos esses recursos informacionais podem ser combinados, para aprimoramento dos resultados tanto nas ações de prevenção como na investigação de crimes, permitindo que investigadores realizem inferências sobre fatos e suas circunstâncias, e aumentem os seus conhecimentos sobre o crime (Sloot; Broeders; Schrijvers, 2016). Por exemplo, impressões digitais obtidas na cena do crime podem levar ao nome de uma pessoa. Esse nome pode ser vinculado a vários registros, como a utilização de cartões de créditos, histórico de chamadas telefônicas, rotinas de viagem ou atividades em redes sociais *online*, e assim por diante.

Dentre as diversas fontes de dados e informações utilizadas pelas polícias, devem ser ressaltados os geradores passivos de dados. Estes são sistemas que coletam ou registram dados automaticamente, e geram material que inicialmente não teria como finalidade atividades policiais, tais como gravações de CFTV, *logs* de endereços de protocolo de internet, registros telefônicos, registros bancários e de cartões de crédito.

Esses sistemas podem gerar grandes quantidades de dados, que são baixados, arquivados ou excluídos periodicamente por diversos tipos de empresas ou instituições públicas. Como os geradores passivos de dados podem criar grande volume de material, a polícia deve selecionar somente o material que agregará valor à investigação. A integridade e precisão de todo material recolhido deve ser garantida, com a criação de arquivos organizados, para garantir a acessibilidade e uso otimizado dos registros obtidos (Stelfox, 2009).

4.3.2. Tratamentos de dados realizados pelas polícias

Para uma melhor compreensão dos tipos de tratamento de dados que são realizados no âmbito policial, devem ser analisados os dois enfoques de atuação dos órgãos de segurança pública: i) abordagem reativa; e ii) abordagem proativa. No modelo reativo, a investigação começa a partir de um crime específico já ocorrido, o qual é levado ao conhecimento da polícia por meio de vítimas, testemunhas ou por qualquer pessoa do povo, bem como mediante representações formais realizadas por outras instituições do sistema de justiça ou órgãos estatais de fiscalização e controle. Por sua vez, a investigação proativa é impulsionada a partir da detecção de eventos criminosos, tendo por base o cruzamento de informações e bancos de dados criados, ou aqueles reunidos pelas próprias polícias.

Embora o principal instrumento de condução das investigações criminais continue sendo o inquérito, a atividade policial moderna passou a ser orientada pela informação, o que possibilita uma atuação mais proativa das polícias, com a ampliação do próprio escopo de suas atividades. Desse modo, por meio de ações proativas, de coleta ativa de dados e de análise criminal, as ações policiais são direcionadas a modalidades criminosas ou grupos criminosos específicos, suspeitos de estarem envolvidos com práticas criminosas reiteradas (Zampronha, 2023).

O modelo reativo pressupõe um procedimento de instrução preparatória delimitado temporalmente, que começa com o cometimento do crime e termina com o início da ação penal, ou com o arquivamento da investigação. Este procedimento tem por objetivo apurar as infrações penais logo que elas sejam cometidas, com a reunião dos indícios e provas de sua ocorrência, para imediata transmissão ao Poder Judiciário. Por sua vez, a abordagem proativa geralmente começa com a realização pelas polícias de análises estratégicas ou operacionais, a partir da coleta de informações de diversas origens, tais como denúncias anônimas, sistemas policiais, fontes abertas (materiais jornalísticos, redes sociais, e internet de forma geral), bancos de dados policiais, sistemas de monitoramento, dentre outras fontes de dados.

No âmbito das investigações criminais, o tratamento de dados pessoais pode estar relacionado a suspeitos, vítimas e testemunhas, dentre outras pessoas relacionadas ao objeto da investigação. Nestes casos, o tratamento têm por objetivo realizar o cruzamento de bancos de dados, para descobrir informações relacionadas a uma determinada pessoa, bem como a um evento já ocorrido ou que possa estar prestes a ocorrer. Por sua vez, o tratamento de dados pessoais realizados no contexto de análises criminais têm por objetivo apoiar estratégias criminais (análise estratégica), ou auxiliar na identificação de atividades ilegais, ou de pessoas e grupos suspeitos, que ainda não chegaram ao conhecimento da polícia (análise operacional)

(Europol, 2023).

A investigação criminal é realizada pela polícia por meio da coleta de dados e informações de diversos tipos, com o objetivo de comprovar a materialidade de um crime e indicar a autoria de fato ilícito específico ou pré-determinado. Após a conclusão das investigações, a autoridade policial responsável pelo caso elabora um relatório detalhado com uma análise das evidências que foram coletadas, contendo a valoração da conduta do investigado e o enquadramento do fato a um determinado tipo penal. Existe uma diversidade de condutas que são tipificadas pela lei como criminosas, que geram diferentes elementos tipos de informações e dados pessoais a serem coletadas pelas polícias.

Por sua vez, a quantidade e as características dos dados, coletados e analisados durante uma investigação criminal serão definidas pela estratégia utilizada para lidar com determinado evento criminoso. Do mesmo modo, a escolha da estratégia de investigação a ser utilizada dependerá da qualidade e da natureza da informação disponível aos órgãos de investigação criminal (Stelfox, 2009). Por exemplo, os órgãos policiais podem interferir nas atividades de uma organização criminosa de narcotráfico por meio de ações de interdição, visando o desmantelamento da estrutura logística e da cadeia produtiva do produto ilegal. Do mesmo modo, podem utilizar estratégias de investigações financeiras e patrimoniais, visando à repressão dos mecanismos de lavagem de dinheiro para legitimar ou ocultar os ativos gerados pelo comércio ilegal. Neste último caso, os órgãos de investigação criminal irão coletar dados bancários e patrimoniais, que possibilitem analisar o volume movimentado e reconstituir o caminho percorrido pelos recursos gerados pela atividade comercial ilícita[11].

Entretanto, independentemente do crime investigado, ou mesmo da estratégia de enfrentamento utilizada pelo órgão policial, o tratamento de dados pessoais constitui uma das atividades essenciais de qualquer investigação criminal, seja realizado em sistemas informatizados ou em sistemas manuais de arquivamento, classificação e consulta. De uma forma geral, as polícias realizam operações de tratamento de dados pessoais com o objetivo de identificar e/ou localizar indivíduos ainda desconhecidos. Para tanto, passam a agregar o maior número de pontos de dados de uma pessoa específica, tais como nomes, números de identificação, dados de localização, imagens, dados biométricos, endereços IP, e toda a variedade de identificadores já mencionados. Do mesmo modo, em alguns casos, as polícias procuram estabelecer as redes de relacionamento pessoal e comercial de investigados e suspeitos já identificados, coletando e processando o máximo de informações julgadas

[11] A investigação financeira, ao mesmo tempo, também permitiria a localização e o confisco dos bens adquiridos com o dinheiro proveniente da venda das drogas.

necessárias para a detecção, prevenção ou apuração de crimes.

Em alguns casos, entretanto, o grande volume de crimes impossibilita a instauração de inquéritos específicos para cada fato individualmente, tendo em vista a baixa probabilidade de que as investigações levem à resolução do caso. Desse modo, atualmente, as polícias passaram a focar em outras atividades, tais como a gestão dos crimes e das próprias organizações criminosas. Nestes casos, os órgãos de segurança pública adotam medidas visando a redução de oportunidades para o cometimento de atos delituosos, através da coleta e da gestão de dados, a interrupção de cadeias comerciais ilícitas, a localização e apreensão de bens e patrimônios de origem ilícita, dentre outras atividades. Assim, as instituições de segurança pública têm avançado em direção à adoção de medidas proativas (*proactive investigation*) e no uso de tecnologias modernas de análise de dados (*inteligence-led policing*). Neste modelo de atuação, as instituições de segurança pública deixam de tratar informações somente sobe crimes específicos e individualizados, passando a focar em problemas de criminalidade em determinada área ou período (Tiley; Robinson; Burrows, 2011).

Hoje em dia a atuação policial não se resume a levar autores de crimes a julgamento perante a Justiça, com o processo de coleta de informações não sendo moldado apenas pela necessidade da polícia de identificar suspeitos e reunir evidências para subsidiar processos criminais. A adoção de um modelo de atuação policial orientada pela informação tem por objetivo impulsionar medidas de segurança pública direcionadas a diversos aspectos da aplicação da lei, desde a condução de investigações criminais até a distribuição de policiamento nas ruas.

Tal abordagem proativa geralmente envolve a análise de informações de várias origens, tais como denúncias anônimas, plataformas integradas de sistemas, fontes abertas (materiais jornalísticos, redes sociais, e internet de forma geral), bancos de dados policiais, sistemas de monitoramento, com ou sem reconhecimento facial, dentre outros tipos de fontes de dados. Por isso, o acesso a grande volume de dados relevantes é a espinha dorsal da atividade policial baseada na informação, havendo uma série de sistemas e bancos nacionais de relevância imediata para policiais e órgãos de segurança pública, os quais oferecem grande potencial para análises sofisticadas de problemas criminais.

Esse novo modelo de atuação policial é caracterizado pelo tratamento de grandes conjuntos de dados, com a criação de mecanismos de computação específicos, visando a triagem de crimes e a identificação de condutas criminosas mais graves, ou de criminosos mais prolíficos. Do mesmo modo, em atenção à ampliação de seu escopo de atuação, as polícias agora elaboram ouros tipos de conhecimento, tais como: i) avaliações estratégicas, voltadas à

análise das principais ameaças à segurança pública; e ii) avaliações táticas, relacionadas à identificação de alvos prioritários e definição das melhores metodologias de investigação a serem empregadas. Ressalte-se que o conhecimento produzido através do tratamento de dados é destinado à própria instituição policial, a qual passa a produzir e consumir simultaneamente estas análises criminais, de modo a alterar as condições de sua atuação na promoção da segurança pública.

Com base em análises estratégicas, que se utilizam cada vez mais informações não estruturada e de cunho textual (Souza; Almeida; Baracho, 2015), as polícias podem: i) coletar informações relevantes para permitir a identificação e a análise clara e precisa dos problemas de segurança pública, atuais e futuros; ii) priorizar os problemas mais importantes e planejar respostas para eles; e iii) avaliar o que foi feito, e realimentar a experiência e o conhecimento produzido. Todos esses processos devem levar à adoção de ações estratégicas, com a identificação das maiores ameaças de crimes atuais e futuros, bem como ações táticas para identificar alvos específicos (que podem ser pessoas, lugares ou atividades), nos quais será mais efetivo para focar quaisquer intervenções (John; Maguire, 2011).

Tais instrumentos permitem a realização de análises, com a criação de relatórios, painéis e visualizações da informação de forma abrangente. Por sua vez, os resultados dessas análises possibilitam a identificação de relações entre entidades, vínculos pessoais e outros pontos de interesse. Com a conversão de dados brutos, ainda inexplorados, em informações úteis e relevantes, as polícias podem iniciar novas investigações, geralmente focando em regiões com grande incidência de fatos ilícitos.

Para a adoção dessa nova forma de abordagem do fenômeno criminoso, as polícias necessitam de sistemas de organização da informação e de meios computadorizados de armazenamento, recuperação e comparação de dados, que facilitem o processo de pesquisa. Na prospecção de casos criminais de forma proativa, as polícias podem empregar sistemas de gerenciamento de bancos de dados, ferramentas de *business intelligence* (BI) e outros meios tecnológicos para a coleta, armazenamento e processamento de grandes quantidades de dados estruturados.

4.3.3. Vigilância, big data e a atividade policial preditiva

O mundo contemporâneo pode ser enxergado pelo ângulo de visão de uma sociedade de vigilância. Este enfoque coloca em destaque não apenas os encontros diários entre as pessoas, mas também os massivos sistemas de vigilância que agora sustentam a existência

moderna. Não se trata apenas de câmeras de vigilância, que podem capturar nossa imagem várias vezes ao dia, cartões de fidelidade de supermercados, ou de e um cartão de acesso codificado para entrar no local de trabalho. Trata-se, na realidade, de sistemas que representam uma infraestrutura básica e complexa, que assume que a coleta e o processamento de dados pessoais são vitais para a vida contemporânea. Tradicionalmente, falar em sociedade de vigilância invoca algo sinistro, com características de governos ditatoriais ou totalitários. Contudo, a vigilância pode também ser vista como um avanço em direção à administração eficiente, um benefício para o desenvolvimento do governo, da sociedade e da própria economia dos países (Wood, 2006).

Muitas vezes, o termo vigilância é empregado em termos bastante específicos e direcionados para o campo policial, mas na realidade sua definição abrange um enfoque muito maior. Assim, antes de uma definição estritamente policial, seu conceito pode ser compreendido a partir de um conjunto de atividades que compartilham certas características, podendo vigilância ser definida como sendo a observação de informações pessoais de forma proposital, rotineira e sistemática, para fins de controle, direitos e legitimidade, gestão, influência ou proteção. Algumas formas de vigilância existem há bastante tempo, uma vez que as pessoas sempre cuidaram uma das outras em busca de benefícios mútuos, de monitoramento moral ou para descobrir informações secretamente. Por sua vez, métodos "racionais" de vigilância começaram a ser aplicados às práticas organizacionais há cerca de 400 anos, com a eliminação progressiva das redes sociais informais de que, até então, dependiam os negócios cotidianos e do próprio governo. Os laços sociais comuns das pessoas foram sendo diminuídas, para que as ligações familiares e as identidades pessoais não interferissem no bom funcionamento destas novas organizações políticas governamentais. Neste contexto, eventualmente as pessoas poderiam esperar que os seus direitos fossem respeitados, porque estavam protegidos pela lei e por registos precisos do governo (Wood, 2006).

A vigilância é um termo cuja definição pode não ter sido alterada ao longo do tempo, mas na prática suas formas e métodos se adaptaram, conforme as novas possibilidades tecnológicas, sobretudo, àquelas voltadas para a observação e cerceamento de indivíduos. Atualmente, com o desenvolvimento de recursos automatizados para a coleta, armazenamento e gestão da informação, o monitoramento dos indivíduos deixou de ocorrer de forma direta, passando a ser feito, em certa medida, através dos dados que os representam. A vigilância moderna ampliou seu *spectrum,* e expandiu seu poder a escalas globais, aumentando a capacidade de visualização e rastreamento dos indivíduos ao nível das populações.

Todas as tecnologias disponíveis para o monitoramento, localização e identificação de

indivíduos, desde os circuitos fechados de TV (CFTV) até os *chips* de identificação por radiofrequência (RFID), bem como ferramentas pessoais de acesso à internet, sistemas de transações bancárias, registros de cartões de crédito, sistemas de geolocalização e controle de trânsito (particulares ou públicos, para o controle de pedestres ou veículos), dentre outros, podem ser utilizados como ferramentas intermediárias na observação e monitoramento de pessoas. Atualmente, tais ferramentas tecnológicas intermediárias são partes essenciais do modelo de vigilância moderno, servindo para ampliar a capacidade de identificação de padrões de comportamento que destoem da normalidade (Lott, Ciancon, 2018).

As informações agora são coletadas por atacado, de forma abrangente, sem distinção ou limite de tempo. Neste contexto, o indivíduo é identificado somente em caso de necessidade ou contextos específicos, bem como quando algum padrão possa ser notado em seu conjunto de dados, de forma a acusar alguma ameaça. Neste momento, as informações pessoais desse indivíduo passam a ser investigadas com mais atenção, além dos algoritmos, por agentes humanos, que podem reconstituir linhas de tempo/eventos que ocorreram há muitos anos (Lott, Ciancon, 2018).

Esse cenário foi agravado ainda mais pelo uso intenso de dados pessoais encontrados na internet, facilitado pelo compartilhamento voluntário, em grande parte, como forma de exposição e recebimento de atenção nas redes sociais. O conceito de rede, em substituição à sociedade, seria o mais adequado para representar o novo campo social que se configurou a partir da internet. O cenário desta organização social em rede se caracteriza pela obsolescência programada, pelas respostas rápidas e superficiais, e pelo acesso a todo tipo de conteúdo com o mínimo de esforço. Nesse contexto, os laços de relacionamento entre as pessoas seriam frágeis, e tão fáceis de serem estabelecidos quanto desfeitos (Lott, Ciancon, 2018).

O processo de informatização dos sistemas de gestão e a expansão da internet ocorreu não somente entre a população residente nos grandes centros econômicos, mas também entre os habitantes de regiões periféricas e menos desenvolvidas. Todos se tornaram, inevitavelmente, dependentes das tecnologias digitais para terem acesso a serviços, e para possibilitar suas ações de trabalho e entretenimento. Neste sentido, o uso de circuitos fechados de câmera, cartões magnéticos e *smartphones*, além das publicações nas redes sociais, registram os passos e guardam as informações de seus usuários com a precisão de horas, minutos e segundos. Cada acesso à internet ou de toque em uma tela interativa é suficiente para criar um conjunto de dados, que pode conter muitas informações determinantes sobre o indivíduo (Lott; Ciancon, 2018).

A manipulação de grandes quantidades de dados (geralmente em *exabytes*), seja na

forma estruturada, semiestruturada ou não estruturada, ou em qualquer combinação dos três, é definido pelo termo *big data*. Este termo pode ser atribuído a Doug Laney, que em 2001 destacou que *big data* era caracterizado pelos "3 Vs" (James, 2016): volume (o método tradicional de armazenamento não é adequado); velocidade (excede a velocidade normal de processamento de dados); e variedade (dados não uniformes).

Embora existam algumas variações para a sua definição, como a inclusão de outros "Vs" – como veracidade e valor (Klous, 2016) –, há um amplo acordo sobre o valor da análise de *big data* e uma grande confiança na capacidade para extrair informações ordenadas, para encontrar padrões em dados anteriormente díspares. Usuários de sistemas de bancos de dados, voluntariamente ou não, geram um grande volume de dados todos os dias. Esta taxa de geração de dados está crescendo exponencialmente, mas o termo *big data* não descreve apenas esta vastidão de dados disponíveis. Grandes volumes de dados somente são considerados *big data* caso exista a possibilidade de serem explorados, através de análises avançadas, para fornecerem informações com valor intrínseco. Essas informações valiosas seriam verdadeiras agulhas a serem encontradas, não importa quão grande seja o palheiro ou quantos palheiros existam. Isso implica que benefícios até então desconhecidos podem surgir, se a ferramenta correta puder ser encontrada e usada (Brakel, 2016).

A expansão do acesso à internet e aos dispositivos móveis, juntamente com o desenvolvimento de tecnologias de *big data*, pode mudar drasticamente as práticas policiais de vigilância. Isto porque os órgãos de segurança pública passaram a utilizar grandes bases de dados para identificar e reconhecer de padrões de comportamento, de forma automática e massiva. Através de grandes volumes de dados, estruturados ou não estruturados, em diferentes formatos e provenientes de diversos tipos de fontes, analistas policiais obtém *insights* e acesso a conhecimentos novos e originais. Este contexto, visto como um fenômeno social e tecnológico, oferece inclusive a possibilidade da realização de vigilância preditiva, ou em tempo real.

As tecnologias de vigilância, que empregam uma lógica preventiva, realizam a coleta e processamento sistemáticos, ou direcionados, de dados pessoais, para fazerem previsões sobre riscos de danos futuros com base em análises de perfis, com o principal objetivo de intervir antes que o dano seja causado. Assim como em outras tecnologias, a vigilância preventiva pode ter efeitos tanto benéficos ou prejudiciais ao conjunto da sociedade, não sendo boa nem ruim em si mesma. Os benefícios do emprego de sistemas de vigilância preditiva vão depender do contexto organizacional de cada instituição policial, pelas razões e justificativas pelas quais a tecnologia está sendo utilizada (Brakel, 2016).

Em termos gerais, o policiamento preditivo (PP) seria o método adotado por agências policiais de utilizar dados sobre crimes passados para prever padrões futuros de crimes ou áreas vulneráveis (James, 2016). Existem basicamente dois tipos de PP: i) mapeamento preditivo, referente à aplicação de análises para prever quando e onde um crime pode ocorrer; e ii) identificação preditiva, que é a análise realizada, no nível individual ou de grupo, com o objetivo de prever possíveis infratores, comportamentos criminosos e potenciais vítimas de crimes. O tipo mais comumente utilizado é o do mapeamento preditivo, existindo vários tipos de *softwares* e programas em utilização, por forças policiais de diversos países, tais como o PredPol nos EUA e no Reino Unido; o Sistema de Conscientização de Criminalidade (*Criminality Awareness System* - *CAS*), nos Países Baixos; e o Precobs, na Alemanha e na Suíça. Algumas aplicações realizam combinações de diferentes fontes de dados, como, por exemplo, um tipo de policiamento preditivo, no qual são utilizados dados extraídos de telefones celulares e dados demográficos.

Outra tendência é o uso de métodos de identificação de pontos de concentração, que estão vinculados a dados de aplicativos de redes sociais para realização de previsões. Nesse caso, o algoritmo busca pelo uso de linguagem específica, que indica uma maior probabilidade de crime em uma determinada área. Por exemplo, se as pessoas estão falando sobre sair, ir a bares e ficarem bêbadas, esses indicadores são identificados pelos modelos de mineração de dados. A partir do momento em que os dados são coletados, as *tags* de GPS possibilitam visualizar as ameaças e os pontos de concentração para crimes potenciais (Brakel, 2016).

Mas também existem exemplos relacionados à identificação preditiva com uso de *big data*, como um aplicativo utilizado nos Estados Unidos chamado *Intrado Beware*, que vem sendo vendido para departamentos de polícia desde 2012. Trata-se de um aplicativo móvel, baseado em nuvem, que coleta informações contextuais de bancos de dados comerciais e públicos existentes. Após analisar informações comerciais, criminais e de redes sociais, o algoritmo do *Beware* atribui uma pontuação e uma classificação de ameaça (verde, amarelo ou vermelho) a uma pessoa, que é automaticamente enviada a um policial encarregado. Entretanto, ainda não seria possível tirar conclusões convincentes sobre a eficácia das aplicações de identificação preditiva. Isto porque essas tecnologias ainda são muito recentes, e as avaliações futuras terão que lançar mais luz sobre sua eficácia na prevenção criminal. No entanto, a metodologia por detrás dessas novas tecnologias deve ser questionada de forma crítica, até mesmo para que se possa garantir que as avaliações sobre a eficácia dos *softwares* sejam conduzidas adequadamente (Brakel, 2016).

Neste sentido, qualquer sistema de policiamento preditivo deve levar em consideração

os riscos envolvendo a elaboração de perfis discriminatórios (*discriminatory profiling*), de cidadãos cujos dados foram coletados, armazenados e analisados por órgãos policiais. Sistemas algorítmicos enviesados podem levar ou ampliar enviesamentos devido aos denominados "ciclos de *feedback*". Um ciclo de *feedback* ocorre quando as previsões feitas por um sistema de informação policial influenciam os dados que são usados para atualizar o mesmo sistema. Isso significa que os algoritmos influenciam os próprios algoritmos, porque as suas recomendações e previsões iniciais influenciam a realidade no terreno. Essa realidade torna-se, então, a base para a coleta de dados na atualização de algoritmos; ou seja, a saída do sistema torna-se a entrada futura no mesmo sistema. Desse modo, qualquer preconceito embutido nos algoritmos utilizados em sistemas preditivos de policiamento pode, portanto, ser potencialmente reforçado e exacerbado ao longo do tempo (Agência dos Direitos Fundamentais da União Europeia, 2022)..

Os ciclos de *feedback* podem levar a resultados extremos e que sobrestimam as realidades, tornando-se particularmente problemáticos quando aplicados em áreas do policiamento preditivo. Vários fatores podem contribuir para a formação de ciclos de *feedback*, incluindo taxas baixas e variáveis de denúncia de crimes por vítimas ou testemunhas, diferentes taxas de detecção de crimes, e uso indevido de *machine learning*. Quando as previsões de taxas de crimes, por exemplo, forem baseadas em taxas de denúncia baixas, que não refletem a realidade da ocorrência de crimes, pode levar a previsões incorretas e decisões políticas equivocadas (Agência dos Direitos Fundamentais da União Europeia, 2022).

Ao mesmo tempo, existem evidências demonstrando que baixos níveis de denúncia à polícia podem decorrer das experiências das pessoas com discriminação, ou crimes com base em gênero, etnia, idade e religião, entre outros fatores. Assim, as taxas de denúncia são influenciadas pelas características pessoais das vítimas e pela sua situação socioeconômica, tornando questionável a precisão das fontes de dados oficiais usadas para as previsões de crimes (Agência dos Direitos Fundamentais da União Europeia, 2022).

Ao mesmo tempo, a detecção dos diferentes tipos de crimes também é muito variada, o que também pode influenciar os dados policiais, já que alguns crimes são mais fáceis de serem detectados e registrados. Este é o caso, por exemplo, do crime de roubo de carros, que as pessoas são incentivadas a denunciarem, em razão da necessidade de reclamarem o seguro. Outros crimes, por sua vez não são tão fáceis de serem detectados, tais como corrupção, evasão de divisas e outros crimes financeiros. Desse modo, certos grupos populacionais podem estar mais frequentemente associados a crimes que são mais fáceis de serem detectados. Isso pode levar a previsões tendenciosas ao longo do tempo, pois neste caso as previsões estão excessivamente

focadas em tipos de crimes que são mais prontamente registrados pela polícia.

Além disso, a polícia pode se comportar de maneira diferente em áreas em que se presume terem taxas de criminalidade mais altas. Por sua vez, um aumento na vigilância por parte da polícia em tais bairros pode levar a um aumento nos crimes detectados, o que também pode resultar em outras análises preditivas tendenciosas. Nesta dinâmica, o desenvolvimento de tendencias ou preconceitos (*bias*) nos algoritmos, ao longo do tempo, através de tais ciclos de *feedback*, corre o risco de criar ou reforçar ainda mais práticas discriminatórias, as quais afetam desproporcionalmente grupos com características sociais ou étnicas específicas. Assim, para avaliar o "excesso de policiamento", potencialmente desproporcional de certos grupos sociais, são necessárias avaliações dos resultados (previsões algorítmicas) no que diz respeito à composição dos grupos-alvo (Agência dos Direitos Fundamentais da União Europeia, 2022).

Apesar dos avanços normativos verificados nos últimos anos, a legislação brasileira ainda adota uma postura omissa em relação à vigilância preditiva, bem como ao próprio policiamento ostensivo de uma forma geral. Tal se deve ao fato que não existe no país uma lei regulando o tratamento de dados pessoais no âmbito das Polícias Militares Estaduais ou da Polícia Rodoviária Federal. Entretanto, seria necessário tornar transparente os escopos dos tratamentos de dados pessoais realizados pelas polícias, bem como das capacidades tecnológicas de cruzamento e monitoramento eletrônico utilizados pelas instituições policiais que realizam as ações preventivas de segurança pública. Somente com o estabelecimento de regras específicas, acerca dos limites e fundamentos dos sistemas de vigilância preditiva, ou até mesmo, da atividade policial proativa em um sentido mais amplo, seria possível evitar ações policiais preconceituosas e enviesadas contra grupos sociais vulneráveis.

4.4. JUSTIFICATIVAS ÉTICO-JURÍDICAS E LIMITES DO PODER DO ESTADO DE REALIZAR O TRATAMENTO DE DADOS PESSOAIS PARA FINS DE INVESTIGAÇÃO CRIMINAL E PREVENÇÃO AO CRIME

A proliferação de dispositivos e soluções tecnológicas para a coleta de dados pessoais está modificando a face da atividade policial, refletindo-se também em mudanças sociais mais amplas, que influenciam a compreensão de nossa sociedade sobre o que constitui segurança pública. Os desafios em fornecer serviços de segurança, e de fazer com que as pessoas se sintam seguras, mudam ao longo dos tempos e através das diversas culturas.

Em muitos casos, a retórica em torno da segurança oscila com facilidade entre fenômenos criminais bastantes distintos, tais como o terrorismo internacional, o crime

organizado e os grupos criminosos regionais ou locais. Dispositivos criados para serem usados inicialmente apenas contra ameaças militares, como vigilâncias eletrônicas, câmeras de alta resolução, sensores termais e drones, agora são implantados nas cidades, para dar às pessoas uma sensação de segurança no uso diário do espaço público. Do mesmo modo, grandes sistemas de coleta e armazenamento de informações pessoais, com a organização sistemática de dados individualizados de pessoas consideradas, por algum motivo, uma ameaça à sociedade, que antes eram utilizados somente por serviços secretos de países militarmente desenvolvidos, agora são utilizados por forças policiais nacionais, regionais e até mesmo municipais (Sloot; Broeders; Schrijvers, 2016).

Com a migração das polícias do campo analógico para o digital (Lott; Cianconi, 2018), o tratamento de dados pessoais, no âmbito das atividades de segurança pública, pode se tornar uma atividade cada vez mais invasiva, inclusive com a realização das chamadas vigilâncias preventivas. Dessa forma, surgem questões sobre a natureza e os limites do poder do Estado, de coletar e analisar dados pessoais, tanto com o objetivo de prevenir crimes ainda não ocorridos quanto de investigar crimes já praticados, sendo necessário lançar luz sobre os fundamentos éticos e jurídicos que justificam essa atividade.

O problema da justificativa do exercício do poder estatal por meio de instituições do sistema de justiça criminal, da capacidade do Estado de restringir direitos e liberdades de membros de uma sociedade, constituem-se em um dos temas centrais da teoria do Estado como detentor do monopólio organizado da força (Dias, 1999). Tais abordagens fornecem as bases conceituais que justificam a própria existência das instituições policiais, e que constituem os principais instrumentos que o Estado se utiliza para exercer seu poder de punir

Segundo a definição de Max Weber, o Estado moderno seria uma entidade que possui um território definido, um governo centralizado e o monopólio do uso legítimo da violência física para fazer cumprir suas leis e manter a ordem social. Em relação à sua atuação no campo criminal, o Estado pode ser encarado como uma “empresa de dominação”, que se utiliza do recurso da violência, em forma de monopólio, para se impor. Por este enforque, verifica-se que o fundamento de legitimação do poder das instituições policiais estaria no exercício do monopólio legal da violência pelo Estado. Neste caso, o Estado utiliza de uma violência legítima, porque ela é autorizada pelo Direito (Weber, 2009). Desse modo, o poder punitivo do Estado pressupõe uma atividade normativa anterior à própria ação dos órgãos do sistema de justiça criminal, com a criação de leis que disciplinam a atuação dos agentes públicos e que estabelecem os procedimentos, bem como definem os casos e condições de legitimidade da intervenção estatal (Choukr, 2001).

Para Ferrajoli, diversas intervenções estatais na esfera da liberdade individual dos cidadãos representariam o exercício do monopólico da força pelo Estado, tais como: i) medidas de segurança pública; ii) medidas de prevenção de crimes; iii) as medidas de detecção ou repressão a crimes; e iv) medidas de investigação criminal. Para o jurista italiano, todas essas atividades policiais constituem restrições à liberdade pessoal e aos direitos das pessoas, que sofrem a intervenção do Estado penitenciário (Ferrajoli, 2002).

Assim, o poder do Estado de realizar o tratamento de dados pessoais possuiria os mesmos fundamentos éticos-jurídicos, que justificam o exercício do monopólio do uso da força de uma forma geral. Isso porque o poder punitivo do Estado abarca todas as medidas de prevenção, investigação, detecção ou repressão de infrações, ou medidas estatais de defesa social e controle da ordem pública diversas da "pena" estritamente dita, ou seja, da sanção penal imposta pelo juiz ao criminoso em razão da prática de um crime. O controle institucionalizado da violência estatal engloba desde o momento em que se tenta detectar uma pessoa, que pode estar envolvida com um crime, indo até o julgamento pelo Poder Judiciário e a posterior execução de sanções penais no sistema penitenciário (Ferrajoli, 2002).

As teorias que buscam justificar o poder punitivo estatal não analisam um simples problema abstrato, ainda que este assunto esteja sendo discutido ao longo dos séculos, pois se trata de um tema de enorme atualidade prática (Roxin, 1998). A razão pela qual a Ciência Penal persiste na discussão acerca do poder punitivo do Estado é que, a partir dela, podem ser abordadas as questões centrais da legitimação, fundamentação, justificação e função da intervenção penal estatal (Dias, 1999).

Dessa forma, as teorias que tentam justificar o poder punitivo do Estado podem ser adaptadas à realidade atual do uso de tecnologias no campo das atividades policiais, subsidiando reflexões sobre problemas relacionados à legalidade, ética e aceitabilidade social dos processos de tratamento de dados pessoais para fins de prevenção, investigação, detecção ou repressão de crimes, bem como a execução de sanções penais. Existem diversos teóricos que abordam o tema do uso da violência pelo Estado, oferecendo perspectivas diferentes sobre a formação e a necessidade do monopólio da força como um elemento central do governo e da organização social, tais como Thomas Hobbes, Max Weber, Charles Tilly e Franz Oppenheimer. A própria expressão "monopólio da violência do Estado" (*Gewaltmonopol des Staates*) foi inicialmente mencionada por Max Weber na conferência "A política como vocação" (*Politik als Beruf*), publicada no ano de 1919 (Weber, 2015).

Entretanto, visando uma abordagem ético-jurídica, a presente pesquisa se utiliza da análise das teorias do poder punitivo geral do Estado, tais como realizadas por Luigi Ferrajoli

no seu livro "Direito e Razão – Teoria do Garantismo Penal" (Ferrajoli, 2002). Além de analisar as diversas correntes ético-filosóficas que justificam o uso da violência pelo Estado, a referida obra também descreve as funções e as atividades exercidas pela polícia[12], tendo influência no meio jurídico brasileiro e internacional por lançar as bases teóricas da corrente do Direito Penal, que passou a ser denominada "Garantismo Penal" (Ferrajoli, 2002).

Para Ferrajoli, o primeiro pressuposto da função garantista do direito e do processo penal é o monopólio legal e judiciário da violência repressiva (Ferrajoli, 2002). Nesse sentido, as correntes teóricas que justificam a intervenção penal estatal – ou justificacionistas[13] – se dividem em duas categorias: i) as teorias retributivistas ou absolutas; e ii) as teorias utilitaristas ou relativas. Para as teorias retributivistas, a necessidade de punição de um criminoso decorre de sua culpa, e a severidade da punição deve depender do grau de depravação de seu ato, sendo a imposição da violência pelo Estado a realização de uma ideia de justiça, de tradição filosófica idealista e cristã.

Por sua vez, são consideradas utilitaristas as teorias que justificam o poder punitivo como meio para a realização do fim utilitário de prevenir futuros crimes. Para as teorias retributivistas, a legitimidade da intervenção Estatal é condicionada por finalidades punitivas, sendo uma retribuição pelo dano causado do ato que a pessoa cometeu no passado. Já para as correntes utilitaristas, a legitimidade do poder do Estado é condicionada pela sua adequação ou não ao fim perseguido de prevenir crimes, o que exigiria um balanceamento concreto entre os valores do fim e o custo do meio (Ferrajoli, 2002).

Ferrajoli afirma que o apelo das teses retributivistas está na preocupação de que a punição não derive de outro fundamento que não a culpa do sujeito. Tal poderia comprometer o princípio basilar da civilização, no qual somente quem cometeu algum ato ilícito pode sofrer uma limitação ou restrição de seus direitos, como a liberdade, em caráter de sanção (*nulla poena sine crimine – não há pena sem crime*). Esse princípio de retribuição constituiria o axioma A1 do sistema garantista do autor italiano, que considera que uma pena somente é aplicável a quem tenha cometido um delito, sendo a existência prévia do crime a causa ou condição necessária da intervenção estatal. A garantia do caráter retributivo da intervenção penal serve justamente

[12] Para Ferrajoli, as funções de polícia são limitadas a três atividades: i) a atividade investigativa; ii) a atividade de prevenção de crimes e as atividades auxiliares da jurisdição e da administração; e iii) a execução de provimentos jurisdicionais (Ferrajoli, 2002).

[13] Ferrajoli utiliza a nomenclatura "justificacionista" em contraste às chamadas teorias "abolicionistas", que são aquelas abordagens que acusam o direito penal de ilegítimo. Isto porque moralmente não admitem nenhum tipo de objetivo capaz de justificar aflições que o mesmo impõe, ou porque consideram vantajosa a abolição da forma jurídico-penal da sanção punitiva, e a sua substituição por meios pedagógicos ou instrumentos de controle de tipo informal e imediatamente social (Ferrajoli, 2002).

para excluir, à margem de qualquer finalidade preventiva, ou de qualquer outro modo utilitarista, o sofrimento de um inocente, ainda quando seja considerado suspeito, perigoso ou propenso ao delito (Ferrajoli, 2002).

Entretanto, exigir dos órgãos policiais que atuem somente contra pessoas comprovadamente culpadas da prática de crimes seria um contrassenso, pois as atividades de investigação criminal, detecção e prevenção de condutas criminosas buscam justamente identificar autores de práticas criminosas ou, em alguns casos, impedir o seu cometimento. Devido à impossibilidade de que a justificação das investigações criminais seja baseada em um princípio de retribuição (*nulla poena sine crimine*), que condiciona a intervenção punitiva estatal ao delito comprovadamente ocorrido no passado, e com culpa cabalmente demonstrada, não seria possível utilizar as teorias retributivistas para amparar teoricamente o poder investigativo do Estado.

Desse modo, a análise das teorias do poder de intervenção do Estado, conforme exposto por Ferrajoli, indica que a atividade de tratamento de dados, para fins de investigação criminal e segurança pública, deve possuir os contornos utilitarista de adequação entre meios e fins, não sendo possível extrair sua justificativa de um fim ou do valor natural intrínseco. Somente as correntes teóricas utilitaristas podem servir para justificar a necessidade do Estado de interferir na esfera da liberdade individual, impondo restrições às liberdades individuais, ainda que sem uma demonstração da existência concreta do crime ou da participação efetiva da pessoa em uma conduta ilícita (Ferrajoli, 2002).

O utilitarismo penal pode ser distinguido segundo o critério do destinatário da prevenção, geral ou especial, dependendo do fato que se refira à pessoa do delinquente ou a dos indivíduos em geral (Ferrajoli, 2002); bem como pelo critério relacionado à natureza da intervenção estatal, que pode ser positiva ou negativa. Tem-se, então, quatro tipos de doutrinas relativas ou utilitaristas, justificadoras do poder punitivo do Estado: i) a doutrina da prevenção especial positiva ou da correção, que confere à intervenção penal a função positiva de corrigir o criminoso; ii) a doutrina de prevenção especial negativa ou da incapacitação, que confere ao poder punitivo a função de eliminar ou neutralizar o criminoso; iii) a doutrina da prevenção geral positiva ou da integração, destinada à reforçar a fidelidade dos indivíduos à ordem jurídico-social constituída; e iv) a prevenção geral negativa ou da intimidação, que confere ao poder punitivo a função de dissuadir os indivíduos, por meio do exemplo ou da ameaça que a mesma constitui.

No que diz respeito a redes criminosas profissionais, em relação às quais o Estado pode se utilizar de técnicas proativas e secretas de produção de informações, o tratamento de dados

possui evidente capacidade de prevenção ou de profilaxia criminal. Ao interromper atividades ilícitas organizadas, por meio da identificação de seus autores e ações, visando a restrição da liberdade de ação que possuem para cometer crimes, bem como pela localização e apreensão dos produtos e instrumentos do crime (prevenção especial negativa), o tratamento de dados tem também o potencial de dissuadir outros criminosos de praticarem condutas ilícitas, devido ao receio de serem igualmente identificados e descobertos (prevenção geral negativa).

Do mesmo modo, ao mostrar capacidade de produzir informações de qualidade sobre crimes, agindo para evitar seu cometimento ou punir os responsáveis, o Estado reafirma a validade de suas normas penais, reforçando a fidelidade dos indivíduos à ordem jurídica constituída (prevenção geral positiva)[14]. O tratamento de ados pessoais constitui, desse modo, um meio utilizado pelo Estado com o fim de evitar danos presentes e futuros causados pelo crime, o que pressupõe o balanceamento entre os custos causados aos direitos dos titulares de dados, os benefícios obtidos com a produção de informações sobre a existência de atividades ilícitas e a identificação de criminosos.

Sob essa perspectiva, o que torna legítimo o exercício do poder do Estado, de realizar o tratamento de dados de um membro da sociedade, é a demonstração de sua capacidade de maximizar o bem-estar geral da comunidade organizada. Assim, reconhecendo-se a natureza utilitária dos fundamentos do poder estatal de produzir informações, não sendo plausível que seu exercício tenha como justificativa um fim ou valor de viés retributivista, a adequação entre meios e fins passa ser uma condição necessária de legitimidade a qualquer apuração criminal.

4.4.1. Utilitarismo

Há muitas formas de utilitarismo, e o desenvolvimento dessa teoria tem sido continuada nos últimos anos (Rawls, 2000). Exposta de forma sistematizada pelo filósofo inglês Jeremy Bentham (1748-1832), a teoria utilitarista é formulada de maneira simples, e tem apelo intuitivo: o mais elevado objetivo da moral é o de maximizar a felicidade, assegurando a hegemonia do prazer sobre a dor. De acordo com Bentham, a aprovação ou desaprovação de determinada ação condiciona-se à sua tendência para aumentar ou diminuir a felicidade, raciocínio que se aplica não apenas a um indivíduo particular, mas também a todas as medidas

[14] Assim, dentre as quatro doutrinas relativas ou utilitaristas, justificadoras do poder punitivo do Estado, somente a prevenção especial positiva ou da correção do réu não teria relação direta com tratamento de dados. O tratamento de dados é uma atividade estatal, que visa prevenir, investigar ou reprimir crimes, sendo que a função positiva de corrigir o réu estaria a cabo de políticas públicas de inclusão social.

do governo (Bentham, 2002). Ainda segundo Bentham, ao determinar as leis ou diretrizes a serem seguidas, um governo deve fazer o possível para maximizar a felicidade da comunidade em geral (Sandel, 2011).

Um dos elementos mais importantes da teoria de Bentham para a abordagem proposta nesse trabalho é a ideia de que os seres humanos agem como maximizadores racionais da própria satisfação. Assim, ao tornar explícito que a intervenção punitiva do Estado é um método de impor custos à atividade criminal, Bentham lançou as bases da moderna análise econômica do crime e das penas (Posner, 2010a). Pelo princípio da utilidade, uma sociedade está adequadamente ordenada quando suas instituições maximizam o saldo líquido de satisfação de seus integrantes, avaliando as vantagens presentes e futuras, com perdas também presentes e futuras (Rawls, 2000). As pessoas, os legisladores, o governo e os juízes devem levar em consideração se determinada diretriz, após subtraída de todos os custos, produzirá mais felicidade geral do que uma decisão alternativa.

Para Bentham, todo argumento moral deve se inspirar implicitamente na ideia de maximizar a felicidade humana. As pessoas não teriam base para defender tais deveres e direitos, se não acreditassem que isto traria como consequência a maximização da felicidade geral da sociedade, pelo menos a longo prazo (Sandel, 2011).

Ao polemizar com o retributivismo vingativo, os utilitaristas consideram que, no exercício da violência legal, não é necessário que o Estado se preocupe com o mal já ocorrido, mas sim com o bem futuro, não sendo lícito infligir penas com o objetivo de corrigir o pecador, ou de melhorar os outros com a advertência da pena imposta. Sendo assim, “as aflições penais, [como] afirmam Motesquieu, Voltaire, Beccaria e Bentham, são preços necessários para impedir males maiores, e não homenagens à ética ou a religião, ou, ainda, ao sentimento de vingança” (Ferrajoli, 2002, p. 210).

A visão utilitarista parte do princípio de que somente as consequências futuras de uma decisão devem ser objeto de consideração, tendo em vista que a tutela penal é justificável apenas como dispositivo de manutenção de ordem social. A intervenção estatal é justificável se puder ser mostrada como fator de promoção efetiva dos interesses da sociedade, caso contrário, não. As teorias relativas reconhecem que a intervenção penal, como instrumento político-criminal, traduz-se em um mal para quem a sofre, e como tal, para se justificar, tem que alcançar sua finalidade precípua de prevenção ou profilaxia criminal (Dias, 1999).

O utilitarismo clássico preceitua um consequencialismo hedonista: a felicidade se consiste unicamente no prazer e na ausência de dor. Como o prazer é o único bem intrínseco – e a dor é o único mal intrínseco –, um ato é moralmente correto se maximiza “a maior felicidade

para o maior número de pessoas" (Stanford Encyclopedia of Philosophy, 2023). Entretanto, a ampliação da forma como prazer e a dor passaram a ser interpretados fez do utilitarismo uma teoria mais complexa do que poderia parecer à primeira vista, tornando-o sujeito a ataques de vários ângulos, lançados por opositores de diversos campos do pensamento filosófico[15].

Assim, a maioria dos utilitaristas modernos deixou de utilizar termos como "felicidade", "prazer" e "dor", por acreditar que eles remetem à discussão do hedonismo, passando a empregar termos mais neutros, como "bem-estar", "bem-estar social", "benefício" e "custo" (Mulgan, 2012). Do mesmo modo, o utilitarismo permitiu a construção de uma ampla variedade de teorias morais que lhe são derivadas. Essas teorias passaram a ser denominadas "consequencialistas" ao invés de "utilitaristas", para que não estivessem sujeitas às refutações associadas com a teoria utilitarista clássica hedonista. Assim, o termo "consequencialismo" costuma ser usado como referência a qualquer teoria originada do utilitarismo clássico, e que com ele mantenha em comum o fato de considerar que a propriedade moral de um ato depende exclusivamente de suas consequências, e não de verdades intrínsecas e auto evidentes. Se este postulado é também descartado, a teoria deixa de ser consequencialista. Uma teoria moral é consequencialista quando avalia atos, traços de caráter, práticas e instituições, apenas sob perspectivas da sua capacidade de promover consequências benéficas (Stanford Encyclopedia of Philosophy, 2023).

O utilitarismo calculista de Bentham[16] foi reformulado por John Stuart Mill[17] (1806-1873), que procurou conciliar a teoria com os direitos individuais ao estabelecer como seu princípio central de que as pessoas devem ser livres para fazer o que quiserem, contanto que não façam mal aos outros. Para Mill, "[...] o único propósito pelo qual o poder pode ser constantemente exercido sobre qualquer membro de uma comunidade, contra a vontade deste,

---

[15] Um dos pontos de vista contra o utilitarismo hedonista encontra-se na história da máquina de sensações de Nozick (cf. o filme "Matrix"). Pessoas conectadas a essa máquina de realidade virtual experimentariam sensações muito aprazíveis, em um mundo ilusório, embora os fatos que gerassem tais prazeres de fato nunca ocorressem (ganhar medalhas de ouro em uma Olimpíadas, a indicação para receber prêmios Nobel, ter relações sexuais com seus amantes favoritos etc.). Uma vez que seria irracional ligar-se a esta máquina, o hedonismo parece inadequado. Para Nozick, conectar-se seria uma má opção, pois nosso bem-estar não é determinado apenas por experiências, mas pela maneira como as coisas se nos apresentam subjetivamente, pois as verdadeiras origens dessas experiências também importam (Stanford Encyclopedia of Philosophy, 2023).

[16] Bentham foi o autor de várias ideias utilitárias radicais, tais como a de que as pessoas deveriam ter seus nomes tatuados no corpo, para facilitar a execução das leis penais; a abolição do júri e do sigilo profissional do advogado; além de ter proposto uma política pública radical em relação aos mendigos. Entretanto, ressaltar somente as tendências repressivas do pensamento de Bentham seria uma injustiça, pois não pode ser esquecida a sua luta pela liberdade religiosa, pelo divórcio civil, por um sistema penal racional, pela reforma processual, entre outras melhorias sociais (Posner, 2010a, p. 50-51).

[17] John Stuart Mill foi membro do Parlamento inglês, e esteve frequentemente envolvido com causas radicais para a época, especialmente a dos direitos das mulheres, o combate à escravidão e o direito dos animais (Mulgan, 2012).

é o de prevenir danos para os outros membros. O próprio bem dele, seja físico ou moral, não é causa suficiente" (Mill, 2010, p. 49).

Segundo Mill, o governo não deve interferir na liberdade individual a fim de impor as crenças da maioria no que concerne à melhor maneira de viver, pois os únicos atos pelos quais uma pessoa deve explicações à sociedade são aqueles que atingem aos demais. Desde que não esteja prejudicando o próximo, a independência do indivíduo é, por direito, absoluta. Ainda para Mill, no que diz respeito a si mesmo, ao próprio corpo e à mente, o indivíduo é soberano (Sandel, 2011). Em contrapartida, Mill renuncia à qualquer ideia que provenha do direito abstrato, como algo independente da teoria utilitarista, que seria a instância final de todas as questões éticas. Mill acredita que a utilidade deve ser maximizada em longo prazo, e não caso a caso, tendo em vista que, com o tempo, o respeito à liberdade individual levará à máxima felicidade humana (Sandel, 2011).

O enfoque utilitarista da investigação criminal, por outro lado, faz com que os métodos de produção de provas devam ser privados de qualquer caráter punitivo. Como a fundamentação teórica da atividade de investigação criminal não encontra sua justificativa nas teorias retributivistas, a interferência causada aos direitos do investigado não pode resultar em aflições ou sofrimentos, e que não estejam diretamente relacionados à produção de informações sobre o crime investigado. Uma técnica de análise de dados poderia ser considerada de natureza punitiva, quando o dano imposto ao indivíduo não constituísse o meio necessário para a produção da informação que se visa obter. Assim, por um enfoque utilitarista, a justificação das atividades de tratamento de dados pessoais depende de um equilíbrio entre os custos da ação estatal sobre o indivíduo, e os benefícios derivados para a segurança pública.

Esses benefícios decorrem da probabilidade de que as atividades de tratamento de dados resultem, de fato, em informações importantes, relacionadas à prevenção, detecção e investigação de crimes. Por sua vez, os custos das medidas estatais devem ser analisados, em função do dano que eles representam aos direitos das pessoas que têm seus dados tratados por instituições policiais. Desse modo, o exercício do poder de realizar o tratamento de dados pessoais deve satisfazer, exclusivamente, a necessidade do Estado de possuir informações sobre condutas criminosas, o que lhe permite proporcionar as condições necessárias de proteção comunitária.

A justificativa para o uso de sistemas de tratamento de dados pessoais, no âmbito da investigação criminal e segurança pública, não possui fundamento em si próprio, estando o emprego de novas tecnologias ancorado na promoção do bem coletivo de segurança pública. Por esse motivo, torna-se necessário ressaltar os benefícios que os diversos recursos

informacionais utilizados pelas polícias representam para a sociedade, pois a coleta e análise de dados pessoais somente encontra sua legitimação caso esteja estritamente condicionada aos valores do Estado Democrático de Direito, e às garantias de respeito aos direitos individuais daqueles que sofrem interferência em sua liberdade informacional. Seguindo a perspectiva da teoria de Stuart Mill, apenas a proteção do direito e da liberdade de outros pode justificar que, de cada pessoa, seja retirada uma parcela de sua liberdade informacional, mesmo que seja temporariamente, pois para assegurar à sociedade a liberdade e o direito de proteção, pode o Estado democrático, pluralista e laico limitar direitos individuais, notadamente, a privacidade (Mill, 2010).

A legitimidade dos sistemas de tratamento de dados pessoais deve estar condicionada pela sua adequação ou não ao fim perseguido, o que exige um balanceamento concreto entre o valor para a sociedade resultante da descoberta de práticas criminosas, e os custos aos direitos individuais causados pelos meios tecnológicos utilizados pelas instituições. Segundo este enfoque utilitarista, as consequências do tratamento de dados devem ser o ponto central de suas considerações de ordem ética, justificando-se a adoção de medidas invasivas apenas como dispositivo para se descobrir atos ilícitos em andamento ou prestes a serem cometidos, bem como para a descoberta de provas de crimes já cometidos. Em todo coso, o tratamento de dados deve visar unicamente a produção de informações necessárias para a promoção efetiva dos interesses da sociedade.

Ressalte-se que, ao se calcular os benefícios promovidos pela intervenção penal estatal, deve ser levado em consideração os efeitos sociais futuros de determinada tecnologia a ser adotada pelos órgãos policiais em suas atividades de prevenção e repressão de crimes; e não apenas as vantagens imediatas relacionadas à resolução de um caso ou de um problema específico. A existência de sistemas de informação policial seria justificada pela necessidade de se impedir violações de direitos de uns por outros, sendo a manutenção da organização social um dos fundamentos essenciais de toda sociedade harmônica e organizada.

No entanto, a desconfiança dos cidadãos sobre as instituições policiais estatais também pode corroer os vínculos de civilidade que unem uma determinada comunidade. Por este motivo, um modelo de tratamento de dados deve levar em consideração a promoção, ao longo do tempo, dos direitos individuais, enquanto fator propulsor da vida comunitária harmônica. Desse modo, os efeitos que um sistema policial de tratamento de dados pessoais pode causar na comunidade devem ser examinados à luz dos interesses em jogo, em cada contexto social e político, verificando-se suas causas, seus custos e suas consequências.

Medidas inspiradas na máxima de que “todos os fins justificam os meios” são

incompatíveis com o Estado de Direito, enquanto um sistema de poder disciplinado e limitado. É certo que os indivíduos depositam na esfera pública uma parcela de sua liberdade, mas somente o mínimo necessário para garantir a sua própria segurança. Assim, sobre o prisma da razão utilitarista, somente seria aceitável sistemas de tratamento de dados de segurança pública e investigação criminal que tenham como ponto de referência o bem-estar e a utilidade não dos governantes, mas sim dos seus governados (Posner, 2012).

Outrossim, seria importante ressaltar que a própria CI pode fornecer subsídios para a manutenção do equilíbrio entre as garantias individuais e a utilidade no acesso a dados pessoais pelas polícias. Ao abordar a análise dos processos de construção, comunicação e uso da informação, a CI considera que a questão da utilidade dos dados, versus a proteção da privacidade, está diretamente ligada à forma de satisfazer a necessidade do usuário. Por sua vez, a satisfação do usuário tem relação com o significado que esses dados irão trazer, tornando possível a apropriação da informação sobre determinado contexto (Affonso; Oliveira; Sant'Ana, 2017).

Não basta a informação estar disponível, ela precisa também ser útil. Assim, caso a polícia armazene e trate dados com os identificadores pessoais suprimidos, com o uso de técnicas como a anonimização, estes dados perdem parte de sua utilidade ao impossibilitar a associação, direta ou indireta, a um indivíduo (Brasil, 2018b). Nestes casos, a utilidade do conjunto de dados constitui um desafio, pois ao utilizar métodos para a proteção da privacidade, pode-se também diminuir a utilidade dos dados (Affonso; Oliveira; Sant'Ana, 2017).

Não é relevante disponibilizar um conjunto de dados se estes não apresentarem utilidade para o usuário, pois "[...] o objetivo final de um produto de informação, de um sistema de informação, deve ser pensado em termos de usos dos dados e informação e dos efeitos resultantes desses usos nas atividades dos usuários" (Le Coadic, 1996, p. 39 *apud* Affonso; Oliveira; Sant'ana, 2017). Em qualquer processo de proteção do indivíduo contra a interferência estatal abusiva, deve-se buscar o equilíbrio entre a utilidade pública verificada no tratamento dos dados e a proteção dos indivíduos a quem os dados se referem. Neste sentido, quanto maior a proteção dos dados, maior a tendência à liberdade individual e, consequentemente, também é maior a probabilidade de redução da utilidade dos dados disponibilizados. Por outro lado, uma proteção dos dados pessoais mínima pode garantir e manter a máxima utilidade dos dados disponibilizados. No entanto, também pode significar riscos ou violação das liberdades individuais dos titulares dos dados (Affonso; Oliveira; Sant'Ana, 2017).

4.4.2. Os direitos humanos como limite ao poder do Estado de realizar o tratamento de dados pessoais

A crítica geral que os adeptos das teorias absolutas fazem às teorias relativas é a de que estas, ao aplicarem o poder punitivo em nome de fins utilitários, transformariam a pessoa humana em objeto, e, nesta medida, violariam a sua dignidade. Esta questão levaria à mais importante objeção contra a teoria punitiva da prevenção geral, ou seja, a dificuldade de se entender como justo o mal imposto a alguém, para que outras pessoas se sintam protegidos contra um risco ou dando. Por tal enfoque, o indivíduo não pode ser utilizado como meio para a proteção de outros, pois isso atentaria contra a dignidade humana (Roxin, 1998).

Do mesmo modo, as teorias utilitaristas da prevenção especial ou geral não resistiriam a um exame crítico, pois ambas não possibilitam uma delimitação do poder punitivo do Estado quanto a seus pressupostos e consequências. Embora deva dirigir-se de antemão apenas contra os inadaptados à sociedade, é possível que um regime autoritário no poder submeta a controle seus inimigos políticos, bem como grupos de indivíduos ou parcela da sociedade que passarem a ser considerada criminosa, tais como “mendigos”, “vagabundos”, “subversivos”, “inimigos do povo”, e outras pessoas indesejáveis para os extratos superiores da comunidade (Roxin, 1998).

É possível que, em regimes antidemocráticos de governo, sejam utilizados sistemas de tratamento de dados do Estado para a coleta de dados e elaboração de informações sobre inimigos políticos, bem como de grupos de indivíduos ou parcelas da sociedade que passem a ser considerados indesejáveis ou perigosos, por parte daqueles que detém o poder econômico e político do país. Em uma vertente autoritária, por exemplo, poderia não ser delimitável a duração ou a profundidade do tratamento de dados pessoais para fins criminais ou de segurança púbica, podendo, no caso concreto, ser utilizado novas tecnologias de vigilância e monitoramento, que ultrapassassem os limites necessários para a promoção do bem comum (Roxin, 1998).

Conforme mencionado na subseção 4.2 do presente trabalho, J. Edgar Hoover era conhecido por suas habilidades na organização da informação, e por sua ênfase na coleta meticulosa de dados e informações, tendo utilizado com eficiência as teorias da CI para estruturar o sistema de bancos de dados do *Federal Bureau of Investigation* (FBI). Quando ainda chefiava a Escritório de Inimigos Estrangeiros, do Departamento de Justiça dos Estados Unidos, logo após a entrada dos Estados Unidos na Primeira Guerra Mundial, Hoover foi o

responsável pela supervisão de 6.200 alemães que estavam internados em campos, e a outros 450.000 que estavam sob vigilância do governo. Com base nos dados tratados, a unidade chefiada por Hoover foi a responsável por identificar e efetuar a prisão de vários estrangeiros considerados politicamente suspeitos, por estarem envolvidos em atos de espionagem (Weiner, 2012).

Entretanto, as ações do primeiro e mais longevo diretor do FBI também representam um dos maiores exemplos de como o tratamento de dados e informações pessoais pode ser utilizado em ações abusivas. Durante sua gestão (1924 a 1972), o FBI estabeleceu um sistema de coleta e armazenamento de informações altamente centralizado e confidencial, que muitas vezes ultrapassou os limites legais e éticos, tendo estimulado a vigilância extensiva de inimigos políticos e movimentos organizados da sociedade civil. A partir desse sistema estruturado, Hoover acumulou um imenso poder e influência política, sendo que sua excessiva busca por informações e seu desejo de controlar muitos aspectos do FBI resultaram em abusos de poder, e diversos casos de violações de direitos humanos (Weiner, 2012, p. 48).

Hoover levou para o FBI a mesma metodologia que ele aprendeu a utilizar quando passou a controlar a Divisão de Radicais do Departamento de Justiça dos EUA, ainda em 1919, sendo então o responsável pelas operações realizadas contra políticos da extrema esquerda e anarquistas do país. Este era um momento de grande ansiedade nos Estados Unidos, impulsionado por uma onda mortal da gripe pandêmica, a revolução bolchevique na Rússia e a subsequente e exagerada "*Red Scare*" (medo do comunismo), além de greves laborais, por vezes violentas, em todo o país.

Após um anarquista militante, de nome Carlo Valdinoci, ter explodido a frente da casa do recém-nomeado Procurador-Geral, A. Mitchell Palmer, em Washington, Hoover foi indicado para assumir a divisão, criada para reunir informações sobre a ameaça radical de esquerda (FBI, 2023). Neste contexto, Hoover coletou e organizou todos os fragmentos de informação, que estavam dispersos em diversos bancos de dados de organismos do governo, com a criação de arquivos sobre dezenas de milhares de pessoas consideradas suspeitas de envolvimento com os movimentos comunistas e anarquistas, tendo por objetivo a planejar uma grande captura em massa.

Assim, com base no tratamento dos dados das pessoas consideradas suspeitas de envolvimento com atos subversivos, Hoover coordenou uma das maiores detenções em massa da história dos Estados Unidos, a denominada Operação Palmer (*Palmer Raids*). Assim, foram desencadeadas, nas primeiras semanas de 1920, uma série de ações visando a detenção e deportação dos alvos selecionados. Hoover coordenou entre 6.000 e 10.000 capturas executadas

em reuniões políticas, residências privadas, clubes sociais, salões de baile, restaurantes e outros locais espalhados pelo país (Weiner, 2012).

Já na década de 1960, o FBI direcionou sua capacidade de coleta e análise de dados para líderes e organizações do movimento dos direitos civis, como Martin Luther King Jr., cujas atividades foram meticulosamente monitoradas e documentadas durante muitos anos. Nestes casos, foram coletadas inclusive informações pessoais comprometedoras, que eram utilizadas para tentar exercer influência sobre o principal líder do movimento pelos direitos civis nos Estados Unidos. Neste contexto, cidadãos norte-americanos poderiam acabar na lista de inimigos de Hoover, somente por terem sido vistos por um informante em uma manifestação ou reunião de organizações civis, ou mesmo por assinar qualquer um dos diversos jornais radicais (Weiner, 2012).

Assim, as práticas de Hoover servem como advertência sobre as ameaças potenciais às liberdades individuais, quando a coleta e o tratamento de dados pessoais não são devidamente regulamentados e controlados. Torna-se necessário, deste modo, definir claramente quais as utilidades trazidas para a sociedade pelos sistemas de processamento de dados pessoais utilizadas pelos órgãos de segurança pública, bem como os danos que tais inovações tecnológicas podem causar à privacidade de cada indivíduo isoladamente.

O risco de que investigadores criminais possam fazer o mal uso do poder estatal, através de um cálculo utilitário que os convença de estarem promovendo o bem comum, foi agravado com o desenvolvimento das tecnologias de armazenamento e análise de dados. Avanços tecnológicos ampliaram consideravelmente as possibilidades de atuação dos órgãos de segurança pública, que passaram a intervir na vida privada dos indivíduos, por meio de ações de prevenção e investigações criminais proativas. Desse modo, os poderes estatais somente podem ser legitimamente exercidos caso as instituições responsáveis sigam regras gerais de promoção do bem comum, e cumpram estritamente as normas que regulam o tratamento de dados pessoais.

A proclamação de ser a pessoa portadora de direitos, estabelecidos em declarações, tratados e jurisprudências internacionais – constituídas por sentenças das Cortes Internacionais –, e comentários gerais – elaborados pelos órgãos do sistema de Direitos Humanos –, confunde-se com a própria democracia, enquanto vida coletiva de alto padrão civilizatório, terminando a sociedade por se autoconferir a credencial de culturalmente avançada (Britto, 2016). Desta maneira, as regras de proteção aos direitos humanos[18] podem servir como fundamento de

[18] Os direitos humanos se referem ao conjunto de normas jurídicas estabelecidas em declarações, tratados, princípios gerais e outras fontes de Direito Internacional. Por sua vez, os direitos fundamentais são preceituados

legitimidade para um modelo de tratamento de dados pessoais moderno, concebido de forma a viabilizar um sistema de segurança público justo e efetivo. Não há nenhum aspecto da atuação dos órgãos de segurança pública que não esteja imbricado com as normas internacionais de direitos humanos, sendo o tratamento de dados pessoais mais um tema que deve ser abordado sob este prisma. A concepção dos direitos humanos pressupõe indiscutivelmente a pessoa, enquanto portadora de direitos reconhecidos internacionalmente, os quais devem ser levados em consideração na adequação entre os fins e os meios do tratamento de dados.

Em uma sociedade democrática, os órgãos policiais responsáveis pelo tratamento de dados pessoais devem reconhecer e acolher o respeito aos direitos humanos, principalmente a privacidade e o direito à liberdade informacional, como componentes dos cálculos utilitaristas de promoção do bem-estar social. Os titulares de dados pessoais são portadores de direitos humanos, como estabelecidos em declarações, tratados e jurisprudências internacionais, constituídas por sentenças das Cortes Internacionais, e comentários gerais elaborados pelos órgãos do sistema de Direitos Humanos. Assim, as regras de proteção aos direitos humanos servem como fundamento de legitimidade para um modelo de tratamento de dados pessoais moderno, concebido de forma a viabilizar um sistema de segurança público justo e efetivo (Schutter, 2010).

Todos esses fatores justificam uma abordagem do tratamento de dados realizados no âmbito policial à luz da teoria dos direitos humanos, com a utilização de tratados e decisões de Corte Europeia de Direitos Humanos no desenvolvimento desta pesquisa. Demandas internacionais relacionadas aos direitos humanos buscam promover mudanças em instituições, práticas ou normas legais, não expressando somente meras sugestões, aspirações ou ideais auspiciosos. As regras de direitos humanos servem como instrumentos para cidadãos reivindicarem que determinados padrões internacionais de organização política e governamental sejam adotados em seus países (Donnelly, 2003).

As técnicas de coleta de informações pela polícia e os serviços de segurança têm apresentado rápido desenvolvimento nos últimos anos. Por sua vez, torna-se evidente que a realização do tratamento de dados, com o uso de ferramentas tecnológicas invasivas, inclusive com o emprego de sistemas de captação de áudio e imagem, rastreamento eletrônico e outros mecanismos de coleta de dados pessoais, representa uma séria ameaça aos direitos humanos. Vários direitos civis e políticos, previstos e protegidos por diversos normativos internacionais, podem ser impactados pelas práticas e procedimentos relacionados à promoção da segurança

nas Constituições dos países, e se inter-relacionam com os direitos humanos (Schutter, 2010).

pública e prevenção ao crime. Dentre elas, o direito ao devido processo legal, a presunção de inocência, o direito à liberdade de expressão e o direito à livre associação. Entretanto, no contexto dos sistemas de tratamento de dados utilizados pelos órgãos estatais de segurança pública, o direito à privacidade se destaca como o principal direito humano em risco.

4.4.3. Direito à privacidade

Conforme previsto no Pacto Internacional sobre Direitos Civis e Políticos da ONU (Art. 15), na Convenção Americana sobre Direitos Humanos (Art. 17) e na Convenção Europeia para a Proteção dos Direitos Humanos e Liberdades Fundamentais (Art. 8), o direito à privacidade protege quatro interesses distintos: i) a vida privada; ii) a vida familiar; iii) o domicílio; e iv) a correspondência. Do mesmo modo como ocorre com outros direitos contidos nos diversos tratados e convenções internacionais, o conceito de privacidade, o seu alcance e escopo, é definido pelas Cortes internacionais de direitos humanos, através de decisões que formam sua jurisprudência.

Embora em alguns casos a abordagem do direito à privacidade requeira que as quatro áreas de interesses sejam consideradas separadamente, podendo ser objetivamente delineadas, a jurisprudência da Corte Europeia de Direitos Humanos (CEDH) estabeleceu que tais áreas, de uma forma geral, se sobrepõem (McKay, 2015). A obtenção de informações e tratamento de dados pessoais constitui ampla parcela das atividades dos órgãos de investigação criminal e segurança pública, o que pode acarretar violações à privacidade daqueles que têm os dados coletados e tratados no âmbito de investigações criminais e em ações de prevenção ao crime.

A CEDH considera o termo “vida privada” como um conceito amplo, não suscetível de definição exaustiva. A partir de várias decisões, a CEDH também consolidou o entendimento de que a “vida privada” abrange a integridade física e psicológica da pessoa, e pode também englobar aspectos de sua identidade, como a sua definição de gênero, nome, orientação sexual e vida sexual, que também pertencem à esfera pessoal, protegida pelo Artigo 8º da Convenção Europeia dos Direitos Humanos (Corte Europeia de Direitos Humanos, 2003a).

Do mesmo modo, a Corte Europeia reiterou diversas decisões em que afirma que o Artigo 8º da Convenção também protege o direito ao desenvolvimento pessoal, e o direito de o cidadão estabelecer relações com outros seres humanos e o mundo exterior, incluindo atividades de natureza profissional ou empresarial. Existiria, desta feita, uma zona de interação de uma pessoa com as outras, mesmo em um contexto público, que é englobado no âmbito da "vida privada". Para determinar se informações pessoais conservadas pelas autoridades estatais

envolvem qualquer aspecto de vida privada, a Corte Europeia leva em consideração o contexto em que as informações foram coletadas e retidas, a natureza dos registros e a forma como esses registros são usados e processados (Corte Europeia de Direitos Humanos, 2003b).

Por exemplo, a Corte Europeia já abordou vários aspectos específicos da proteção à privacidade, como na decisão que estabeleceu que o registro de imagens de CFTV, tomadas em um lugar público, podem sim representarem uma interferência na vida privada do indivíduo (Corte Europeia de Direitos Humanos, 2003a), a depender da forma como tais vídeos são coletados e processados. Do mesmo modo, a CEDH tem afirmado repetidamente que o armazenamento e a conservação de dados pessoais pelas autoridades policiais constitui uma ingerência no direito à privacidade, sendo que muitas dessas decisões dizem respeito às justificativas destas ingerências.

Uma decisão da CEDH envolveu um caso relacionado a uma pessoa que foi condenada pela prática de crimes sexuais contra uma menor de 15 anos de idade e que, após cumprir a sua pena de prisão, requereu que a menção desta sentença fosse suprimida do seu registo penal. Entretanto, o pedido foi indeferido em razão de uma lei francesa, que havia criado uma base de dados judicial nacional de pessoas condenadas pela prática de crimes sexuais, na qual o requerente havia sido informado que seu nome seria incluído. O CEDH considerou que a inclusão de uma pessoa, condenada pela prática de crimes sexuais em uma base de dados judicial estava abrangida pelo Artigo 8° da CEDH. Como na lei francesa havia sido implementadas garantias suficientes, em matéria de proteção de dados, tais como o direito de a pessoa titular dos dados requerer a eliminação dos dados, o período limitado de conservação dos dados e o acesso limitado aos mesmos, tinha sido encontrado um equilíbrio justo entre os interesses privados e públicos concorrentes em jogo. Assim, a CEDH concluiu que não tinha havido uma violação do Artigo 8° da CEDH (Corte Europeia de Direitos Humanos, 2009).

Segundo a jurisprudência da CEDH, podem ser impostas limitações ao direito humano à privacidade caso sejam satisfeitas três condições específicas: i) que a interferência esteja prevista em lei, em seu sentido formal e material (condição de legalidade); ii) que os fins a serem alcançados pela restrição sejam legítimos (condição de legitimidade); e iii) que a interferência se limite ao que seja estritamente necessário para o cumprimento do objetivo a que se propõe (condição de proporcionalidade). Embora os diferentes órgãos ou Cortes de direitos humanos apliquem essas condições de várias maneiras, e ainda que suas abordagens não sejam uniformes em todos os aspectos, a gramática básica utilizada para examinar a aceitabilidade das restrições impostas aos direitos humanos é essencialmente a mesma, em todas as jurisdições (Schutter, 2010). Essas condições, que permitem a intervenção do Estado

na vida privada das pessoas, foram incorporadas, de uma forma ou outra, pela Diretiva da EU, que elenca uma série de princípios que devem conformar todas as etapas e as cadeias do tratamento de dados no âmbito da investigação e segurança pública.

Segundo a jurisprudência internacional, o teste de legalidade requer que as leis, em sentido formal e material, que embasam as restrições aos direitos humanos preencham os seguintes critérios: i) serem leis acessíveis (*accessibility*), publicadas e com acesso à sociedade em geral; ii) previsíveis (*foreseability*), isto é, aqueles que provavelmente serão afetados pela restrição aos seus direitos devem ser capazes de entender o significado e a natureza da medida que será aplicada; e iii) precisas (*precise laws*), que seja, a lei deve especificar todas as circunstâncias nas quais as interferências serão permitidas (McKay, 2015). Com base nas decisões da CEDH, os países signatários da Convenção Europeia dos Direitos Humanos, mesmo aqueles que não integram a União Europeia, passaram a regular detalhadamente, em leis específicas, as atividades de suas polícias, tendo em vista o risco de serem submetidos a processos perante aquela Corte.

A condição de legitimidade, por sua vez, implica que a restrição a ser imposta à privacidade observe estritamente a finalidade para a qual se destina a medida, todas de interesse coletivo. Por exemplo, o Artigo 8º, § 1º da Convenção Europeia dispõem que o direito à vida privada somente pode sofrer ingerência quando tal medida constituir uma providência que, em uma sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem, a prevenção de infrações penais, a proteção da saúde ou para a proteção dos direitos e liberdade de terceiros.

Assim, o aspecto mais importante para o cumprimento da Convenção Europeia é definir quando a interferência ao direito à privacidade é "necessária em uma sociedade democrática". Na busca da definição do que seja necessário, a Corte Europeia afirmou no caso que o adjetivo "necessário" não é sinônimo de "indispensável", ou "desejável". Para os juízes da CEDH, a frase "necessária em uma sociedade democrática" significa que, para ser compatível com a Convenção, a interferência deve corresponder a uma "necessidade social premente", e ser "proporcional ao objetivo legítimo perseguido" (Corte Europeia de Direitos Humanos, 1983).

O teste de necessidade em uma "sociedade democrática" requer o equilíbrio entre os direitos do indivíduo, de um lado, e os interesses da comunidade de outro. Necessário não significa "indispensável", mas tampouco significa "razoável" ou "desejável". O que isso implica é uma necessidade social para a restrição do direito, e essa necessidade social urgente deve estar de acordo com os requisitos de uma sociedade democrata, cujas características

fundamentais são a tolerância, o pluralismo e uma mentalidade sofisticada. As condições de legitimidade buscam permitir que os órgãos de monitoramento de direitos humanos examinem os motivos das restrições impostas em casos particulares, com a exclusão das situações ilegítimas; por exemplo, quando as restrições são animadas pelo preconceito contra certos grupos (Schutter, 2010).

A definição do objetivo perseguido pela restrição da privacidade é também decisiva, para que se possa verificar quando a interferência pode ser considerada "proporcional" ou, de acordo com a terminologia da Convenção Europeia sobre os Direitos Humanos, "necessária em uma sociedade democrática". Assim, a legitimidade estaria diretamente relacionada à própria condição de proporcionalidade, cujo atendimento também subordina o regime de limitação da privacidade. Por sua vez, ainda quando seja evidente a existência de um propósito legítimo para a restrição da privacidade de alguém, as autoridades estatais devem demonstrar que a interferência imposta não vai além do que seja estritamente necessário para o alcance daquele objetivo (McKay, 2015). O que a proporcionalidade requer, de qualquer modo, é que exista uma razoável relação entre os meios empregados e os fins desejados.

O termo "proporcionalidade" define uma característica inerente aos tratados e convenções, sendo fundamental para o modo como as Cortes internacionais abordam a proteção do direito à vida privada. O termo proporcionalidade também foi incorporado, ao longo dos anos, à própria atividade investigativa criminal do Estado (McKay, 2015). Por exemplo, em última análise será um aspecto do teste de proporcionalidade que decidirá sobre a necessidade absoluta do recurso a determinada tecnologia. Essencialmente, a proporcionalidade exige que o julgador determine, em última instância, se uma interferência, que visa promover um bem comum, é inaceitável em sua aplicação, ou se esta impõe um encargo excessivo ou irracional a certos indivíduos. Dentre os fatores que devem ser considerados ao se avaliar quando uma atividade de tratamento de dados é ou não proporcional, podem ser citados: i) a existência de medidas menos restritivas que podem ser impostas; ii) a presença de salvaguardas contra o uso abusivo da medida; e iii) a utilização de medidas equitativas no processo de tomada de decisão (Colvin; Cooper, 2009).

4.4.4. Direito à proteção dos dados pessoais

O direito à privacidade surgiu no direito internacional na Declaração Universal dos Direitos Humanos (DUDH), que foi criada em 1948 no âmbito da Organização das Nações Unidas (ONU). Logo após, a Europa também afirmou o direito à privacidade na Convenção

Europeia para a Proteção dos Direitos Humanos e Liberdades Fundamentais (Convenção Europeia dos Direitos Humanos, 1950), um tratado juridicamente vinculativo que foi redigido em 1950. Verifica-se que a DUDH e a Convenção Europeia foram adotadas bem antes do desenvolvimento dos computadores e da internet, e mesmo do surgimento da sociedade da informação. Esses desenvolvimentos tecnológicos trouxeram vantagens consideráveis para os indivíduos e para a sociedade, melhorando a qualidade de vida, a eficiência e a produtividade. Entretanto, ao mesmo tempo, tais avanços representam novos riscos ao direito e ao respeito à vida privada.

Em resposta à necessidade de regras específicas relacionadas à coleta e ao uso de informações pessoais, um novo conceito de privacidade passou a ser considerado no âmbito da União Europeia. Conhecido em algumas jurisdições como “privacidade informativa”, e em outras como “direito à autodeterminação informativa”, este conceito levou ao desenvolvimento de regulamentos legais especiais, que fornecem proteção aos dados pessoais.

Embora derivado diretamente do direito à privacidade, o direito à proteção dos dados pessoais passou a ser considerado, em vários países da Europa, como um direito específico. O Tribunal Constitucional Federal Alemão afirmou o direito à autodeterminação informacional em um julgamento de 1983, que seria derivado do direito fundamental ao respeito à personalidade, protegido na constituição do país. Segundo esse enfoque, o direito ao respeito pela vida privada e o direito à proteção dos dados pessoais, embora intimamente relacionados, são direitos distintos (Conselho da Europa, 2018).

A proteção de dados na Europa teve início na década de 1970, com a adoção de legislação específica por alguns países para controlar o processamento de informações pessoais por autoridades públicas e grandes empresas. Novos instrumentos de proteção de dados foram estabelecidos e, ao longo dos anos, a proteção de dados evoluiu para um valor distinto, que não é embarcado somente pelo direito ao respeito pela vida privada. Assim, o direito ao respeito à vida privada e o direito à proteção dos dados pessoais estão intimamente relacionados. Ambos se esforçam para proteger valores semelhantes, que sejam, a autonomia e a liberdade dos indivíduos, concedendo-lhes uma esfera pessoal, na qual possam desenvolver livremente suas personalidades, pensar e formar suas opiniões. Tais valores, por sua vez, são pressupostos essenciais para o exercício de outras liberdades fundamentais, como a liberdade de expressão, a liberdade de reunião e de associação pacífica, e a liberdade de religião (Conselho da Europa, 2018).

Os dois direitos se diferem em sua formulação e alcance. O direito à privacidade consiste em uma proibição geral de interferência na vida privada das pessoas, estando sujeita a

alguns critérios de interesse público, que podem justificar a interferência em certos casos. A proteção de dados pessoais, por sua vez, é vista como um direito moderno e ativo, necessário na implementação de um sistema de freios e contrapesos para proteger os indivíduos sempre que seus dados pessoais são processados. Assim, tem-se por um lado o direito "clássico" de proteção da privacidade, e por outro um direito mais "moderno", o direito à proteção de dados.

O Artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (CDF) não só afirma o direito à proteção de dados pessoais, como também especifica os valores fundamentais associados a este direito. Neste sentido, o normativo europeu prevê que o processamento de dados pessoais deve ser justo, para fins específicos, e com base no consentimento da pessoa em questão, ou em uma base legítima estabelecida por lei. Os indivíduos devem ter o direito de acesso aos seus dados pessoais e de sua retificação, e o cumprimento desse direito deve estar sujeito ao controle de uma autoridade independente (Conselho da Europa, 2018).

Segundo a concepção europeia, o direito à proteção de dados pessoais é exercido sempre que sejam tratados dados pessoais. Assim, qualquer operação de processamento de dados pessoais está sujeita à proteção adequada. Do mesmo modo, a proteção de dados diz respeito a todos os tipos de dados pessoais e de processamento de dados, independentemente do relacionamento e do impacto na privacidade. O processamento de dados pessoais também pode infringir o direito à vida privada; no entanto, não é necessário demonstrar uma violação da vida privada para que as regras de proteção de dados sejam acionadas (Conselho da Europa, 2018). O direito à privacidade, por conseguinte, diz respeito a situações em que um interesse privado – ou a "vida privada" – de um indivíduo foi comprometido. Conforme já mencionado, o conceito de "vida privada" tem sido amplamente interpretado na jurisprudência dos tribunais de direitos humanos, abrangendo situações íntimas, informações sensíveis ou confidenciais, ou que possam prejudicar a percepção do público contra um indivíduo, e até mesmo aspectos de sua vida profissional e comportamento público. No entanto, a avaliação da existência ou não de interferência na "vida privada" depende do contexto e dos fatos de cada caso.

Em contrapartida, qualquer operação que envolva o tratamento de dados pessoais pode ser abrangida pelas regras de proteção de dados, e desencadear o direito à proteção de dados pessoais. Por exemplo, quando um empregador registra informações relativas aos nomes e à remuneração paga aos empregados, o mero registro dessas informações não pode ser considerado uma interferência na vida privada. Tal interferência poderia, no entanto, ser argumentada se, por exemplo, este mesmo empregador transferisse as informações pessoais dos funcionários para terceiros. Os empregadores devem, em qualquer caso, cumprir as regras de proteção de dados, porque o registro das informações dos funcionários constitui-se em um

processamento de dados (Conselho da Europa, 2018).

No que diz respeito ao processamento de dados pessoais, realizado pelos órgãos de investigação criminal e segurança pública, a Corte de Justiça da União Europeia (CJUE)[19] já decidiu sobre limites de normativos da União Europeia, em face aos direitos à proteção de dados pessoais e respeito à vida privada, afirmados na Carta dos Direitos Fundamentais da UE. Neste sentido, a CJUE declarou inválida a Diretiva 2006/24/EC, aprovada pelo Parlamento Europeu, que exigia que os fornecedores de serviços de comunicações eletrônicas, ou das redes de comunicações públicas, retivessem os dados de telecomunicações dos cidadãos por até dois anos, para garantir que tais informações estivessem disponíveis para fins de prevenção, investigação e repressão de crimes graves. A medida referia-se apenas a metadados, dados de localização e dados necessários à identificação do assinante ou utilizador, não se aplicando ao conteúdo das comunicações eletrônicas (Corte de Justiça da União Europeia, 2014).

Já um segundo exemplo diz respeito a dois requerentes, que tinham sido acusados da prática de certos crimes, mas não tinham sido condenados. Não obstante, a polícia inglesa tinha conservado e armazenado as suas impressões digitais, perfis de ADN e amostras de células. A lei permitia a conservação dos referidos dados biométricos por tempo indeterminado, nos casos em que uma pessoa fosse uma suspeita da prática de um crime, ainda que esta fosse posteriormente absolvida ou o processo fosse arquivado. O CEDH entendeu que a conservação generalizada e indiscriminada de dados pessoais, sem qualquer limitação temporal, quando as pessoas absolvidas têm apenas possibilidades limitadas de requerer a eliminação, constituía uma ingerência desproporcional no exercício do direito dos requerentes ao respeito pela vida privada. Assim, neste caso, a CEDH concluiu que tinha havido uma violação do Artigo 8º da CEDH (Corte Europeia de Direitos Humanos, 2008).

O CJUE considerou a diretiva uma interferência no direito fundamental à proteção de dados pessoais, "porque previa o tratamento de dados pessoais"; tendo, do mesmo modo, considerado que a diretiva interferia no "direito ao respeito pela vida privada". Segundo a CJUE, os dados pessoais retidos ao abrigo da diretiva, aos quais as autoridades competentes poderiam ter acesso, poderiam, no seu conjunto, permitir às autoridades policiais

> [...] tirar conclusões muito precisas elaborados sobre a vida privada das pessoas cujos dados foram retidos, como os hábitos de a vida quotidiana, os locais de residência permanente ou temporária, os movimentos quotidianos ou outros, as atividades desenvolvidas, as relações sociais dessas pessoas e os ambientes sociais por elas

[19] O Tribunal de Justiça da União Europeia lida com questões relacionadas ao direito da UE, enquanto a Corte Europeia dos Direitos Humanos trata de casos de violações de direitos humanos, cometidas pelos Estados membros do Conselho da Europa.

frequentados.

Assim, a CJUE declarou a Diretiva 2006/24/CE inválida, por ser muito ampla. Considerou que, embora perseguisse um objetivo legítimo, a interferência nos direitos à proteção de dados pessoais e à vida privada era grave, e não se limitava ao estritamente necessário (Corte de Justiça da União Europeia, 2014).

4.5. SISTEMA DE PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DAS ATIVIDADES POLICIAIS

O sistema europeu de proteção de dados pessoais, no âmbito das atividades policiais, foi construído a partir das normas da Convenção Europeia dos Direitos Humanos, e de parâmetros interpretativos estabelecidos por algumas decisões proferidas pelo Corte Europeia de Direitos Humanos (CEDH). As regras de proteção dos dados pessoais no âmbito policial refletem o conceito de proteção à vida privada, como definido pela jurisprudência da CEDH. Neste sentido, a coleta e utilização de dados pessoais para fins de prevenção, investigação, detecção ou processamento de uma ofensa criminal, ou de execução de uma sanção penal, representa uma interferência no direito à vida privada e à proteção de dados pessoais, tal como previsto no Artigo 8º da Convenção Europeia dos Direitos do Homem. Entretanto, deve ser ressaltado que, mesmo reconhecendo explicitamente todos os direitos e liberdades estabelecidas pela Convenção, a CEDH consolidou a regra geral de que as polícias podem tratar os dados pessoais, desde que essa interferência no direito à privacidade seja baseada em lei (clara, previsível e acessível); tenha um objetivo legítimo; e se limite ao estritamente necessário e proporcional, para que este objetivo legítimo seja alcançado (Conselho da Europa, 2018).

Um sistema de proteção de dados pessoais deve impossibilitar a coleta geral e indiscriminada de dados por parte das instituições policiais, que precisam se limitar somente ao que for necessário para prevenir um perigo real, ou a repressão de um crime específico. Desse modo, o tratamento de dados pessoais pela polícia precisa possuir finalidades pré-definidas, claras e legítimas, sendo estabelecidas em normativos que regulamentem a atividade.

Ao mesmo tempo, o tratamento deve ser necessário e proporcional a essas finalidades legítimas, não podendo os dados pessoais serem utilizados de forma incompatível com essas mesmas finalidades. O processamento de dados deve ser realizado de forma legal, justa e transparente. Ao mesmo tempo, os dados pessoais dentro da polícia devem ser adequados, relevantes e não excessivos, em relação às finalidades pelas quais foram coletados. Finalmente,

devem ser precisos e atualizados, para garantir a mais alta qualidade possível dos dados (Conselho da Europa, 2018).

A base teórica dos normativos europeus sobre tratamento de dados pessoais no âmbito policial, conforme se verifica pela própria terminologia utilizada, teve origem na jurisprudência da CEDH. Neste sentido, a Diretiva da União Europeia nº 680/2016 assenta que o tratamento de dados pessoais deverá ser concebido para servir aos cidadãos, afirmando, ao mesmo tempo, que o direito à proteção de dados pessoais não é absoluto, e que deve ser considerado em conformidade com o princípio da proporcionalidade. Do mesmo modo, seguindo os princípios dispostos nas regras de proteção aos direitos humanos, os dados somente podem ser tratados para fins específicos, explícitos e legítimos, devendo as polícias dos países implementarem medidas de segurança técnicas e organizacionais adequadas aos riscos apresentados pelo tratamento de dados (União Europeia, 2016b).

A Diretiva n° 680/2016, ao criar regras mais específicas para regulamentar o tratamento de dados, para fins de pudessem harmonizar a legislação, que regulamenta o tratamento de dados pessoais para fins de prevenção, investigação, detecção ou repressão de infrações criminais, e execução de sanções penais, possui escopo significativamente mais restrito que o do Regulamento UE n° 679/2016 (RGPD). Caso os direitos à informação sobre a existência de tratamento dos dados, o acesso a estes dados e a sua retificação forem exercidos em sua máxima extensão, esses direitos podem prejudicar o trabalho da polícia e da justiça criminal. Neste sentido, a Diretiva UE n° 680/2016 busca estabelecer um claro equilíbrio entre o direito individual à proteção de dados, e os interesses e objetivos dos órgãos de persecução criminal. Do mesmo modo, deve ser levado em consideração que a Diretiva UE n° 680/2016 possui como base teórica um robusto arcabouço legal europeu sobre segurança pública e persecução criminal, que foi sendo consolidado nos países do continente ao longo dos anos, principalmente a partir de inúmeras decisões sobre o tema, tal como proferidas pela Corte Europeia de Direitos Humanos (CEDH).

Pode-se afirmar que não existe nenhum aspecto da atividade de segurança pública dos países membros que não tenha sido submetido, de alguma forma, aos padrões europeus de respeito aos direitos humanos. Tem-se vista que a grande maioria dos casos apresentados perante a CEDH estão relacionados a investigações e processamento de crimes perante a Justiça dos países signatários da Convenção Europeia dos Direitos Humanos. Por isso, a Diretiva UE n° 680/2016 se utiliza de conceitos que primeiramente surgiram em decisões da CEDH, tais como as condições de limitação ao direito à privacidade, que é prevista no Artigo 8º da Convenção Europeia.

O conceito de “necessidade em uma sociedade democrática” é mencionado inúmeras vezes na Diretiva UE n° 680/2016, como nos dispositivos que limitam os direitos dos titulares à informação, acesso ou retificação quanto ao tratamento de seus dados pessoais pelos órgãos de segurança pública. Segundo os referidos dispositivos, os Estados-Membros podem adotar restrições legislativas aos direitos dos titulares dos dados pessoais, quando quanto tais medidas sejam “necessárias e proporcionais em uma sociedade democrática”, e tenham por finalidade: i) evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais; ii) evitar prejudicar a prevenção, detecção, investigação ou repressão de infrações penais, ou a execução de sanções penais; iii) proteger a segurança pública e a segurança nacional; e iv) proteger os direitos e as liberdades de terceiros.

Todo sistema de banco de dados policial deve partir de uma classificação detalhada dos diferentes tipos de dados pessoais, que são armazenados pelas instituições policiais, com o escalonamento dos níveis de proteção de acordo com as características específicas de cada elemento informacional coletado. Por sua vez, a necessidade de se atribuírem medidas protetivas de forma escalonada, e de acordo com o nível de proteção exigido para os diferentes tipos de dados e informações pessoais tratadas, constitui-se uma das principais dificuldades para a estruturação de normas de sistemas de organização do conhecimento policial..

Neste sentido, os princípios e regras de tratamento de dados no âmbito policial são estabelecidos a partir da divisão da classe “dado pessoal” em suas respectivas subclasses, tais como “dado pessoal sensível” e “dado pessoal sigiloso”. Ao mesmo tempo, a classe “dados pessoais” pode ser também classificada de acordo com as diferentes categorias de titulares de dados. Dentre as classes de pessoas que se encontram em torno dos fatos criminosos, e que podem ter os seus dados tratados pelas polícias estão, especialmente, as pessoas suspeitas de terem praticado um crime, pessoas contra as quais existam existem indícios suficientes de que estão prestes a cometer uma infração penal, pessoas processadas judicialmente, pessoas condenadas definitivamente, vítimas e testemunhas (União Europeia, 2016b).

Em alguns casos, entretanto, a diferença entre os diversos tipos de dados ocorre não pelo dado em si, mas sim em razão o tipo de tratamento ao qual ele é submetido. Neste sentido, a classificação do tipo de tratamento se dará de acordo com a finalidade buscada pelo usuário policial. Por exemplo, uma base de dados formada pelo acervo de investigações de uma instituição policial pode ser consultada/tratada por diferentes propósitos, tais como a realização de uma avaliação estratégica, para a definição das principais modalidades criminosas existentes em uma área específica; a elaboração de avaliações táticas, visando a definição de alvos prioritários em um estratégia de enfrentamento a um tipo de crime; o mapeamento de redes de

relacionamento entre criminosos, visando a definição de uma estratégia de investigação; e até mesmo para a elaboração de perfis detalhados de suspeito(s) ou vítima(s). Nestes casos, como não é possível separar os diferentes tipos de dados pessoais reunidos em um conjunto de investigações criminais, torna-se necessário a definição de níveis de controle de acesso dos usuários à base de dados, conforme a finalidade do tratamento a ser realizado.

De qualquer forma, o tratamento de dados pessoais no âmbito policial deve estar condicionado pela promoção efetiva da segurança pública, enquanto bem coletivo, e na sua compatibilização com os direitos humanos. O respeito às liberdades individuais deve ser inserido no cálculo de maximização do bem-estar social a ser produzido pelas instituições estatais, responsáveis pelas investigações criminais e pela prevenção do crime.

Por sua vez, os desafios que se apresentam ao tratamento de dados pessoais têm como ponto central verificar se as técnicas e metodologias adotadas pelos órgãos de segurança pública são justificadas, efetivamente, pelos benefícios sociais que afirmam buscar. Torna-se cada vez mais necessária a criação de sistemas de tratamento de dados pessoais no âmbito policial, a partir da análise de modelos já existentes. Qualquer projeto a ser desenvolvido pelas polícias deve buscar a manutenção do equilíbrio entre a necessidade do Estado de garantir a segurança e de proteger, ao mesmo tempo, o direito à privacidade dos seus cidadãos.

4.5.1. Controle por tipo de dado

Os dados pessoais que geralmente são processados pelas polícias incluem nome, data e local de nascimento, nacionalidade, sexo, local de residência, profissão, localização, números de previdência social, licenças de motorista, documentos de identificação e dados de passaporte. Do mesmo modo, quando for necessário, podem ser objeto de tratamento de dados outras características pessoais, que possam auxiliar na identificação do suspeito, incluindo quaisquer características físicas objetivas específicas e que não estejam sujeitas a alterações, como dados dactiloscópicos e perfil de DNA. Por fim, também podem ser armazenadas, as informações relacionadas aos crimes praticados pela pessoa, condenações anteriores e passagens pelo sistema prisional (Europol, 2023).

Segundo a Diretiva UE n° 680/2016, no desenvolvimento de seus bancos de dados, os órgãos policiais devem promover uma distinção clara entre os dados pessoais de diferentes categorias, de acordo com a natureza dos respectivos titulares dos dados, tais como:

a) Pessoas relativamente às quais existem motivos fundados para se crer que cometeram, ou que estão prestes a cometer uma infração penal;

b) Pessoas condenadas por uma infração penal;
c) Vítimas de uma infração penal, ou pessoas contra as quais existam fatos que levam a crer que possam vir a ser vítimas de uma infração penal; e,
d) Outras pessoas relacionadas a uma infração criminal.

Podem ser considerados terceiros relacionados ao crime as pessoas que possam ser chamadas a testemunhar em investigações criminais ou em processos penais subsequentes, e pessoas que possam fornecer informações sobre infrações penais, contatos ou associados aos investigados, suspeitos ou condenados da prática de crimes. Do mesmo modo, tais bancos de dados devem distinguir, na medida do possível, os dados pessoais baseados em fatos dos dados pessoais baseados em apreciações pessoais (União Europeia, 2016c).

Para realizar o tratamento de dados pessoais, os órgãos policiais podem utilizar tanto bancos de dados próprios, como de outras organizações públicas ou privadas, mediante convênios ou acordos de compartilhamento. Por sua vez, a crescente quantidade de dados pessoais controlados por diversos organismos públicos e entidades privadas, e que são coletados e armazenados pelas polícias, pode levar a graves vulnerabilidades e risco subsequente de violação dos direitos dos titulares dos dados, caso a segurança da informação não seja garantida (Conselho da Europa, 2018).

O processamento de diversas bases de dados pode ajudar as polícias a detectarem ou o esclarecerem crimes, mas existem riscos consideráveis neste tipo de processamento de dados, que devem ser levados em consideração. Por exemplo, bases de dados originárias de um domínio podem ser utilizadas em outro, e para outra finalidade, o que altera o contexto e pode levar a conclusões imprecisas, causando possíveis consequências graves para os indivíduos envolvidos. Do mesmo modo, a criação de bancos de dados policiais pode levar à criação de perfis e conclusões discriminatórias, resultando no reforço de estereótipos, estigmatização e discriminação (Conselho da Europa, 2018).

Segundo a Diretiva UE n° 680/2016, os dados pessoais recolhidos pelas autoridades policiais competentes, para os fins de prevenção, investigação e detecção ou repressão de crimes, não podem ser tratados para fins diferentes, a não ser que esse outro tratamento seja também autorizado por lei. No âmbito europeu, o intercâmbio de dados pessoais entre organizações públicas, caso esteja previsto pelo ordenamento jurídico do país membro, não dever ser limitado nem proibido por razões relacionadas com a proteção das pessoas singulares. O que se exige é que a integridade e precisão de todo material recolhido deva ser garantida, com a criação de arquivos organizados de um modo que permita a acessibilidade e uso otimizado dos registros e dados obtidos (União Europeia, 2016c).

Como as necessidades e circunstâncias de processamento de dados pessoais não podem ser previstas em detalhes, a relação entre normas de tratamento de dados no âmbito policial e o tratamento de dados pessoais, de modo geral, torna-se bastante relevante. Em particular, pode haver casos em que as autoridades relacionadas com a segurança pública realizem formas de tratamento de dados pessoais que se enquadram no âmbito das leis gerais de proteção de dados. Do mesmo modo, o oposto também pode ser verdadeiro: as agências que normalmente realizam o processamento de dados pessoais, para fins gerais, podem se ver envolvidas no tratamento de dados para fins de investigação criminal e segurança pública. Para o efeito dessa relação entre os dois sistemas de proteção de dados, a Diretiva UE n° 680/2016 fornece algumas orientações úteis. Este normativo europeu esclarece, por exemplo, que quando os dados são inicialmente recolhidos por uma autoridade competente com finalidades de segurança pública, mas passem a serem utilizados para outras finalidades alheias às atividades policiais, o Regulamento Geral de Proteção de Dados (Regulamento UE n° 679/2016) deve ser aplicado ao tratamento dos dados também para essas outras finalidades (Hert; Papakonstantinou, 2016).

Na abordagem sobre os dados tratados pelas polícias, também merece destaque a classificação relacionada aos dados pessoais considerados "sensíveis"[20]. Esta categoria de dados pessoais possui uma natureza especial, em razão dos riscos que o tratamento dos mesmos pode representar aos direitos e liberdades fundamentais do titular dos dados, nomeadamente o risco de discriminação (Europol, 2023). No âmbito europeu, a consulta a dados genéticos, dados pessoais relacionados com infrações, processos e condenações penais, e quaisquer medidas de segurança conexas, dados biométricos que identifiquem de forma única uma pessoa, bem como quaisquer dados pessoais sensíveis, só pode ser permitida se existirem garantias adequadas de proteção aos seus titulares. Do mesmo modo, o tratamento de dados pessoais sensíveis deve se destinar a proteger os interesses vitais do titular dos dados ou de outras pessoas, mesmo nos casos em que tenham sido manifestamente tornados públicos pelo próprio sujeito a que se referem (União Europeia, 2016b).

De acordo com a Diretiva UE n° 680/2016, devem ser definidos como dados genéticos todos os dados pessoais relacionados com as características genéticas, hereditárias ou adquiridas de uma pessoa. Tais dados geram informações únicas sobre a fisionomia ou a saúde

[20] No âmbito nacional, a LGPD considera sensíveis os dados pessoais sobre a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, bem como os dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos, quando vinculado a uma pessoa natural.

do indivíduo, resultantes, designadamente, da análise cromossômica do ácido desoxirribonucleico (ADN) e do ácido ribonucleico (ARN), ou de qualquer outro elemento que permita obter informações equivalentes. Segundo a norma europeia, em razão da complexidade e da natureza sensível das informações genéticas, existe um elevado risco de sua utilização injustificada e de reutilização para diversos fins não autorizados. Assim, qualquer tratamento de dados pessoais pelas polícias, que envolva discriminações com base em características genéticas, deverá ser proibido (União Europeia, 2016b).

Do mesmo modo, no âmbito europeu, são consideradas sensíveis quaisquer informações sobre uma doença, deficiência, risco de doença, histórico clínico, tratamento clínico, ou estado fisiológico ou biomédico atual do titular dos dados. A proteção dos dados relativos à saúde deve ocorrer independentemente da sua fonte, podendo ser oriunda de um médico ou outro profissional de saúde, ou um hospital. Por sua vez, deverão ser considerados dados pessoais relativos à saúde todos os dados que revelem informações sobre a saúde física ou mental no passado, no presente ou no futuro. Segundo a Diretiva UE n° 680/2016, tal definição abrange informações sobre a pessoa singular, recolhidas durante a sua inscrição para a prestação de serviços de saúde e durante essa prestação. Do mesmo modo, qualquer número das informações obtidas a partir de análises ou exames de uma parte do corpo, ou de substância corporal (União Europeia, 2016b).

A Diretiva UE n° 680/2016 considera necessário que as autoridades competentes tratem os dados pessoais recolhidos no contexto de ações policiais de prevenção e investigação de infrações penais específicas, para além de um contexto isolado. Com uma análise ampliada é possível obter uma melhor compreensão das atividades criminais de um grupo criminoso ou determinada região, estabelecendo ligações entre as diferentes infrações penais detectadas. Do mesmo modo, o Regulamento da Europol considera que o conjunto de informações sobre crimes oferece um enorme potencial para se desenvolver a compreensão dos fenômenos e tendências criminais, recolhendo informações sobre redes criminosas para detectar ligações entre diferentes infrações penais (Regulamento UE n° 794/2016, Art. 17.º, § 2; União Europeia, 2016c). Assim, de acordos com os princípios do sistema de proteção de dados da União Europeia, todas as informações relacionadas a crimes podem ser armazenadas e consultadas pelas polícias de forma integrada.

Entretanto, segundo a mesma Diretiva, os dados pessoais coletados e reunidos, no âmbito de investigações criminais, deverão ser tratados de uma forma que garanta um nível adequado de segurança e confidencialidade, para evitar o acesso ou a utilização desses dados e do equipamento o qual gerou o tratamento, por parte de pessoas não autorizadas. Do mesmo

modo, todo banco de dados a ser criado pelas polícias deve levar em consideração as técnicas e tecnologias mais avançadas, os custos da sua aplicação em função dos riscos, e a natureza dos dados pessoais a proteger (recomendações n^{os}26 e 27; União Europeia 2016a).

Em âmbito nacional, tanto o Código de Processo Penal como a Lei n° 12.830/2013 e Lei n° 12.850/13 permitem que as autoridades policiais (delegados de polícia) requisitem dados pessoais que interessem à investigação ou detecção de crimes. Com base neste poder estatal de produzir informações sobre crimes, as polícias utilizam recursos tecnológicos cada vez mais avançados para a coleta, registro, análise, recuperação e uso seguro de dados pessoais, de pessoas de interesse para a investigação. Somente a criação de sistemas informatizados permite que as polícias, durante o processo de pesquisa e análise, tenham acesso automatizado a meios de armazenamento, recuperação e comparação de dados.

Neste ponto, deve ser destacado que os dados pessoais classificados como sigilosos, ou seja, sujeitos à reserva de jurisdição, somente podem ser obtidos pelas polícias mediante decisão judicial. A Constituição Federal faz uma distinção entre os dados pessoais que podem ser obtidos diretamente pelos órgãos de investigação criminal, junto aos controladores dos dados de interesse, e os dados pessoais que são fornecidas apenas por meio do Poder Judiciário. Segundo a Constituição, somente um juiz teria a legitimidade necessária para permitir que o Estado tenha acesso, para fins de investigação criminal, a registros de comunicações telefônicas ou de movimentações financeiras. Para a concretização dessas medidas, também existem leis específicas regulamentando os meios especiais de produção de provas, como o afastamento do sigilo das interceptações telefônicas e do sigilo de dados bancários.

Por sua vez, em relação ao conhecimento acumulado pelas polícias ao longo do tempo, através de inquéritos policiais individualizados, devem ser adotadas medidas adequadas para conferir um adequado nível de proteção aos dados sigilosos. Neste caso, seria proibido armazenamento e utilização de tais para finalidades diversas daquelas que foram definidas pelo juiz, geralmente relacionadas a análises e cruzamento para a obtenção de evidências em uma investigação específica. A utilização de tais dados para fins de análises criminais estratégicas, por exemplo, somente poderia ocorrer a partir de uma nova decisão do Poder Judiciário, pois este seria o verdadeiro controlador dos dados sigilosos protegidos por garantias constitucionais.

4.5.2. Controle por tipo de tratamento

Neste sentido, verifica-se que o sistema de proteção dos dados pessoais da União Europeia, por meio da Diretiva UE n° 680/2016, estabelece a exigência de que os países

membros do bloco adotem regras específicas regulamentando o tratamento de dados pessoais pelas polícias e demais órgãos do sistema de segurança pública. O regulamento se aplica tanto no exercício de ações de investigação criminal, quanto em atividades de prevenção e detecção de crimes. Pelas regras estabelecidas, podem ter seus dados tratados em sistemas policiais e serem objeto de pesquisa ou verificação cruzada (*cross-checking*) em bancos de dados policiais os seguintes tipos de pessoas: i) pessoas relativamente às quais existem motivos fundados para crer que cometeram, ou que estão prestes a cometer uma infração penal; ii) pessoas condenadas por uma infração penal; iii) vítimas de uma infração penal, ou pessoas contra as quais existam fatos que levam a crer que possam vir a ser vítimas de uma infração penal; iv) outras pessoas relacionadas a uma infração criminal, como associados aos suspeitos, testemunhas, peritos, ou qualquer um que se encontre em torno do fato. Do mesmo modo, segundo o Regulamento da Europol, a verificação cruzada é possível para as pessoas em relação às quais existam indicações objetivas, ou motivos razoáveis, para se acreditar que irão cometer ofensas criminais futuras (Europol, 2023).

Por sua vez, as polícias devem ser capazes de detectar relações entre investigações e grupos criminosos, analisando dados criminais para identificar áreas de maior concentração de atividade ilícitas, principais modalidades ilícitas, criminosos mais prolíficos, e novas tendências criminais. Para melhorar a eficácia da Europol, no fornecimento de análises criminais precisas, o Regulamento da Europol determina que a organização deve utilizar novas tecnologias para processar dados e ser capaz de detectar rapidamente as ligações entre investigações. Através do cruzamento de dados é possível identificar casos com *modus operandi* comuns, sendo possível, por exemplo, estabelecer relações entre diferentes grupos criminosos ou obter uma visão clara das novas tendências criminais. Por conseguinte, as bases de dados da Europol devem ser estruturadas de forma a permitir a escolha da estrutura de informática mais eficiente (União Europeia, 2016c).

Entretanto, deve-se garantir simultaneamente um elevado nível de proteção dos dados pessoais das pessoas singulares. Desse modo, um elemento central do sistema de análise criminal da Europol é a introdução de um conceito de gerenciamento integrado de dados (IDMC), com a adoção de sistemas e operações de processamento com propósitos definidos, que podem ser implementados de maneira tecnologicamente neutra. O conceito é baseado em princípios gerais de proteção de dados e salvaguardas especificamente definidas, como prazos para armazenamento de informações, consulta prévia e implementação de proteção de dados por *design* (*privacy by design*), bem como requisitos de registro e documentação. A gestão integrada de dados pode ser definida como a possibilidade de utilizar a informação relacionada

com o crime para múltiplos fins, conforme indicado pelo titular dos dados, permitindo a sua gestão e tratamento de forma integrada e tecnologicamente neutra. Nisso se difere de estruturas legais anteriores, que eram centradas no sistema em termos de processamento geral de dados (Europol, 2023).

Ainda segundo o Regulamento da Europol, entende-se por tratamento de dados pessoais para fins de análise estratégica todos os métodos e técnicas através dos quais a informação é recolhida, armazenada, tratada e avaliada, com o objetivo de desenvolver ou apoiar uma estratégia de enfrentamento a determinada modalidade criminosa (Europol, 2023). Por sua vez, o modo de enfrentar uma ameaça criminal pode abordar diversos aspectos, tais como a coleta e gestão de dados sobre organizações criminosas, a adoção de medidas visando a redução de oportunidades para o cometimento de atos delituosos, interrupção de cadeias comerciais ilícitas, a identificação e a compreensão dos fluxos financeiros ilegais, ajustes legislativos, dentre outras atividades. As análises estratégicas de controle da criminalidade são materializadas por meio da análise de grande quantidade de dados, com o uso de mecanismos de computação específicos e técnicas modernas de gestão do conhecimento (União Europeia, 2016c).

A análise estratégica visa gerar uma melhor compreensão do crime e das tendências criminais em geral. Do mesmo modo, permite que decisões em nível estratégico possam influenciar a adoção de medidas específicas, tais como ajustes legislativos, treinamentos e capacitações para melhorar as investigações, bem como medidas preventivas e de conscientização. A análise criminal estratégica também pode indicar em quais pontos uma análise concreta é recomendada, no sentido de especificar melhor como abordar os problemas a partir de uma perspectiva operacional. Neste sentido, o tratamento de dados pessoais, para fins de análise criminal estratégica, engloba todos os métodos e técnicas pelas quais a informação é recolhida, armazenada, processada e avaliada, com o objetivo de determinar o foco operacional, e as táticas e métodos mais adequados para prevenir, interromper e investigar determinada modalidade criminosa (Europol, 2023).

Ainda que as análises estratégicas possam fazer uso de dados pessoais mais relevantes, o objetivo não é focar em infrações penais concretas. Antes, busca-se entender um determinado fenômeno criminal, com as indicações dos principais fatores, atores e facilitadores, a fim de indicar onde direcionar os recursos investigativos, e como lidar com o problema de forma mais eficaz. Estes estudos buscam orientar decisões sobre a priorização ou o início de investigações criminais ou outras ações operacionais. Assim, embora dados pessoais possam ser usados para processamento para fins de análise estratégica, os resultados apresentados geralmente não

contêm referências a titulares de dados concretos (Europol, 2023).

Já o objetivo das análises operacionais ou táticas seria o de apoiar investigações criminais, por meio de métodos e técnicas pelas quais as informações são coletadas, armazenadas, processadas e avaliadas. Do ponto de vista do sistema europeu de proteção de dados, esta é a operação de processamento mais eficiente, mas também a mais intrusiva, e por isso, devem ser aplicadas as salvaguardas de proteção de dados mais robustas. As análises operacionais podem ser realizadas em face de suspeitos, pessoas condenadas e potenciais futuros criminosos, bem como, caso considerado necessário, em relação aos seus contatos e associados. Do mesmo modo, apenas quando for estritamente necessário e proporcional, também podem ser inclusos dados pessoais relativos a testemunhas, vítimas, informantes e menores de idade (Europol, 2023).

A Diretiva EU n° 680/2016 da União Europeia proíbe o tratamento de dados pessoais, por meios automatizados ou manuais, que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical do indivíduo, bem como o tratamento de dados genéticos, ou relativos à saúde ou à vida sexual de uma pessoa, salvo se for estritamente necessário para prevenir ou combater o crime. Da mesma forma, a seleção de um determinado grupo de pessoas, apenas com base nesses dados pessoais, não é permitida (União Europeia, 2016b). Por isso, essas operações de processamento de dados mais intrusivas, com foco em indivíduos pré-determinados, só podem ser realizadas sob estrito controle de órgãos de supervisão e controle das ações policiais.

No âmbito da Europol, por exemplo, análises criminais operacionais somente são realizadas com a aprovação do Diretor Executivo, que define a sua finalidade específica, as categorias de dados pessoais coletados, participantes, duração do armazenamento, condições de acesso, transferência e utilização dos dados em análise. Todos esses parâmetros são estabelecidos em protocolos de projetos de análise operacionais específicos, os quais devem apresentar uma tabela com a categorias de dados nomeadamente definidos. Assim, dados pessoais só podem ser coletados e processados para um projeto de análise operacional especificado. Do mesmo modo, somente pessoas devidamente autorizadas podem acessar e processar os dados de cada projeto de análise (União Europeia, 2016c).

Outro ponto importante a ser destacado na Diretiva UE n° 680/2016 é a proibição que decisões estratégicas, ou mesmo operacionais, sejam tomadas exclusivamente com base no tratamento automatizado de dados; incluindo a definição de perfis que possam produzir efeitos adversos na esfera jurídica do titular dos dados, ou que o afetem de forma significativa, a menos que sejam autorizadas por lei específica. De todo modo, qualquer lei que autorize que polícias

utilizem de sistemas automatizados de tomada de decisão, deverá estabelecer garantias adequadas aos direitos e liberdades do titular dos dados, pelo menos o direito de obter a intervenção humana do responsável pelo tratamento. Pelas normas da União Europeia, são terminantemente proibidas as definições de perfis que conduzam à discriminação de pessoas singulares com base em informações consideradas sensíveis (União Europeia, 2016c).

Para que uma análise estratégica ou operacional seja eficiente, os dados coletados e arquivados devem ser verificados minuciosamente, seguindo o princípio de que somente informações de alta qualidade geram análises de alta qualidade. As polícias necessitam manipular grandes volumes de dados, para fins de suporte à gestão do crime ou da predição de cenários criminais, com a utilização crescente de informação não estruturada, principalmente de cunho textual. Destarte, os órgãos policiais e demais autoridades devem confiar que as informações fornecidas para uma análise sejam corretas e válidas, com o processamento somente de dados precisos e atualizados. Após uma verificação inicial, ao se inserirem os dados, revisões regulares devem ocorrer, garantindo que os dados continuem a cumprir os requisitos de conformidade geral (União Europeia, 2016c).

Por sua vez, em atenção ao direito fundamental à proteção dos dados pessoais, a Diretiva UE n° 680/2016 estabelece que não se devem conservar dados pessoais por um período superior ao estritamente necessário para o desempenho das funções para a qual foi coletado. Assim, a necessidade de armazenamento continuado de tais dados deve ser revista no prazo máximo de três anos após o início de seu processamento inicial. Do mesmo modo, verificações regulares de conformidade, com o objetivo de conferir a legalidade do processamento de dados, bem como de garantir a integridade e segurança adequadas dos dados, são medidas essenciais de promoção dos mais altos padrões de proteção de dados (União Europeia, 2016c).

5. RESULTADOS

Após analisar os padrões normativos internacionais de proteção e salvaguarda de direitos no tratamento de dados pessoais por organizações policiais, com ênfase nos dispositivos da Diretiva UE nº 680/2016 e no Regulamento UE nº 794/2016 (Regulamento Europol – RE), torna-se necessária a sistematização dos princípios e regras que devem nortear as operações de tratamento de dados pessoais para fins de prevenção, investigação, detecção ou repressão de infrações penais. Tais princípios e regras tem por objetivo criar parâmetros para o desenvolvimento de medidas a serem observadas desde o estágio inicial do desenvolvimento de qualquer sistema de organização do conhecimento no âmbito policial, bem como na elaboração de avaliações do impacto de operações de tratamento de dados pessoais criadas a partir de novas tecnologias adotadas pelas polícias. Do mesmo modo, a referida sistematização pode orientar a adoção de medidas técnicas e organizativas, que garantam níveis satisfatórios de proteção dos direitos e garantias dos titulares dos dados pessoais no âmbito policial.

De acordo com o subitem 2.4 desta dissertação, os objetivos específicos da presente pesquisa consistem em:

a) Analisar os padrões normativos internacionais de proteção e salvaguarda de direitos no tratamento de dados pessoais, realizados por organizações policiais, com ênfase nos dispositivos da Diretiva UE nº 680/2016 e no Regulamento UE nº 794/2016 (Regulamento Europol – RE);
b) Analisar as salvaguardas e mecanismos de mitigação de risco de violação dos direitos dos titulares dos dados;
c) Classificar os tipos de dados pessoais que são produzidos ou coletados pelas polícias;
d) Classificar as categorias de tratamento de dados pessoais realizadas pelos órgãos de segurança pública;
e) Sistematizar, em forma de tabelas, os princípios e normas relacionadas à proteção e à garantia dos direitos e liberdades individuais dos titulares de dados.

O primeiro e segundo objetivos específicos indicados foram apresentados no decorrer do Capítulo 3, destinado ao processo de análise documental e à aplicação do referencial teórico da pesquisa. Por sua vez, esta seção inclui os resultados referentes ao terceiro, quarto e quinto objetivos específicos.

5.1. SISTEMATIZAÇÃO DOS PRINCÍPIOS E NORMAS DE PROTEÇÃO DE DADOS

PESSOAIS NO ÂMBITO DAS ATIVIDADES POLICIAIS

Para a facilitar a apresentação de tal resultado, com a disposição em tabelas estruturadas dos princípios e regras que devem nortear os sistemas nacionais de tratamento de dados pessoais na atividade policial, foram utilizados os referenciais da teoria sistêmica da Ciência da Informação (Araújo, 2018, p. 22-23). Sob o aspecto das diversas teorias sobre os sistemas de informação, pode-se dizer que as atividades de coleta, registro, armazenamento, análise, recuperação e uso seguro da informação, de interesse dos órgãos de segurança pública podem ser relacionadas com a teoria sistêmica da CI.

Partindo de princípios que podem ser utilizados como uma espécie de método no estudo de qualquer fenômeno, esta teoria parte da visão de que o todo de um sistema é maior do que as partes. Por sua vez, as partes devem ser estudadas, necessariamente, a partir da função que desempenham para a manutenção e sobrevivência do todo. Desse modo, a lógica sistêmica privilegia a ideia de ciclo, de circularidade, tendo em vista que todo processo sempre representa a saída de alguma entidade, ou *output*. Por sua vez, essa saída vai provocar a formação de novos elementos de entrada, expresso no conceito de *input* (Araújo, 2018).

Desse modo, o modelo da teoria sistêmica articula uma série de conceitos particulares, tais como a ideia de totalidade (o conjunto, como por exemplo em um sistema de organização do conhecimento geral de uma determinada instituição policial, uma delegacia, uma equipe); os objetos que compõem a totalidade (o acervo de investigações, sistemas de bancos de dados, registros de ocorrência, bancos de fotografias, impressões digitais, DNA, dentre outros itens de dados reunidos pela polícia); os atributos destes objetos (características específicas que cada objeto tem para o desempenho adequado da sua função); os processos (entendido como as tarefas necessárias para a sobrevivência do próprio sistema); e o ambiente (aquilo que é externo à totalidade, de onde ela retira os elementos de entrada, e para onde dirige os elementos de saída). Assim, pelo enfoque sistemista, o tratamento de dados em um sistema de informação deve ser pensados a partir da lógica dos processos de entrada (entrada de dados, com a aquisição de itens informacionais, a seleção destes itens para a composição de determinado acervo); de processamento (os itens informacionais que dão entrada num sistema de informação precisam ser descritos, catalogados, classificados, indexados); e de saída (pelo acesso aos itens informacionais por parte dos usuários, na forma de disseminação, entrega da informação etc.) (Araújo, 2014).

Outra abordagem inerente à teoria sistêmica da CI consiste no entendimento de que os sistemas precisam ser estáveis. Em outros termos, deve-se manter uma determinada dinâmica

de funcionamento, com controle do que entra e do que sai, sempre com a ideia de que os bancos de dados são organismos em crescimento. Entretanto, a necessidade de manter a sua estabilidade faz com que um sistema de informação não possa ir crescendo e adquirindo novos itens informacionais infinitamente. Então, os sistemas de informação precisam promover desbastes, descartes, como forma de manter um equilíbrio e continuar cumprindo suas funções (Araújo, 2014).

Interessante notar, neste ponto, que o processo de saída da visão sistemista se coadunaria com o entendimento consolidado pelas decisões da Corte Europeia de Direitos Humanos que estabeleceram o princípio da limitação temporal do armazenamento de dados pessoais, conforme já mencionado neste trabalho (subseção 4.4.4). Este princípio vetaria a conservação generalizada e indiscriminada de dados pessoais sem qualquer limitação temporal, constituindo uma ingerência desproporcional ao direito do respeito à vida privada. Assim, deve-se evitar a adoção de modelos em que os titulares de dados têm apenas possibilidades limitadas de requerer a eliminação de suas informações dos sistemas policiais (Corte Europeia de Direitos Humanos, 2008).

Por sua vez, os resultados a serem produzidos pela atividade policial de tratamento de dados pessoais podem ser medidos pelo impacto calculado em termos de redução do crime, prisões, interrupções e maior segurança da comunidade. Com isto, a atuação policial orientada pela informação também se relaciona, de certa forma, com a segunda grande manifestação da teoria sistêmica da CI, que busca levar em consideração a função da informação na sociedade. Para tanto, cada sistema de análise de dados pessoais deve ser analisado pelo enfoque da promoção da segurança coletiva, sendo necessário buscar o adequado balanceamento entre as medidas de tratamento de dados pessoais, e o respeito aos direitos individuais de cada um dos seus membros (Araújo, 2014).

Assim, visando a sistematização dos princípios que devem nortear sistemas nacionais de tratamento de dados pessoais na atividade policial, relacionados à proteção e garantia dos direitos dos titulares de dados, foram elaboradas tabelas indicando a vinculação dos princípios e normas às respectivas fases do rastreamento de dados, conforme conceitos extraídos da teoria sistêmica da CI. Nos Quadros 1 a 3 a seguir, são apresentados os princípios referentes a cada fase de processamento no tratamento de dados, ou seja: i) entrada; ii) processamento; e iii) saída.

Quadro 1 – Princípios do processo de entrada (entrada de dados, aquisição de itens informacionais, e a seleção de itens para a composição de determinado acervo).

Art. 4º da Diretiva UE nº 680/2016	**Conteúdo**
Princípio da finalidade	Os dados devem ser recolhidos para finalidades determinadas, explícitas e legítimas.
Princípio da qualidade dos dados	Os dados devem ser adequados, pertinentes e limitados ao mínimo necessário, relativamente às finalidades para as quais são tratados.
Princípio da exatidão	Os dados devem ser exatos e atualizados sempre que necessário.
Princípio da utilidade pública	Os dados podem ser tratados para fins de interesse público e a utilização científica, estatística ou histórica, sob reserva de garantias adequadas dos direitos e liberdades do titular dos dados.
Art. 28º do Regulamento Europol	**Conteúdo**
Princípio da finalidade	Os dados devem ser coletados para finalidades determinadas, explícitas e legítimas, e não são tratados ulteriormente de forma incompatível com essas finalidades. O tratamento ulterior, para fins cronológicos, estatísticos ou de investigação científica, não é considerado incompatível, desde que sejam estabelecidas as garantias adequadas, em especial para assegurar que os dados só sejam tratados para essas novas finalidades.
Princípio da adequação ou necessidade	Os dados coletados devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para que são tratados.

Fonte: Adaptado pelo autor a partir da Diretiva UE nº. 680/2016.

Os princípios mencionados e resumidos no Quadro 1 (entrada) desempenham um papel fundamental na construção de projetos de sistemas informatizados de informação policial. O princípio da finalidade, previsto tanto na Diretiva UE nº. 680/2016, quanto no Regulamento da Europol, estabelecem que, desde a fase inicial do planejamento e elaboração do *design,* devem ser definidos objetivos do sistema de informação policial, com a identificação das finalidades específicas para as quais os dados serão coletados e usados, de modo a garantir que o sistema tenha um foco claro e legítimo. Pelo enfoque da teoria sistêmica, o objetivo do sistema direciona a entrada de informações relevantes para atingir esse objetivo. Em um sistema de informação policial, o objetivo deve estar relacionado à prevenção, investigação, detecção ou repressão de infrações criminais, e execução de sanções penais. Portanto, o *input* de dados deve

estar alinhado com esses objetivos específicos.

Já o princípio da qualidade dos dados é crucial para a precisão e confiabilidade do sistema. Na teoria sistêmica, isso se relaciona com a ideia de que a entrada de dados deve ser precisa e de alta qualidade, para garantir que as informações sejam úteis e confiáveis. Dados imprecisos ou de baixa qualidade podem levar a saídas (*outputs*) problemáticas, e a prejudicar o funcionamento do sistema. Assim, devem ser estabelecidos protocolos de qualidade de dados que incluam a verificação da precisão e da integridade das informações, bem como a implementação de procedimentos de atualização regular, para manter os dados sempre precisos. Garantir a qualidade dos dados é fundamental em sistemas de informação policial, pois informações imprecisas podem levar a investigações equivocadas, detenções injustas e erros judiciais. Portanto, a construção do sistema deve incluir medidas robustas para manter a integridade e a qualidade dos dados ao longo do tempo.

O princípio da qualidade dos dados se relaciona, de certa forma, com o princípio da exatidão, que estabelece que os dados devem ser exatos e atualizados sempre que necessário. Esse princípio estaria relacionado com o estabelecimento de verificações automáticas de integridade de dados e validações, com a implementação de um sistema de controle que monitorasse continuamente a exatidão das informações nele armazenadas. Isso implicaria em uma estratégia de atualização de dados regular, identificando quais informações precisam ser atualizadas e quando. Da mesma forma, os administradores e usuários do sistema devem possuir as ferramentas e recursos para relatar e corrigir quaisquer erros ou imprecisões de dados, que encontrem durante o uso do sistema. Os usuários devem ser treinados sobre a importância da exatidão dos dados, e incentivados a uma cultura de responsabilidade em relação à precisão e atualização das informações inseridas no sistema.

O princípio da utilidade pública se relaciona à capacidade do sistema de informação policial contribuir para o bem-estar público ou outros fins de segurança pública. Neste caso, um sistema de informação policial deve proporcionar o tratamento de dados somente para fins de interesse público, como a prevenção, investigação, detecção ou repressão de infrações criminais, e execução de sanções penais. Entretanto, deve ser reconhecido que os sistemas de informação podem ter impactos e utilidade além de suas funções principais, como estudos estatísticos, elaboração de políticas públicas ou pesquisa científica. De qualquer forma, todos os diferentes usos dos dados devem estar relacionados com o bem público e o interesse coletivo, com a adoção de regulamentados para garantir a proteção dos dados pessoais e a utilidade do sistema.

Por fim, o princípio da adequação (ou necessidade), como previsto no Regulamento

da Europol, está relacionado à noção de eficiência em um sistema de informação. Isso se alinha, na teoria sistêmica, com o conceito de otimização de recursos, garantindo que estes – no caso, os dados – sejam usados de maneira eficiente e relevante para o funcionamento do sistema. Assim, ao projetar ou descrever o banco de dados do sistema, devem ser selecionados cuidadosamente os tipos de dados a serem coletados, garantindo que sejam adequados e relevantes para atender às necessidades da atividade policial. Neste caso, devem ser implementados mecanismos de validação da entrada de dados, para garantir que apenas informações pertinentes e úteis sejam inseridas no sistema e, ao mesmo tempo, evitar a sobrecarga de dados não essenciais.

Quadro 2 – Princípios do processamento (descrição, classificação, indexação e tratamento de dados).

Art. 4 da Diretiva UE nº 680/2016	**Conteúdo**
Princípio da legalidade	Os dados devem ser objeto de um tratamento lícito e justo.
Princípio da finalidade	Os dados devem ser tratados de forma compatível com as finalidades para a qual foram recolhidos. Excetua-se as seguintes hipóteses: i) o responsável pelo tratamento esteja autorizado por lei a tratar esses dados pessoais, conforme nova finalidade; ii) o tratamento seja necessário e proporcionado para essa outra finalidade.
Princípio da segurança	Os dados devem ser tratados de uma forma que garanta a sua segurança adequada, incluindo a proteção contra o seu tratamento não autorizado ou ilícito, e contra a sua perda, destruição ou danificação acidentais, recorrendo-se a medidas técnicas ou organizativas adequadas.
Art. 28º do Regulamento Europol	**Conteúdo**
Princípio da equidade/legalidade	Os dados devem ser tratados com equidade e em conformidade com a lei.
Princípio da segurança	Os dados devem ser tratados de uma forma que garanta a sua devida segurança.

Fonte: Adaptado pelo autor a partir da Diretiva UE nº 680/2016 e do Regulamento eu n° 794/2016 (Europol).

Os princípios mencionados no Quadro 2, que foram extraídos da Diretiva UE nº 680/2016 e do Regulamento Europol, podem ser relacionados com as fases do processamento de informações na teoria sistêmica da informação. Neste sentido, o princípio da legalidade significa que o tratamento de dados seja feito de maneira legal e justa, ou seja, o tipo de processamento a ser realizado deve estar legalmente autorizado. Assim, os sistemas de informação policial devem ser compatíveis com as regulamentações que protegem a privacidade e os direitos dos titulares dos dados que estão sendo processados.

Do mesmo modo, os dados somente podem ser tratados de acordo com uma finalidade específica, que deve ser compatível com àquela original da coleta dos dados. Assim, na fase de processamento torna-se essencial garantir que os dados sejam tratados de maneira compatível

com as finalidades para as quais eles foram coletados. Todo sistema de informação policial deve ser configurado de um modo que permita ao processamento de dados ocorrer de acordo com os objetivos originais da coleta, garantindo que não sejam usados de maneira incompatível.

Já o princípio da segurança, previsto na Diretiva UE nº 680/2016 e no Regulamento da Europol engloba várias fases do processamento da informação. Este princípio enfatiza a necessidade de proteger os dados contra tratamento não autorizado ou ilícito, bem como contra a perda, destruição ou danos acidentais. Isso significa que, ao longo de todas as fases do processamento, medidas técnicas e organizacionais apropriadas devem ser implementadas, para garantir a segurança e proteção dos dados.

Quadro 3 – Princípios da fase da saída (acesso aos itens informacionais por parte dos usuários, disseminação, entrega da informação, descartes etc.).

Art. 4º da Diretiva UE nº 680/2016	**Conteúdo**
Princípio da exatidão	Devem ser tomadas todas as medidas razoáveis, para que os dados inexatos, tendo em conta as finalidades para as quais são tratados, sejam apagados ou retificados sem demora.
Princípio da limitação temporal	Os dados devem ser conservados apenas durante o período necessário, e para as finalidades para as quais devem ser tratados.
Art. 28º do Regulamento Europol	**Conteúdo**
Princípio da exatidão	Devem ser adotadas todas as medidas razoáveis, para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora.
Princípio da temporariedade	Os dados devem ser conservados, de forma a permitir a identificação dos titulares apenas durante o período necessário, para a prossecução das finalidades a que são tratados.

Fonte: Adaptado pelo autor a partir das Diretiva UEnº680/2016 e do Regulamento UE n° 794/2016 (Europol).

Os princípios da exatidão e da limitação temporal, conforme estabelecidos nos Artigos 4º da Diretiva UE nº 680/2016 e 28º do Regulamento Europol, podem ser relacionados à fase de saída (*output*) da teoria sistêmica da informação. Na teoria sistêmica da ciência da informação, durante a fase de saída, é essencial considerar tanto a exatidão dos dados que estão sendo compartilhados, quanto o período de retenção adequado desses dados.

O princípio da exatidão significa que os dados ou informações, a serem extraídos dos sistemas de informação policial, devem ser precisos e corretos. Assim, é fundamental a criação de mecanismos ou metodologias que assegurem que os dados sejam verificados quanto à sua precisão, e que quaisquer dados inexatos sejam corrigidos ou atualizados antes da utilização, divulgação ou compartilhamento. Esse princípio busca garantir que as informações sejam transmitidas de forma precisa, e que a gestão de dados se mostre eficaz e em conformidade com as garantias individuais de proteção de dados.

Já o princípio da limitação temporal (ou princípio da temporariedade) diz respeito ao período durante o qual os dados serão mantidos, antes de serem devidamente descartados ou arquivados em outros sistemas de dados. Neste sentido, esse princípio implica que os dados devem ser mantidos apenas pelo tempo necessário para alcançar as finalidades para as quais foram coletados ou tratados. Para tanto, devem ser estabelecidos procedimentos que garantam que os dados não sejam mantidos além do prazo necessário, evitando o armazenamento excessivo e a potencial exposição de informações sensíveis ou obsoletas.

5.2. CLASSIFICAÇÃO DOS TIPOS DE DADOS PESSOAIS QUE SÃO PRODUZIDOS OU COLETADOS PELAS POLÍCIAS

De acordo com o referencial teórico analisado na presente pesquisa, verifica-se que o tratamento de dados pessoais, na atividade policial, deve partir de uma distinção clara entre as diferentes categorias de dados pessoais e os respectivos titulares dos dados coletados. Assim, qualquer modelo de proteção contra o tratamento de dados pessoais ilegítimos ou abusivos deve partir de uma classificação detalhada dos diferentes tipos de dados pessoais, que são armazenados pelas instituições policiais. A partir desta classificação é possível conceber um escalonamento dos níveis de proteção dos dados pessoais, de acordo com as características específicas de cada elemento informacional coletado. Neste sentido, a classe "dado pessoal" pode ser dividida nas seguintes subclasses:

i. *Dado pessoal*: informações relativas a uma pessoa singular, identificada ou identificável
ii. *Dado pessoal sensível*: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, dado genético ou dado biométrico (fotos).
iii. *Dado pessoal sigiloso*: dados sujeitos à reserva de jurisdição, ou seja, dados que somente podem ser obtidos mediante decisão judicial

O escalonamento do grau de proteção, a ser garantido aos titulares dos dados, também depende do tipo de resultado que se busca com o tratamento do dado, ou seja, do conteúdo da informação que será produzida a partir dos dados tratados. Conforme Artigo 6º da Diretiva, os dados pessoais também podem ser classificados de acordo com diferentes categorias de titulares de dados, especialmente:

i. Pessoas em relação às quais existem indícios suficientes de que cometeram um crime;

ii. Pessoas em relação às quais existem indícios suficientes de que estão prestes a cometer um crime;
iii. Pessoas processadas pela prática de um crime;
iv. Pessoas condenadas definitivamente pela prática de um crime;
v. Vítimas de um crime;
vi. Pessoas em relação às quais certos fatos indicam que podem ser vítimas de um crime;
vii. Testemunhas ou pessoas que possam ser chamadas a testemunhar em investigações criminais;
viii. Contatos ou associados a uma das pessoas indicadas nos itens i) e ii);
ix. Pessoas que possam fornecer informações sobre os crimes em causa.

Conforme o regulamento da Europol (União Europeia, 2016c), os dados relativos às pessoas referidas nos itens (i) e (ii) citados acima podem incluir as seguintes categorias de dados pessoais:

1) Dados pessoais:

1.1) Nome atual e anterior;

1.2) Nome de solteiro(a);

1.3) Nome do pai (quando necessário para efeitos de identificação);

1.4) Nome da mãe (quando necessário para efeitos de identificação);

1.5) Sexo;

1.6) Data de nascimento;

1.7) Local de nascimento;

1.8) Nacionalidade;

1.9) Estado civil;

1.10) Outros nomes pelos quais a pessoa é conhecida;

1.11) Alcunha;

1.12) Pseudónimo ou nome falso utilizado;

2) Descrição física:

2.1) Descrição física;

2.2) Sinais particulares (marcas/cicatrizes/tatuagens etc.);

3) Meios de identificação:

3.1) Documentos de identidade/carta de motorista;

3.2) Números do cartão de identidade/passaporte;

3.3) Número de identificação tributária nacional/número de segurança social;

3.4) Imagens fotográficas e outras informações sobre o aspeto físico;

3.5) Dados de identificação obtidos por métodos de polícia científica, nomeadamente impressões digitais, perfil de DNA, perfil vocal, grupo sanguíneo, informações sobre a dentição;

4) Profissão e aptidões:

4.1) Emprego e ocupação atuais;

4.2) Emprego e ocupação anteriores;

4.3) Estudos (ensino secundário/universitário/profissional);

4.4) Habilitações e diplomas;

5) Dados econômicos e financeiros:

5.1) Dados financeiros;

5.2) Patrimônio em dinheiro,

5.3) Ações;

5.4) Dados imobiliários;

5.5) Vínculos a sociedades e empresas;

5.6) Contatos de bancos e instituições de crédito;

5.7) Situação fiscal;

5.8) Outras informações sobre a gestão dos negócios financeiros da pessoa;

6) Dados comportamentais:

6.1) Estilo de vida (por exemplo, viver acima das suas posses) e hábitos;

6.2) Deslocamentos;

6.3) Locais frequentados;

6.4) Armas e outros instrumentos perigosos;

6.5) Nível de perigosidade;

6.6) Riscos específicos, nomeadamente probabilidade de fuga, ligações com agentes públicos;

6.7) Perfis e traços de caráter de tendência criminosa;

6.8) Consumo de drogas;

7) Contatos e associados, incluindo o tipo e a natureza do contato ou da associação;

8) Meios de comunicação utilizados, como telefone (fixo ou móvel), fax, pager, correio eletrônico, endereços postais, ligações internet;

9) Meios de transporte utilizados, nomeadamente carros, barcos, aeronaves, incluindo informações que permitam a identificação desses meios de transporte (números de registo ou matrícula);

10) Informações relativas a atos criminosos:

10.1) Condenações anteriores;

10.2) Presumível participação em atividades criminosas;

10.3) Formas de atuação;

10.4) Meios que foram ou possam ser utilizados para preparar e/ou cometer crimes;

10.5) Associação a grupos ou organizações criminosas e lugar que ocupa dentro delas;

10.6) Função na organização criminosa;

10.7) Área geográfica das atividades criminosas;

10.8) Material reunido no decurso de uma investigação, nomeadamente imagens fotográficas e de vídeo;

11) *Referência a outros sistemas de informação,* que conservem informações sobre a pessoa:

11.1) Organismos policiais internacionais (Interpol, Ameripol, Europol);

11.2) Autoridades policiais/aduaneiras;

11.3) Outras autoridades;

11.4) Organizações internacionais;

11.5) Entidades públicas;

11.6) Entidades privadas;

12) Informações sobre pessoas jurídicas associadas:

12.1) Denominação da pessoa jurídica;

12.2) Localização;

12.3) Data e lugar do estabelecimento;

12.4) Número de registo administrativo;

12.5) Forma jurídica;

12.6) Capital social;

12.7) Setor de atividade;

12.8) Filiais nacionais e internacionais;

12.9) Diretores e sócios;

12.10) Ligações com instituições financeiras.

Em relação aos "contatos e associados", tal como referido no item (viii), trata-se das pessoas através das quais há razões suficientes para se crer que podem ser obtidas informações relevantes para a investigação ou análise, ou seja, que dizem respeito às pessoas em relação e às quais existem indícios suficientes de que cometeram um crime, ou de que estão prestes a cometer um crime. "Contatos" seriam todas as pessoas que mantêm contatos esporádicos com o suspeito/investigado, sendo que "associados" são todas as pessoas que mantêm contatos

regulares (União Europeia, 2016c).

Em relação aos contatos e associados, seus dados pessoais podem ser conservados na medida do necessário, desde que haja motivos para crer que são pertinentes para a análise da relação com suspeitos de terem cometido, ou de estarem prestes a cometer um crime. Neste contexto, essa relação do suspeito com o contato ou associado deve ser esclarecida o mais cedo possível. Caso a presunção dessa relação se revelar infundada, os dados do contato ou associado devem ser imediatamente apagados (União Europeia, 2016c).

No que diz respeito a pessoas que tenham sido vítimas de crime, ou relativamente às quais existem motivos para crer que possam vir a ser vítimas de crime, podem ser conservados dados como a identificação, o motivo pelo qual foi vítima da infração, danos e prejuízos (físicos/financeiros/psicológicos/outros), a necessidade de garantir o anonimato e a possibilidade de ser ouvida em tribunal. Se necessário, podem ser conservados outros dados, desde que existam motivos para crer que são pertinentes para a análise do papel de determinada pessoa enquanto vítima real ou potencial. Os dados que não sejam necessários para análises ulteriores devem ser apagados (União Europeia, 2016c).

Já em relação a pessoas que possam ser chamadas a testemunhar em investigações relacionadas com crimes em causa, ou em subsequentes processos penais, podem ser conservados os seus dados de identificação. Também podem ser conservadas informações sobre atos criminosos testemunhados por essas pessoas, incluindo sobre o seu relacionamento com outras pessoas associadas ao caso, necessidade eventual de garantir o anonimato, necessidade de possível proteção a quem a fornece, eventual nova identidade, e a possibilidade de ser ouvido em tribunal. Se necessário, também podem ser conservados outros dados, desde que haja motivos para crer que são pertinentes para a análise do papel dessas pessoas como testemunhas, sendo que os dados que não sejam necessários para análises ulteriores também devem ser apagados (União Europeia, 2016c)

Por fim, no que diz respeito a pessoas que possam fornecer informações sobre crimes em causa, podem ser conservados os dados de identificação, bem como dados pessoais codificados, os tipos de informações fornecidas, necessidade eventual de garantir o anonimato, necessidade de eventual proteção a quem a fornece, nova identidade, a possibilidade de ser ouvido em tribunal, experiências negativas, e recompensas recebidas (financeiras/favores). Do mesmo modo, se necessário, podem ser conservados outros dados indicados, desde que haja motivos para crer que são pertinentes para a análise do papel dessas pessoas como informantes. De qualquer modo, os dados que não sejam necessários para análises ulteriores deverão ser também apagados.

5.3. CLASSIFICAÇÃO DAS CATEGORIAS DE TRATAMENTO DE DADOS PESSOAIS REALIZADAS PELOS ÓRGÃOS DE SEGURANÇA PÚBLICA

A classificação dos diferentes titulares de dados, por sua vez, possui relação com as diferentes finalidades que a polícia pretende alcançar com o tratamento. Assim, o tipo de tratamento é também definido em razão das diversas categorias de atividades conduzidas pela polícia, tais como ações preventivas, investigação criminal, análises estratégicas e análises operacionais, bem como análises para fins de interesse público, científicos, estatísticos ou históricos. Neste contexto, devem ser estabelecidas regras específicas de segurança técnica e organizacional, em relação aos diferentes riscos apresentados por cada um dos seguintes tipos operações de tratamento:

i. Ações preventivas: cruzamento de dados de pessoas relativamente às quais haja indícios factuais ou motivos razoáveis, nos termos da legislação, para suspeitar estão cometendo um crime, ou que virão a cometer infrações penais;
ii. Investigação criminal: cruzamento de dados de pessoas suspeitas da autoria ou coautoria de uma infração penal;
iii. Análise estratégica: voltada à identificação de ameaças à segurança pública;
iv. Análises operacionais: relacionadas à identificação de alvos prioritários, definição das melhores metodologias de investigação a serem empregadas, apoio operacional em investigações complexas que envolvam grande volume de dados;
v. Análises para fins de interesse público: científicos, estatísticos ou históricos.

Em qualquer estudo sobre o tratamento de dados pessoais no âmbito policial, faz-se necessário estabelecer uma distinção entre “dado” e “informação”. Segundo algumas teorias da CI, dado seria qualquer elemento identificado em sua forma bruta que, por si só, não conduz a uma compreensão de determinado fato ou situação. Por sua vez, a informação está relacionada ao contexto de dados que permitem a representação de fatos, conceitos ou instruções. Em termos gerais, informação é o conhecimento produzido como resultado do processamento dos dados (Milagre; Sengundo, 2015). Esta relação conceitual entre dado e informação tem reflexo direto na sistematização das regras de proteção e garantia de segurança, tendo em vista a categorização das diversas finalidades pelas quais o tratamento do dado é realizado pela polícia.

As regras em matéria de acesso e utilização de informações, previstas no regulamento da Europol, podem ser utilizadas para a compreensão de como um sistema de proteção de dados pessoais no âmbito da atividade policial é formalmente constituído. A Europol pode tratar dados

e informações que lhe são fornecidos pelos Estados-Membros, nos termos de cada legislação nacional, por outros organismos da União Europeia, por países terceiros não membros da UE, outras organizações internacionais como a Interpol, organismos privados e pessoas particulares.

Do mesmo modo, a agência policial europeia pode obter e tratar diretamente informações, incluindo dados pessoais, provenientes de fontes de acesso público, tais como a internet e bases de dados públicas. Na medida em que tenha acesso informatizado a dados constantes de sistemas de informações policiais a níveis nacionais, bem como a outras fontes de dados públicas ou privadas, a Europol passa a tratar dados pessoais caso seja necessário para o exercício das suas atribuições. Por sua vez, o acesso a tais sistemas de informação só é concedido a membros do pessoal da Europol devidamente autorizados, unicamente na medida em que tal acesso seja necessário e proporcional ao desempenho das suas funções (União Europeia, 2016c).

Por sua vez, a Europol realiza, tanto quanto possível, a avaliação da confiabilidade e exatidão da fonte das informações que recebe, através do seguinte código específico:

I. Quanto à fonte:

A. quando não há dúvidas quanto à autenticidade, à credibilidade e à competência da fonte, ou quando as informações são fornecidas por uma fonte que tem provado ser fiável em todos os casos;
B. Quando as informações são fornecidas por uma fonte que tem provado ser fiável na maioria dos casos;
C. Quando as informações são fornecidas por uma fonte que tem provado não ser fiável na maioria dos casos;
D. Quando as informações são fornecidas por uma fonte cuja fiabilidade não pode ser avaliada.

II. Quanto à exatidão da informação:

1. Informações cuja exatidão não suscita dúvidas;
2. Informações conhecidas pessoalmente pela fonte, mas não conhecidas pessoalmente pelo agente que a transmite;
3. Informações não conhecidas pessoalmente pela fonte, mas corroboradas por outras informações já registadas;
4. Informações não conhecidas pessoalmente pela fonte, e que não podem ser corroboradas.

Por sua vez, tendo em vista o tipo de dados, o contexto e as finalidades do tratamento dos dados, bem como a probabilidade e a gravidade dos riscos que o tratamento pode

representar para os direitos e a liberdade das diversas classes de titulares dos dados, os normativos europeus analisados adotam as seguintes medidas de segurança e controle:

i. *Controle de acesso ao equipamento*: impedir o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento;
ii. *Controle dos suportes de dados*: impedir que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização;
iii. *Controle da conservação*: impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou eliminação de dados pessoais arquivados;
iv. *Controle dos utilizadores*: impedir que os sistemas de tratamento automatizado sejam utilizados por pessoas não autorizadas, por meio de equipamento de comunicação de dados;
v. *Controle do acesso aos dados*: assegurar que as pessoas autorizadas a utilizarem um sistema de tratamento automatizado só tenham acesso aos dados pessoais abrangidos pela sua autorização de acesso;
vi. *Controle da comunicação*: assegurar que possa ser verificado e determinado se os dados pessoais foram, ou podem ser transmitidos, utilizando-se equipamento de comunicação de dados;
vii. *Controle da introdução*: assegurar que possa ser verificado e determinado a posteriori quais os dados pessoais introduzidos nos sistemas de tratamento automatizado, quando e por quem;
viii. *Controle do transporte*: impedir que, durante as transferências de dados pessoais ou o transporte de suportes de dados, os dados pessoais possam ser lidos, copiados, alterados ou suprimidos sem autorização;
ix. *Recuperação*: assegurar que os sistemas utilizados possam ser restaurados, em caso de interrupção;
x. *Integridade*: assegurar que as funções do sistema funcionem, que os erros de funcionamento sejam assinalados (fiabilidade) e que os dados pessoais conservados não possam ser falseados por um disfuncionalidade do sistema.

6. DISCUSSÕES: ANÁLISE CRÍTICA

No cenário contemporâneo, a crescente digitalização da sociedade gerou um vasto acervo de dados pessoais, levando à necessidade premente de analisar a complexa interseção entre o sistema de proteção de dados pessoais no âmbito policial e o sistema de proteção geral de dados. Grandes empresas da internet realizam a coleta incessante de dados comportamentais que usam para o aprimoramento de produtos e serviços, bem como para alimentar processos de fabricação de produtos de predição. Tais produtos antecipam o que um determinado indivíduo fará naquele momento ou logo em seguida, sendo comercializados em um tipo de mercado de comportamento futuro. Neste contexto, máquinas automatizadas não só conhecem o comportamento das pessoas, como também moldam esse comportamento em larga escala em prol das finalidades de terceiros (Zuboff, 2021).

Com a difusão e o barateamento dos custos de sensores, câmaras e sistemas de armazenamento, as pessoas passaram a gerar enormes quantidades de dados. Tudo o que a pessoa algum dia ouviu ou viu ou vivenciou se torna pesquisável, ou seja, a vida inteira das pessoas se torna pesquisável. As grandes empesas que lidam com informações pessoais, como o Google, Meta, Microsoft, Apple, dentre outras, perceberam que a "experiência humana" podia ser extraída de forma *on-line*, e com um custo muito baixo no mundo real. Uma vez extraída, a experiência humana pode ser transmitida na forma de dados comportamentais, formando a base de uma categoria nova de trocas de mercado. Nesta nova lógica, a experiência humana é subjugada aos mecanismos de mercado do capitalismo e renasce como "comportamento", que é transformado em dados que alimentam as máquinas de fabricação de predições (Zuboff, 2021).

Apesar de todo avanço tecnológico e capacidade computacional da maioria dos negócios que tem a internet como base e informações pessoais como principal matéria prima, o que realmente está por trás do sucesso de tais empresas são os mecanismos econômicos que desconsideram o respeito aos limites privados da experiência humana. Ao invés de garantir a integridade da vida privada do indivíduo, grandes empresas da internet declaram o direito de usurpar os direitos de escolha individual em prol da vigilância unilateral e extração autoautorizada da experiência humana, tendo por objetivo o lucro de outras empresas ou organizações. Baseadas nesse modelo padrão de atuação, as chamadas Big Techs desfrutam de extraordinárias assimetrias de conhecimento e poder, em um nível sem precedentes na história da humanidade (Zuboff, 2021).

Assim, em um contexto em que empresas privadas detêm quantidades massivas de

informações pessoais, muitas vezes superando em escala o que é mantido pelo Estado, a reflexão sobre o alcance das regras de proteção de dados no âmbito da segurança pública torna-se imperativa. Na busca por regulamentar a atividade de tratamento de dados pessoais pelas polícias, seria uma posição ingênua ignorar a complexidade do cenário atual, onde as Big Techs detêm vastos volumes de dados pessoais, enquanto as instituições estatais, incluindo as forças policiais, enfrentam desafios significativos em lidar com a assimetria de conhecimento e poder diante dessas corporações.

Desse modo, é crucial adotar abordagens regulatórias equilibradas e contextuais. A tentativa de estabelecer regulamentações estritas para as atividades das polícias sem considerar um paralelo com as Big Techs seria uma grande contradição, pois resultaria em um sistema de proteção de dados pessoais insuficiente e limitado em seu alcance. A influência dessas corporações transcende fronteiras e abrange múltiplos setores da sociedade, colocando em evidência a necessidade de uma abordagem holística e adaptável às dinâmicas atuais.

Para a discussão da regulamentação das atividades das polícias no tratamento de dados pessoais, é crucial levar em consideração não apenas a necessidade de proteger os direitos individuais dos cidadãos, mas também de realizar um paralelo com os desafios impostos pela presença das Big Techs. Enquanto redes sociais coletam e tratam dados pessoais somente para fins de interesse privado e obtenção de lucros comerciais, a atividade policial realiza o tratamento de dados para fins de segurança pública. Dessa forma, a regulamentação do tratamento de dados nas polícias deve ser cuidadosamente desenhada de modo a reconhecer não apenas as assimetrias de conhecimento e poder entre o Estado e as Big Techs, mas também para garantir que os interesses de segurança da sociedade sejam preservados em meio às rápidas mudanças e avanços tecnológicos.

A ponderação cuidadosa de regras e diretrizes torna-se essencial para garantir que as atividades das forças policiais não se vejam excessivamente dificultadas, ao mesmo tempo em que se assegura a preservação dos direitos fundamentais dos cidadãos. Neste contexto, a busca por equilíbrio é fundamental para o desenvolvimento de políticas e práticas eficazes que resguardem tanto a segurança pública quanto a privacidade individual. Assim, qualquer modelo a ser proposto necessita partir de uma análise dos prós e os contras dos interesses concorrentes, e mais precisamente, da segurança coletiva e os direitos individuais. Por este enfoque, quanto mais a sociedade se sentir segura, maior proteção deve ser dada aos direitos individuais. Do mesmo modo, quanto mais a comunidade se sinta ameaçada por alguma atividade criminosa, maiores serão os motivos encontrados para restringir direitos individuais com o objetivo de impedir essa atividade.

É necessário reconhecer que os direitos individuais são instrumentos utilizados para a promoção do bem-estar social e, conforme as condições necessárias para esse bem-estar são alteradas, a abrangência dos direitos individuais também deve diminuir ou aumentar (Posner, 2010a). Torna-se, pois, importante realizar uma abordagem crítica a respeito da utilização de um modelo legislativo estrangeiro em âmbito nacional, ainda mais se levarmos em consideração a discrepância que existe entre o Brasil e alguns países da Europa em termos de índices de criminalidade, violência urbana, e da estrutura logística do sistema jurídico-policial e penitenciário.

Tecnologias de tratamento de dados pessoais não podem ser consideradas como certas ou erradas em si mesmas. Desse modo, qualquer sistema de proteção dos dados pessoais deve levar em consideração todos os aspectos do tratamento de dados como atividade essencial das polícias, devendo ser alcançado um modelo que seja razoável e aceito como eficiente pelos órgãos do sistema de segurança pública e, ao mesmo temo, que seja compreendido como justo e legítimo pela sociedade em geral. Assim, para avaliar os interesses sociais em disputa, deve-se buscar o conhecimento necessário na experiência e na reflexão, sendo difícil determinar, de forma apriorística, quais tecnologias são consideradas “boas” ou “más” (Posner, 2012, p. 40-41).

A legitimidade da utilização de novas tecnologias de coleta e análise de dados pessoais, como aquelas relacionadas à identificação de suspeitos por meio de amostras de DNA, encontrados em um local de crime, decorre das inúmeras consequências positivas que tais inovações promovem para a persecução criminal. Entretanto, as condições de legitimidade e proporcionalidade desta medida não podem estar vinculadas simplesmente à incorporação e ponderação de princípios, como o princípio da liberdade versus o princípio da segurança. Ao contrário, deve-se buscar o estabelecimento de regras claras e precisas sobre os limites de atuação dos órgãos de segurança pública.

Assim, ao invés de promover a segurança jurídica, para que a persecução penal possa ser realizada de forma mais eficiente e eficaz, modelos de proteção com base apenas na ponderação de princípios pode se tornar uma fonte inesgotável de disputas judiciais, principalmente quando a atividade policial estiver relacionada à investigação de grandes esquemas de corrupção ou da criminalidade financeira de colarinho branco.

Por um enfoque de inspiração utilitarista ou pragmática deve-se atribuir um papel fundamental à experiência e à análise das consequências, como fundamento de legitimidade das atividades policiais. Por uma visão pragmática, o equilíbrio entre o direito individual e a segurança deve ser obtido, no ponto em que qualquer limitação ao primeiro passe a criar um

mal maior à sociedade, pela redução das liberdades, do que os benefícios esperados decorrentes da atividade de investigação criminal. Do mesmo modo, qualquer expansão adicional dos direitos individuais causaria um desequilíbrio no sistema jurídico, caso resultasse em um mal maior à sociedade, em decorrência da redução da segurança coletiva, do que os benefícios esperados pelo aumento da liberdade.

Deve-se ressaltar, do mesmo modo, a natureza probabilística da avaliação de novas tecnologias de tratamento de dados, com a adoção de noções como "benefício esperado" para a sociedade, e o "custo esperado" que o indivíduo irá sofrer pela intervenção estatal. Assim, compreender como a ampliação do escopo dos direitos individuais pode afetar a capacidade do estado de prevenir, detectar e investigar crimes é tão importante quanto verificar em que medida o aumento do poder de tratamento de dados pelo Estado pode afetar o direito dos cidadãos. O sistema de justiça criminal deve balancear os dois tipos de consequências, de forma igualmente cuidadosa, pois não é pragmático priorizar nem a segurança coletiva, nem os direitos individuais (Posner, 2010b).

Por sua vez, devem ser proibidos os tratamentos de dados pessoais que sejam desarrazoados. Em outros termos, deve ser feita uma comparação entre os benefícios e os custos dessas medidas para as atividades de prevenção, investigação, detecção ou repressão de infrações penais, ou execução de sanções penais. Exemplificando, quanto mais custoso for o tratamento de dados para o seu titular, e menos eficiente for a técnica utilizada para detectar crimes, e identificar ou localizar os atores de crimes, mais provável será que a medida seja considerada desarrazoada.

Uma abordagem de escala móvel implica na concessão de valores diferentes para cada tipo de dado pessoal tratado, bem como para cada elemento justificador da atividade estatal. Por exemplo, se o custo de uma medida de tratamento de dados for mantido constante, o nível de elementos exigidos para sua justificação passa a diminuir, caso a magnitude do crime investigado aumente, tendo em vista que o mal causado à sociedade pela não detecção de um crime é acrescido na exata proporção de sua gravidade (Posner, 2010b).

Um enfoque pragmático do tratamento de dados fornece elementos para a realização do correto balanceamento entre as novas metodologias de produção de prova, e a preservação dos direitos individuais do investigado. O tratamento de dados se traduz em um mal para quem o sofre, e como tal, para se justificar, tem que alcançar sua finalidade precípua de promoção do bem-estar social (Dias, 1999). Entretanto, certas críticas da adoção de novas tecnologias de tratamento de dados refletem uma visão que não leva em consideração cálculos baseados em análises de custos e benefícios, conferindo aos direitos individuais prioridade absoluta em

relação aos valores sociais. Para se evitar tais críticas, é necessária a realização de uma abordagem que incorpore o respeito aos direitos humanos no cálculo do bem-estar social a ser promovido pelas instituições detentoras do poder investigativo estatal.

7. CONSIDERAÇÕES FINAIS

O tratamento de dados faz parte da própria essência da atividade policial, constituindo a produção de informações e conhecimentos, sobre crimes e criminosos, como o principal produto das instituições que compõem o sistema brasileiro de segurança pública. Entretanto, verifica-se que esta atividade essencial ainda não foi devidamente discutida e regulamentada em âmbito nacional. Neste sentido, o presente estudo se propôs a analisar criticamente o microssistema legislativo europeu de proteção de dados pessoais, no contexto das atividades policiais, fornecendo uma visão aprofundada sobre as questões éticas, jurídicas e operacionais sobre o tema.

O trabalho procurou estabelecer uma base teórica sólida, abrangendo conceitos essenciais relacionados à proteção de dados pessoais e à Ciência da Informação, de modo a proporcionar um entendimento profundo das principais questões legais relacionadas com a criação e a manutenção de sistemas de informação policial. Foi verificada a existência de um robusto conjunto de princípios e normas internacionais de proteção de dados pessoais, relacionados às atividades de prevenção, investigação, detecção ou repressão de infrações criminais, e execução de sanções penais. Isso demonstra a necessidade de se adotar, no Brasil, mecanismos semelhantes, que forneçam garantias de proteção da privacidade e liberdade informacional de seus cidadãos.

Procurou-se também realizar uma descrição dos diversos tipos de dados pessoais produzidos ou coletados pelas polícias, bem como das diferentes categorias de tratamento de dados realizadas pelos órgãos de segurança pública. Foram descritas as principais práticas de coleta, armazenamento e uso de informações no contexto policial moderno, caracterizado pelo uso da informação como principal ativo das polícias. A partir da descrição das práticas policiais atuais, com o possível uso de tecnologias de vigilância e policiamento preditivo, verificou-se como a proteção dos dados pessoais deve acompanhar tais inovações, verificando os impactos destas tecnologias na criação de diretrizes para a atuação policial.

A compreensão das práticas de coleta, armazenamento e uso de informações no contexto policial é fundamental para a compreensão dos limites éticos e jurídicos do poder do Estado sobre o tratamento de dados pessoais, para fins de segurança pública. Neste contexto, foi enfatizada a importância dos direitos humanos, incluindo o direito à privacidade e à proteção de dados, como princípios balizadores da atividade policial moderna. Ao destacar o contexto europeu, e o atual estágio nacional de proteção de dados no âmbito policial, este estudo permitiu a adoção de uma perspectiva comparativa essencial para o avanço das discussões do tema.

Assim, as conclusões deste trabalho reforçam a importância do estabelecimento da proteção de dados pessoais no contexto policial, ressaltando a necessidade de um equilíbrio entre a eficácia da atuação policial e a preservação dos direitos individuais.

Reconhecendo que a proteção de dados pessoais está em constante evolução no âmbito policial, este trabalho buscou, por fim, induzir pesquisas futuras, que visem acompanhar as mudanças dinâmicas do uso da informação no âmbito da segurança pública, com o desenvolvimento de diretrizes práticas para a aplicação eficaz das regulamentações existentes.

REFERÊNCIAS

AFFONSO, E. P.; OLIVEIRA, S. C. de; SANT'ANA, R. C. G. Análise do equilíbrio entre privacidade e utilidade no acesso a dados. **Informação &Amp; Sociedade: Estudos**, v. 27, n. 1, 2017. Disponível em: https://periodicos.ufpb.br/ojs/index.php/ies/article/view/29422. Acesso em: 10 fev. 2023.

AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA. **Bias in Algorithms** – Artificial Intelligence and Discrimination. Viena: FRA, 2022. Disponível em: https://fra.europa.eu/en/publication/2022/bias-algorithm. Acesso em: 11 maio 2023.

AGÊNCIA DOS DIREITOS FUNDAMENTAIS DA UNIÃO. **Manual da Legislação Europeia sobre proteção de dados**. Edição de 2018. Disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. Acesso em: 15 nov. 2022.

ALVAREZ, E.B.; ALONSO, B. T.; SILVEIRA, P. C. (ed.). **Ciência da Informação e Ciências Policiais Conexões e Experiências**. Vol. 4. Tallinn, Estonia: Pro-Metrics, 2023.

ARAÚJO, Carlos Alberto Ávila de. Correntes teóricas da ciência da informação. **Ciência da Informação**, v. 38, n. 3, 2009.

ARAÚJO, Carlos Alberto Ávila de. Fundamentos da Ciência da Informação: correntes teóricas e o conceito de informação. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 4, n. 1, p. 67, jan./jun. 2014.

ARAÚJO, Carlos Alberto Ávila de. **O que é ciência da informação**. Belo Horizonte: KMA, 2018.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BENTHAM, J. Uma introdução aos princípios da moral e da legislação. *In*: MORRIS, C. (org.). **Os grandes filósofos do direito**. São Paulo: Martins Fontes, 2002. p. 260-288.

BORKO, H. Information Science: What is it? **American Documentation**, v.19, n.1, p.3-5, Jan. 1968. Disponível em: https://www.marilia.unesp.br/Home/Instituicao/Docentes/EdbertoFerneda/mri-01---information-science---what-is-it.pdf. Acesso em: 20 set. 2021.

BRAKEL, Rosamunde van. Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing. *In*: SLOOT, Bart van der; BROEDERS, Dennis; SCHRIVERS, Erik (ed.). **Exploring the Boundaries of Big Data.** Amsterdam: Amsterdam University Press, 2016.

BRASIL. **Lei nº 13.675/2018, de 11 de junho de 2018.** Cria a Política Nacional de Segurança Pública e Defesa Social (PNSPDS) e institui o Sistema Único de Segurança Pública (SUSP). Brasília, DF: Presidência da República, 2018a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13675.htm. Acesso em: 27 abr. 2023.

BRASIL. **Lei nº 13.709/2018, de 18 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República, 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 fev. 2023.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Lei de Interceptações Telefônicas e Telemáticas. Brasília, DF: Presidência da República, 1996. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 18 jul. 2023.

BRITTO, Ayres. **O Humanismo como categoria constitucional**. Belo Horizonte: Fórum, 2016.

BUCKLAND, Michael. Information as Thing. **Journal of the American Society of Information Science**, v. 42, n. 5, p. 351-360, 1991.

BUSH, V. As we may think. **Atlantic Monthly**, v. 176, n. 1, p.101-108, 1945. Disponível em: http://www.theatlantic.com/unbound/flashbks/computer/bushf.htm. Acesso em: 28 ago. 2021.

CÂMARA DOS DEPUTADOS. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. Brasília, DF: Câmara dos Deputados, 2020. Disponível em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em: 28 ago. 2021.

CEBALLOS, Erica Janet Agudelo Ceballos; ARIAS, Alejandro Valencia. La gestión del conocimiento, una política organizacional para la empresa de hoy. **Ingeniare – Revista chilena de ingeniería**, v. 26, n° 4, 2018.

CHOUKR, Fauzi Hassan. **Garantias Constitucionais na Investigação Criminal**. Rio de Janeiro: Lumen Juris, 2001.

COLVIN, Madeleine; COOPER, Jonathan. **Human Rights in the Investigation and Prosecution**. New York: Oxford, 2009.

COMISSÃO EUROPEIA. **The Guide to Data Protection in the European Comission**. Bruxelas: Comissão Europeia, 2023. Disponível em: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en. Acesso em: 09 set. 2022.

CONSELHO DA EUROPA. **Convenção Europeia dos Direitos Humanos**. Roma: Conselho da Europa, 1950. Disponível em: https://www.echr.coe.int/documents/d/echr/convention_por. Acesso em: 18 dez. 2022.

CONSELHO DA EUROPA. **Manual da Legislação Europeia sobre Proteção de Dados**. Edição 2018. Luxemburgo: Conselho da Europa, 2018. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_pt.pdf. Acesso em: 15 fev. 2023.

CONSELHO DA EUROPA. **Manual da Legislação Europeia sobre Proteção de Dados**. Edição 2018. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf. Acesso em: 15 nov. 2022.

CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. **Acórdão de 13 de maio de 2014 no processo C-131/12.** Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. Espanha: Grand Court, 2014b. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:62012CJ0131. Acesso em: 14 fev. 2023.

CORTE DE JUSTIÇA DA UNIÃO EUROPEIA. **Cases C-293/12 and C-594/12.** Digital Rights Ireland Ltd v. Minister for Communications,Marine and Natural Resources and Others and Kärntner Landesregierung and Others. Ireland: Grand Court, 2014a. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0293. Acesso em: 14 fev. 2023.

CORTE EUROPEIA DE DIREITOS HUMANOS. **Case of Peck v. The United Kingdom, jan. 2003**. Strasbourg: CEDH, 2003a. Disponível em: http://hudoc.echr.coe.int/eng?i=001-60898. Acesso em: 07 nov. 2022.

CORTE EUROPEIA DE DIREITOS HUMANOS. **Case of Perry v. The United Kingdom, out. 2003**. Strasbourg: CEDH, 2003b. Disponível em: http://hudoc.echr.coe.int/eng?i=001-61228. Acesso em: 07 nov. 2022.

CORTE EUROPEIA DE DIREITOS HUMANOS. **Case of Pretty v. The United Kingdom, abr. 2002**. Strasbourg: CEDH, 2002. Disponível em: http://hudoc.echr.coe.int/eng?i=001-60448. Acesso em: 04 nov. 2022.

CORTE EUROPEIA DE DIREITOS HUMANOS. **Case of Silver and others v. The United Kingdon , mar. 1983**. Strasbourg: CEDH, 1983. Disponível em: http://hudoc.echr.coe.int/eng?i=001-57577. Acesso em: 02 fev. 2023.

CORTE EUROPEIA DE DIREITOS HUMANOS. **ECHR Knowledge Sharing platform (ECHR-KS)**. Estrasburgo: CEDH, 2023a. Disponível em: https://ks.echr.coe.int/. Acesso em: 12 abr. 2023.

CORTE EUROPEIA DE DIREITOS HUMANOS. **Guide to the Case-Law of the of the European Court of Human Rights** – Data Protection. Estrasburgo: CEDH, 2023b. Disponível em https://ks.echr.coe.int/documents/d/echr-ks/guide_data_protection_eng. Acesso em: 12 abr. 2023.

CORTE EUROPEIA DE DIREITOS HUMANOS. **Petições n. 30562/04 e 30566/04.** Acórdão S. e Marper c. o Reino Unido [GS] de 4 de dezembro de 2008. Inglaterra: CEDH, 2009a. Disponível em: https://rm.coe.int/16806ae65f. Acesso em: nov. 2023.

CORTE EUROPEIA DE DIREITOS HUMANOS. **TEDH, acórdão B.B. c. França de 17 de dezembro de 2009, petição n. 5335/06**. França: CEDH, 2009b. Disponível em: https://rm.coe.int/16806ae65f. Acesso em: nov. 2023.

CRESPO, Enrique B. Estudio Preliminar. *In*: BENTHAM, Jeremy (org.). **Un Fragmento sobre el Gobierno**. Madri: Editorial Tecnos, 2010.

DIAS, Jorge de Figueiredo. **Questões Fundamentais do Direito Penal Revistadas**. São Paulo: Editora Revista dos Tribunais, 1999.

DONNELLY, Jack. **Human Rights**: Teory & Practice. Londres. Cornell, 2003.

EMYGDIO, Jeanne Louize Ensaio sobre ontologia aplicada na recuperação da informação para a Ciência da Informação. **Ponto de Acesso**, v. 15, n. 3, p. 323-343, dez. 2021.

EUROPOL. Data Protection Officer. **Freedom and Security**. Fighting serious crime and terrorism – defending European values. Países Baixos: Agência da União Europeia para a Cooperação Policial, 2023. Disponível em: https://www.europol.europa.eu/DPF/index.html. Acesso em: 10 set. 2022.

FBI. Federal Bureau of Investigation. **J. Edgar Hoover's First Job and the FBI Files.** Disponível em: https://www.fbi.gov/news/stories/2012/june/j-edgar-hoovers-first-job-and-the-fbi-files/j.-edgar-hoovers-first-job-and-the-fbi-files/. Acesso em: 15 ago. 2023.

FERRAJOLI, Luigi. **Direito e Razão** – Teoria do Garantismo Penal. São Paulo: Editora Revista dos Tribunais, 2002.

FLETCHER, Robin. An intelligent use of intelligence: Developing locally responsive information systems in the post-Macpherson era. *In:* MARLOW, A.; LOVEDAY, B. (ed.). **After Macpherson**: Policing after the Stephen Lawrence inquiry. Dorset, UK: Russell House Publishing, 2000.

FRONTEX. **Agência Europeia da Guarda de Fronteiras e Costeira**. Polônia: Frontex, 2023. Disponível em https://frontex.europa.eu/pt/. Acesso em: 03 ago. 2023.

GALVÃO, Pedro. Introdução. *In*: MILL, John Stuart Mill (ed.). **Utilitarismo**. São Paulo: Hunter Books, 2014.

GARTNER GLOSSARY. **Big Data definition**. Connecticut, EUA: Gartner Company, 2023. Disponível em: https://www.gartner.com/en/information-technology/glossary/big-data#:~:text=Big%20data%20is%20high%2Dvolume,decision%20making%2C%20and%20process%20automation. Acesso em: nov. 2023.

GRISOTO, A. P.; SANT'ANA, R. C. G.; SANTAREM SEGUNDO, J. E. A questão da privacidade no contexto da Ciência da Informação: uma análise das Teses e Dissertações do Programa de Pós-Graduação em Ciência da Informação da UNESP campus de Marília. **Revista Ibero-Americana de Ciência da Informação**, v. 8, n. 2, p. 165-181, 2015. DOI: https://doi.org/10.26512/rici.v8.n2.2015.2066.

HERT, Paul; PAPAKONSTANTINOU, Vagelis. The new police and criminal justice data protection directive - a first analysis. **New Journal of European Criminal Law**, v.7, n. 1, 2016.

HJØRLAND, B.; CAPURRO, R. O conceito da informação. **Perspectivas em Ciência da Informação**, v. 12, n. 1, p. 148–207, 2007.

JAMES, Adrian. **Understanding Police Intelligence Work**. Bristol: Policy Press, 2016.

KAISER, Brittany. **Manipulados**. Como a Cambridge Analytica e o Facebook Invadiram a

Privacidade de Milhões e Botaram a Democracia em Xeque. Rio de Janeiro: Harper Collins, 2020.

KLOUS, Sander Klous. Sustainable harvesting of the big data potential. *In*: SLOOT, Bart van der; BROEDERS, Dennis; SCHRIVERS, Erik (ed.). **Exploring the Boundaries of Big Data**. Amsterdam: Amsterdam University Press, 2016.

LAKE, Peter; DRAKE, Robert. **Information Systems Management in the Big Data Era.** Switzerland: Springer Cham, 2014.

LAUDON, Kenneth C.; LAUDON, Jane P. **Management Information Systems** - Managing the Digital Firm. Harlow: Pearson Education Limited, 2014.

LOTT, Yuri Monnerat; CIANCON, Regina de Barros. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da ciência da informação no Brasil. **Perspectivas em Ciência da Informação**, v. 23, n. 4, p. 117-132, out./dez. 2018.

McKAY, Simon. **Covert Policing**. Law and Practice. Oxford: Oxford University Press, 2015.

MILAGRE, J. A.; SEGUNDO, J. E. S. A propriedade dos dados e a privacidade na perspectiva da ciência da informação. **Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação**, v. 20, n. 43, p. 47-76, 2015. Disponível em:. https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2015v20n43p47. Acesso em: 17 mar. 2023.

MILL, John Stuart. **Sobre a Liberdade**. São Paulo: Hedra, 2010.

MOREIRA, Marcelo da Silva; MURIEL-TORRADO, Enrique. A relação da inteligência policial com a Ciência da Informação. *In*: PINTO, Adilson Luiz (org.). **Aproximação entre a Ciência da Informação com a Ciência Policial**. Florianópolis, SC: SENAC-SC, 2019.

MULGAN, Tim. **Utilitarismo**. Petrópolis: Editora Vozes, 2012.

NAVATHE, Shamkant B.; ELMASRI, Ramez. **Fundamentals of database systems**. Boston, Massachusetts: Addison-Wesley, 2010.

NETO, Paulo Mesquita. Prevenção do crime e da violência e promoção da segurança pública no Brasil. *In*: LESSA, R. (coord.). **Arquitetura Institucional do Sistema Único de Segurança Pública**. Rio de Janeiro: SESI-RJ, 2004. p. 200-311. Disponível em http://www.dhnet.org.br/redebrasil/executivo/nacional/anexos/arquiteturainstitucionaldosistemaunicodesegurancapubl.pdf. Acesso em: 16 abr. 2023.

POLÍCIA FEDERAL. **Plano Diretor de Tecnologia de Informação e Comunicação (PDTIC) 2020-2021** - Prorrogado para 2023. Brasília: PF, 2022. Disponível em: https://www.gov.br/pf/pt-br/acesso-a-informacao/acoes-e-programas/plano-diretor-e-estrategico-de-tecnologia-de-informacao-e-comunicacao/pdtic-2020-2021.pdf. Acesso em: 26 ago. 2023.

POSNER. Richard A. **A economia da Justiça**. São Paulo: Martins Fontes, 2010a.

POSNER, Richard A. **Direito, pragmatismo e democracia**. Rio de Janeiro: Forense, 2010b.

POSNER, Richard A. **A problemática da teoria moral e jurídica**. São Paulo: Martins Fontes, 2012.

PUBLICATIONS OFFICE OF THE EUROPEAN UNION. **Directive (EU) 2016/680** – Protecting individuals with regard to the processing of their personal data by police and criminal justice authorities and on the free movement of such data. Luxemburgo: Office of the European Union, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=legissum:310401_3. Acesso em: 10 jan. 2021.

QUIROGA, Cecília Medina; ROJAS, Claudio Nash. **Sistema Interamericano de Directos Humanos**. Introducción a sus Mecanismos de Protección. Santiago: UDEF, 2011.

RAINER, R. Kelly; PRINCE, Brad; CEGIELSKI, Casey G. **Introduction to Information Systems** – Supporting and Transforming Business. 5. ed. Nova Jersey: Wiley, 2013.

RAWLS, John. **Uma Teoria da Justiça**. São Paulo: Martins Fontes, 2000.

ROBERTS, Paul. Law and Criminal Investigation. *In*: NEWBURN, Tim; WILLIAMSON, Tom; WRIGHT, Alan. **Handbook of Criminal Investigation**. New York: Willan Publishing, 2011.

ROXIN, Claus. **Problemas fundamentais de direito penal**. Trad. Ana Paula dos Santos Luís Natscheradet; Maria Fernanda Palma; Ana Isabel de Figueiredo. 3. ed. Lisboa: Vega, 1998.

SÁNCHEZ, Adriana Suárez. Sistemas para la organización del conocimiento: definición y evolución. **e-Ciencias de la Información**, v. 7, n. 2, jul./dez. 2017. Disponível em: **https://revistas.ucr.ac.cr/index.php/eciencias/article/view/26878/29693. Acesso em: jun. 2022**.

SANDEL, Michel J. **Justiça** – O que é fazer a coisa certa. Rio de Janeiro: Civilização Brasileira, 2011.

SARMIENTO, Daniel. O Neoconstitucionalismo no Brasil: Riscos e possibilidades. *In*: SARMENTO, D. (org.). **Filosofia e Teoria Constitucional Contemporânea**. Rio de Janeiro: Editora Lumen Juris, 2009.

SCHUTTER, Olivier de. **International Human Rights Law**. Cambridge: Cambridge, 2010.

SILBERSCHATZ, Abraham; KORTH, Henry F.; SUDARSHAN S. **Database System Concepts.** 6. ed. Nova York: McGraw-Hill, 2011.

SILVA, Leonardo Santiago Melgaço. **Viabilidade do uso da Inteligência Artificial (IA) em lista de passageiros do sistema privado aéreo internacional brasileiro, na busca de passageiro com perfil criminoso relacionado ao tráfico internacional de entorpecentes e drogas afins pela Polícia Federal Brasileiro**. Projeto de pesquisa (Mestrado Interinstitucional em Ciência da Informação) – Polícia Federal de Santa Catarina; Programa de Pós-graduação em Ciência da Informação, Universidade Federal de Santa Catarina, Florianópolis, 2021.

SOCTT, John. **Social Network Analysis**: A Handbook. London: Sage Publications, 2000.

SOUZA, R. R.; ALMEIDA, M. B.; BARACHO, R. M. A. Ciência da Informação em transformação: big data, nuvens, redes sociais e web semântica. **Ciência da Informação**, v. 42, n. 2, 2015. DOI: https://doi.org/10.18225/ci.inf.v42i2.1379.

STANFORD ENCYCLOPEDIA OF PHILOSOPHY. **Rule Consequentialism**. Califórnia: Standford University, 2023. Disponível em: http://plato.stanford.edu/entries/consequentialism-rule/. Acesso em: 15 jul. 2023.

STELFOX, Peter. **Criminal Investigation** – An Introducition to principles and pratice. Cullompton, UK: Willan Publishing, 2009.

SUPREMO TRIBUNAL FEDERAL. **RE 973.837.** Recurso extraordinário em que se discute, à luz do princípio constitucional da não autoincriminação e do art. 5º, II, da Constituição Federal, a constitucionalidade do art. 9º-A da Lei 7.210/1984, introduzido pela Lei 12.654/2012, que prevê a identificação e o armazenamento de perfis genéticos de condenados por crimes violentos ou por crimes hediondos. Tema 905 - Constitucionalidade da inclusão e manutenção de perfil genético de condenados por crimes violentos ou por crimes hediondos em banco de dados estatal. Brasília, DF: STF, 2023. Disponível em: https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=4991018&numeroProcesso=973837&classeProcesso=RE&numeroTema=905. Acesso em: nov. 2023.

UCHÔA, A. P. de M.; SALES, R. de. A importância do uso de ontologias como ferramenta de organização e representação do conhecimento na investigação policial. *In:* ALVAREZ, E.B.; ALONSO, B. T.; SILVEIRA, P. C. (ed.). **Ciência da Informação e Ciências Policiais**: Conexões e Experiências. Vol. 4. Tallinn, Estonia: Pro-Metrics, 2023.

UNIÃO EUROPEIA. **General Data Protection Regulation Compliance Guidelines**. Luxemburgo: União Europeia, 2023. Disponível em https://gdpr.eu/eu-gdpr-personal-data/. Acesso em: 10 set. 2022.

UNINÃO EUROPEIA. **Regulamento (UE) 679/2016 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Luxemburgo: União Europeia, 2016a. Disponível em ttps://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 09 set. 2022.

UNIÃO EUROPEIA. **Diretiva UE 680/2016 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.** Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados. Luxemburgo: União Europeia, 2016b. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri= CELEX%3A32016L0680. Acesso em: 14 dez. 2020.

UNIÃO EUROPEIA. **Regulamento (UE) 794/2016 do Parlamento Europeu e do Conselho, de 11 de maio de 2016**. Cria a Agência da União Europeia para a Cooperação

Policial (Europol). Luxemburgo: União Europeia, 2016c. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri= CELEX:32016R0794&qid=1677940587777&from=EN. Acesso em: set. 2022.

WEBER, Max. **Ciência e Política**: duas vocações. São Paulo: Martin Claret, 2015.

WEBER, Max. **Economia e sociedade**. Vol.1. Brasília: Universidade de Brasília, 2009.

WINER, Tim. **Enemigos**: Una Historia del FBI. Buenos Aires: Debate, 2012.

WOOD, David Murakami (ed.). **A report on the surveillance society: report for the UK information commissioner's office**. Surveillance Studies Network, 2 nov. 2006. Disponível em: http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf. Acesso em: 23 jun. 2015.

ZAMPRONHA, Luís Flávio. Anteprojeto de LGPD Criminal: Desafios conceituais de uma nova estrutura legal da investigação criminal. Brasília, DF: Associação Nacional dos Delegados e Polícia Federal (ADPF), 2021. Disponível em https://web.adpf.org.br/noticia/adpf/adpf-divulga-resultado-de-concurso-de-artigos-cientificos-sobre-lgpd-criminal/. Acesso em: 20 jun. 2021.

ZAMPRONHA, Luís Flavio. A Ciência da Informação e a atividade policial: uma aproximação necessária. Em E.B. ALVAREZ, B. T. ALONSO, P. C. SILVEIRA (Eds.). *In*: ALVAREZ, E.B.; ALONSO, B. T.; SILVEIRA, P. C. (ed.). **Ciência da Informação e Ciências Policiais**: **Conexões e Experiências**. Vol. 4. Tallinn, Estonia: Pro-Metrics, 2023a.

ZAMPRONHA, Luís Flávio. Inovação na Polícia Judiciária: novos produtos para uma nova estratégia. *In*: ALVAREZ, E.B.; ALONSO, B. T.; SILVEIRA, P. C. (ed.). **Ciência da Informação e Ciências Policiais**: **Conexões e Experiências**. Vol. 4. Tallinn, Estonia: Pro-Metrics, 2023b.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância – A luta por um futuro humano na nova fronteira do pode**r. Rio de Janeiro: Intrínseca, 2021.