UNIVERSIDADE ESTADUAL DE LONDRINA

VINICIUS CHELIGA

CIDADES INTELIGENTES:

IMPLEMENTAÇÃO, RESPONSABILIDADE E PROTEÇÃO DE DADOS PESSOAIS

Londrina
2022

VINICIUS CHELIGA

CIDADES INTELIGENTES:
IMPLEMENTAÇÃO, RESPONSABILIDADE E PROTEÇÃO DE DADOS PESSOAIS

Dissertação apresentada ao Programa de Pós-Graduação em Direito Negocial da Universidade Estadual de Londrina-UEL, como requisito parcial à obtenção do título de Mestre.

Orientador: Prof. Dr. Tarcísio Teixeira

Londrina
2022

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática do Sistema de Bibliotecas da UEL

CHELIGA, VINICIUS.
Cidades inteligentes : Implementação, responsabilidade e proteção de dados pessoais / VINICIUS CHELIGA. - Londrina, 2022.
116 f.

Orientador: Tarcísio Teixeira.
Dissertação (Mestrado em Direito Negocial) - Universidade Estadual de Londrina, Centro de Estudos Sociais Aplicados, Programa de Pós-Graduação em Direito Negocial, 2022.
Inclui bibliografia.

1. cidades inteligentes - Tese. 2. proteção de dados - Tese. 3. privacidade - Tese. 4. responsabilidade civil - Tese. I. Teixeira, Tarcísio . II. Universidade Estadual de Londrina. Centro de Estudos Sociais Aplicados. Programa de Pós-Graduação em Direito Negocial. III. Título.

CDU 34

VINICIUS CHELIGA

CIDADES INTELIGENTES:
IMPLEMENTAÇÃO, RESPONSABILIDADE E PROTEÇÃO DE DADOS PESSOAIS

Dissertação apresentada ao Programa de Pós-Graduação em Direito Negocial da Universidade Estadual de Londrina-UEL, como requisito parcial à obtenção do título de Mestre.

BANCA EXAMINADORA

_____
Orientador: Prof. Dr. Tarcísio Teixeira
Universidade Estadual de Londrina – UEL

_____
Prof. Dr. Miguel Etinger de Araujo Junior
Universidade Estadual de Londrina – UEL

_____
Profa. Dra. Renata Capriolli Zocatelli Queiroz
Universidade Estadual de Londrina – UEL

Londrina, 29 de novembro de 2022

AGRADECIMENTOS

Ao Prof. Dr. Tarcísio Teixeira, meu orientador e amigo de todas as horas, que me acompanhou nas inúmeras dificuldades que a pandemia trouxe, tendo o zelo e a paciência necessários para se chegar neste texto.

Aos professores que contribuíram com o seu conhecimento em todas as disciplinas feitas, principalmente para aqueles que também tiveram a paciência e o amor necessário para ensinar e auxiliar em um tempo tão difícil.

Agradeço à Universidade Estadual de Londrina, lugar que amo, e agradeço a Deus pela graduação e pelo mestrado feito aqui. Acrescento com muito carinho o agradecimento a todos os funcionários, colegas de turma, professores e amigos que consegui por meio dessa instituição.

Agradeço também o imenso apoio da minha família, principalmente nos momentos em que estive doente e cuidaram de mim. Agradeço a minha namorada, aos amigos de casa e a todos que me apoiaram nesse tempo.

Ao Prof. Danilo Doneda, *in memoriam*, que esteve presente como referência desde o primeiro projeto.

Por fim, glorifico a Deus por tudo o que foi alcançado e por todo o aprendizado desse tempo.

“A verdadeira sabedoria, fruto da reflexão, do diálogo e do encontro generoso entre as pessoas, não se adquire com uma mera acumulação de dados, que, numa espécie de poluição mental, acabam por saturar e confundir.”

(Papa Francisco)

CHELIGA, Vinicius. **Cidades Inteligentes:** Implementação, Responsabilidades e Proteção de Dados Pessoais. 116 f. Dissertação (Mestrado em Direito Negocial) - Universidade Estadual de Londrina, Londrina, 2022.

RESUMO

Observando o conjunto de proposições que interpretam o direito positivado, escopo do direito negocial, principalmente aquelas interpretações trazidas decorrentes das consequências das revoluções tecnológicas, temos hoje a instrumentalização de tecnologias para a construção de um ambiente que propicie uma maior qualidade de vida para todos os cidadãos. Assim, para a construção de uma cidade inteligente, através deste planejamento tecnológico, temos a geração, por agentes públicos e privados, de uma imensa quantidade de dados, os quais devem ser adequadamente tratados. Esses dados são normalmente geridos por uma cadeia de sujeitos, possuindo assim uma multiplicidade de agentes e do cruzamento de vários bancos de dados frutos de uma massiva coleta. Visto isto, este estudo objetiva demonstrar pontos primordiais a serem explorados para a construção de políticas e planos para estas cidades, a responsabilidade de cada um dos sujeitos envolvidos e como o direito negocial é a ferramenta primordial para a resolução de conflitos de responsabilidade, quando se trata do uso destes dados. Para determinar tais responsabilidades diante da complexidade de múltiplos agentes, foram utilizadas como base a Constituição Federal (BRASIL, 2022), a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018), o Código de Defesa do Consumidor (BRASIL, 1990), o Marco Civil da Internet (BRASIL, 2014), entre outras. Ainda mais, tecnologias embarcadas com sensores mais aprimorados, carros inteligentes, drones, inteligência artificial (IA), big data, dentre outros, causam grande impacto na construção de uma cidade. Assim, a pesquisa faz-se necessária em razão do surgimento de novas tecnologias e das suas consequências, com foco nas tecnologias destinadas à transformação urbana. Para tanto, foi realizado um levantamento sobre quais os itens fundamentais para construir uma cidade inteligente e quais os papeis entre os agentes públicos e privados; sobre o modo de coleta e de tratamento dos dados em ambos os casos; sobre os contratos de utilização dos recursos de uma cidade inteligente; e sobre a delimitação das responsabilidades em concordância com a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018) e com todo o ordenamento brasileiro. Como resultado, foram levantadas boas práticas para a construção de cidades inteligentes e do tratamento de dados pessoais em três grandes áreas de concentração: saúde, segurança pública e mobilidade urbana, além do uso de inteligências artificiais que tratam dados e da responsabilização de agentes de tratamento de dados.

Palavras-chave: cidades inteligentes; proteção de dados; privacidade; responsabilidade civil; responsabilidade proativa.

CHELIGA, Vinicius. **Smarts City:** Implementation, Responsabilites and Protection of Personal Data. 2022. 116 p. Master's Degree in Law – CESA, Universidade Estadual de Londrina, Londrina, 2022.

ABSTRACT

Observing the set of propositions that interpret positive law, the scope of business law, especially those interpretations brought as a result of the consequences of technological revolutions, today we have the instrumentalization of technologies for the construction of an environment that provides a better quality of life for all citizens. Thus, for the construction of a smart city, through this technological planning, we have the generation, by public and private agents, of an immense amount of data, which must be adequately treated. These data are usually managed by a chain of subjects, thus having a multiplicity of agents and the crossing of several databases resulting from a massive collection. Given this, this study aims to demonstrate key points to be explored for the construction of policies and plans for these cities, the responsibility of each of the subjects involved and how the negotiation law is the primordial tool for the resolution of conflicts of responsibility, when it comes to deals with the use of this data. To determine such responsibilities in the face of the complexity of multiple agents, the Federal Constitution (BRASIL, 2022), the General Law for the Protection of Personal Data (LGPD) (BRASIL, 2018), the Consumer Protection Code (BRASIL, 1990), the Civil Rights Framework for the Internet (BRASIL, 2014), among others. Even more, technologies embedded with more improved sensors, smart cars, drones, artificial intelligence (AI), big data, among others, have a great impact on the construction of a city. Thus, research is necessary due to the emergence of new technologies and their consequences, focusing on technologies aimed at urban transformation. For that, a survey was carried out on which are the fundamental items to build a smart city and which are the roles between public and private agents; on the method of data collection and processing in both cases; on contracts for the use of resources in a smart city; and on the delimitation of responsibilities in accordance with the General Law for the Protection of Personal Data (BRASIL, 2018) and with the entire Brazilian legal system. As a result, good practices were raised for the construction of smart cities and the processing of personal data in three major areas of concentration: health, public safety and urban mobility, in addition to the use of artificial intelligence that process data and the accountability of treatment agents.

Key-words: smart cities; data protection; privacy; responsibility in law; proactive responsibility.

LISTA DE ABREVIATURAS E SIGLAS

ABIN	Agência Brasileira de Inteligência
ADI	Ação Direta de Inconstitucionalidade
ANAC	Agência Nacional de Aviação Civil
ANPD	Autoridade Nacional de Proteção de Dados
CEDES	Centro de Estudos de Direito Econômico e Social
CGST	Coordenação-Geral de Segurança no Trânsito
DECEA	Departamento de Controle do Espaço Aéreo
DENATRAN	Departamento Nacional de Trânsito
IBGE	Instituto Brasileiro de Geografia e Estatística
INMETRO	Instituto Nacional de Metrologia, Qualidade e Tecnologia
LAPIN	Laboratório de Políticas Públicas e Internet
LGPD	Lei Geral de Proteção de Dados Pessoais
OCR	Optical Character Recognition (Reconhecimento ótico de caracteres)
PC do B	Partido Comunista do Brasil
PSB	Partido Socialista Brasileiro
PSDB	Partido da Social Democracia Brasileira
PSOL	Partido Socialismo e Liberdade
STF	Supremo Tribunal Federal

SUMÁRIO

INTRODUÇÃO

A construção e a implementação de cidades inteligentes despertam um olhar multidisciplinar a fim de alcançar sua efetividade: uma cidade que auxilie os cidadãos. Áreas como Direito – mais especificamente o Direito Ambiental e Urbanístico – e Engenharia Ambiental e Urbanística, voltadas à tecnologia e à infraestrutura, contribuem fortemente para a construção de uma cidade inteligente; sem ainda considerarmos o auxílio da iniciativa privada.

Perante o exposto, faz-se alguns questionamentos: em uma cidade com problemas de asfaltamento, seria interessante automatizar os meios de transporte a fim de localizá-los em tempo real para a facilidade dos passageiros? Ou seria melhor manter o foco dos investimentos em cobrir toda a malha asfáltica da cidade? Outros ainda discutem se realmente é necessário esse poder tecnológico dentro de uma cidade, acreditando que as tecnologias poderiam levar a um gasto de energia desnecessário e a um ataque ao meio ambiente.

Considerando esses dois argumentos contra o investimento tecnológico, dentro do primeiro capítulo será abordado o conceito de “cidade inteligente”, promovendo uma conceituação atual que visa colocar o cidadão como centro e motivo de construção da mesma e não somente o uso da tecnologia por ela mesma. A partir disso, são colocados exemplos que abraçam os conceitos de meio ambiente e de responsabilidade social. A partir desse cenário, as cidades inteligentes podem ser importantes ferramentas para efetivar o que está previsto na Constituição Federal (BRASIL, 2022) e nos planos diretores quanto ao bem-estar social efetivado nas cidades.

Ideias futurísticas, como aquelas propagadas pelo desenho animado *Jetsons* nos anos 60, aos poucos vão se concretizando e já é possível ver alguns exemplos, como os carros voadores, a comunicação por vídeo em todos os lugares, o uso extensivo da robótica, as roupas inteligentes etc.

Contudo, nesse avanço tecnológico, é importante destacar que se corre o risco de focar somente no avanço e nas inovações, e esquecer o sujeito final, aquele que faz o uso efetivo da tecnologia: as pessoas; principalmente nas áreas que dependem primordialmente desse progresso tecnológico, como as áreas de Computação Aplicada e Engenharias.

O segundo capítulo é destinado a discutir sobre a ideia de privacidade e proteção de dados pessoais. Neste capítulo começa-se a criar as convergências entre cidades inteligentes e de como a massiva coleta de dados pode interferir na privacidade e proteção de dados. O difícil entendimento sobre privacidade e também o conceito de proteção de dados pessoais em solo brasileiro, em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) se fazem necessárias para a compreensão do restante desta obra. Em todo o processo tecnológico, deve-se pensar na ética da construção das soluções e no *privacy by design,* respeitando desde o início, o direito sobre a proteção de dados dos cidadãos.

A partir desse apontamento, três áreas de concentração foram escolhidas como os maiores campos de estudo: a segurança pública, a saúde e a mobilidade urbana.

O terceiro capítulo trata da segurança pública e de como deve ser enfrentado o estado autoritário tecnológico, para que não tenha um vigilantismo que retire a qualidade de vida e a privacidade dos cidadãos.

Já o quarto capítulo tem o seu núcleo a área da saúde, com a necessidade de se verificar a classificação dos dados ali presentes, em sua maioria, classificados como “dados sensíveis”, tendo assim o dever de receber cuidados maiores com o seu manuseio a fim de que não ocorra discriminações inaceitáveis e contrárias a legislação brasileira em caso de um incidente.

Dentro do quinto capítulo é abordado o tema da mobilidade urbana, levando em consideração a análise de dados de tráfego urbano, e a troca de dados entre estruturas da cidade com titulares de bens, como carros, motos e drones e da necessidade de um sólido planejamento também relacionado aos dados produzidos ali.

Após vistas estas três áreas de concentração, o sexto capítulo trata da inteligência artificial, do seu uso dentro de cidades inteligentes e qual o seu impacto diante da massiva coleta e do tratamento de dados pessoais, inclusive desta se há a necessidade de um órgão estatal que trabalhe exclusivamente com a evolução tecnológica e o seu impacto na sociedade.

Por fim, perante todo o exposto, tem-se como objeto principal deste estudo, contido dentro do capítulo sétimo, a responsabilidade civil dentro das cidades inteligentes sob três pontos de vista: do agente estatal, das regras de consumo e da regra geral prevista na LGPD (BRASIL, 2018).

Utilizou-se nesta pesquisa o método dedutivo, por meio do qual foi possível partir de argumentos gerais, como a evolução da tecnologia, o seu impacto nas cidades e o respeito ao tratamento de dados dos cidadãos, vinculando, assim, as conclusões deste trabalho ao que foi construído logicamente nas premissas estabelecidas em conformidade com a lei. Ademais, por meio dessa metodologia, também foi possível identificar o estado atual da ciência em estudo, do ponto de vista jurídico e, em determinadas situações, do ponto de vista tecnológico.

Também aqui foi aplicado o método indutivo, a fim de criar um arcabouço geral de conhecimento sobre o tema e estabelecer premissas gerais, ao analisar as soluções encontradas dentro das cidades inteligentes, principalmente as relacionadas com a proteção e a privacidade de dados.

1 CIDADES INTELIGENTES

Antes de adentrar no tema das cidades inteligentes, e para melhor entender o descrito, é preciso diferenciar o conceito de cidade e o conceito de município. Neste estudo, deve ser considerado como “cidade” o perímetro urbano delimitado dentro de um munícipio onde se possui uma mínima infraestrutura, como segurança, saúde, moradia e educação, e é designado pelo poder municipal. Já o “município” pode ser conceituado como o espaço territorial e político dentro de um estado, administrado por uma prefeitura e que pode compreender tanto as áreas urbanas quanto as áreas rurais.

Para iniciarmos a problemática da construção de cidades inteligentes, levando em consideração o aspecto da proteção de dados pessoais, é preciso conceituá-la e entendê-la, a partir de sua evolução em relação a uma cidade clássica. A diferença entre elas é o uso de tecnologias; retira-se a cidade de um papel passivo, em que é tida apenas como um espaço de moradia e proteção para os moradores, e a evolui para uma função diferente: uma cidade que passa a responder através da tecnologia, coletando os dados das pessoas, dos sensores, do clima e das rotas, fornecendo-os para os cidadãos e governantes, obtendo-se melhores respostas da situação atual e auxiliando na tomada de decisões.

De acordo com o CEDES (JUNIOR; AMIM; BRAIDE, 2021, p. 21), o conceito de cidades inteligentes é visto desta maneira:

> Cidade inteligente é o espaço urbano orientado para o investimento em capital humano e social, o desenvolvimento econômico sustentável e o uso de tecnologias disponíveis para aprimorar e interconectar os serviços e a infraestrutura das cidades, de modo inclusivo, participativo, transparente e inovador, com foco na elevação da qualidade de vida e do bem-estar dos cidadãos.

Já a Carta Brasileira de Cidades Inteligentes (BRASIL, 2021, p. 28-29) apresenta o seguinte conceito:

> Cidades Inteligentes são cidades comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural, que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas,

> garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação.

Em vista dessas duas conceituações, percebe-se que, no início, a tecnologia estava no centro da ideia de cidades inteligentes, contudo, hoje, o bem-estar, o meio ambiente e os parâmetros não tecnológicos estão no cerne da discussão. Ainda assim, para se alcançar tais elementos, é preciso um grande fator tecnológico.

A cidade inteligente, em sua natureza, tem como um dos princípios um grande escalonar de tecnologia, desde um simples *QR Code* em uma estátua da cidade para conhecer a história da obra, até semáforos inteligentes e carros autônomos que auxiliam na locomoção. Áreas como saneamento, educação, cultura, esportes, mobilidade urbana, segurança, entre outras, são impactadas pela coleta de dados para uma resposta mais assertiva quanto ao que fazer diante dos problemas urbanos.

Um dos obstáculos verificados dentro desse escalonamento tecnológico para suprir as demandas de uma cidade inteligente, é a coleta massiva de dados, inclusive pessoais. Diante disso, é preciso estabelecer quem são os titulares dos dados e os seus direitos, respeitando a finalidade da coleta a fim de que os dados não necessários sejam eliminados, inclusive em ambientes públicos.

1.1 Um Olhar à Constituição Federal em Relação às Cidades Inteligentes

O constituinte quis que houvesse uma Constituição Federal dirigente, com nortes e objetivos claros para que o poder público pudesse agir. É importante recordar que dentro desse conjunto de leis fundamentais, o município é colocado como um dos entes do pacto federativo no primeiro artigo:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito (BRASIL, 2022, s.p.)

Portanto, o conteúdo descrito e os objetivos dentro da Constituição Federal também valem para os municípios. Um dos dispositivos mais importantes retratados no documento é a previsão do seu artigo 3º, que trata de seus objetivos,

mais especificamente, o seu inciso III, que trata de “erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais” (BRASIL, 2022, s.p.). Apoiando-se em Sarlet, Marinoni e Mitidieto (2020, p. 307), é bem claro que o poder público deve estar envolvido na luta contra essas condições sociais adversas:

> Dito de outro modo, embora não se possa, em regra, admitir um direito subjetivo a erradicação da pobreza atribuído a algum indivíduo em particular (o que não afasta um direito fundamental ao mínimo existencial do indivíduo, ou mesmo de um direito a assistência social), os Poderes Públicos estão positivamente vinculados a encetar passos concretos, na esfera de suas competências e atribuições, na direção da realização dos objetivos constitucionalmente estabelecidos, ainda que a CF não disponha exatamente sobre os modos de realização de tais objetivos.

Tratando-se do Poder Público, e ainda entendendo que o município participa do pacto federativo, percebe-se que os órgãos do poder municipal também estão comprometidos no combate às desigualdades regionais, inclusive internamente. Ao se envolver nas lutas não somente regionais, mas também contra a desigualdade social, a pobreza e a marginalização, é possível agraciar bairros periféricos com a construção de cidades inteligentes a partir do avanço da tecnologia atrelada a políticas públicas.

Ainda, diante do exposto, é importante ressaltar que quando o município isenta-se da responsabilidade de combater a desigualdade regional dentro de uma cidade, pode-se configurar como uma postura inconstitucional, como Sarlet, Marinoni e Mitidiero (2020, p. 308) afirmam:

> Assim, verifica-se que os objetivos fundamentais também implicam a adoção, pelos órgãos estatais, aqui com destaque para os Poderes Legislativo e Executivo, de um conjunto de políticas de Estado e de Governo que busquem realizar tais objetivos, pena de desvio de finalidade ou omissão total ou parcial, a depender do caso, cabendo ao Poder Judiciário, no âmbito de suas limitações, uma intervenção indutiva e/ou corretiva.

Portanto, cabe ao município efetivar esse combate, inclusive, implementando políticas que favoreçam a construção de cidades inteligentes em lugares mais afastados.

1.2 Construção de uma Cidade Inteligente

Como visto anteriormente, é de responsabilidade do município atender as necessidades não somente dos locais onde a renda *per capita* é maior, mas também dos outros lugares onde a média salarial é menor. Ainda mais, com a bairrização (processo em que o bairro se torna autossustentável, podendo causar uma grande valorização em comparação a outros locais da cidade), o poder público deve efetivar políticas em lugares onde se é possível verificar uma maior precariedade no acesso a serviços e a melhores condições de qualidade de vida. É preciso sempre observar a efetivação do pacto federativo, o qual ao trazer mais benefícios aos moradores promove a satisfação de residir nesses bairros, estimulando um sentimento de pertença e o investimento no comércio, consequentemente, aprimorando a qualidade de vida nessas regiões.

Contudo, essa não é a única pauta que precisa ser discutida. É preciso pensar também na sustentabilidade urbana, pois a garantia de melhorias no estilo de vida das pessoas depende do olhar sustentável sobre o ambiente. O Centro de Estudos e Debates Estratégicos (JUNIOR; AMIM; BRAIDE; CATHEDRAL, 2021, p. 95) coloca da seguinte maneira a sustentabilidade urbana:

> A sustentabilidade urbana requer que o crescimento populacional seja absorvido de forma a provocar menos impacto ambiental, e que a cidade seja pensada de modo que as moradias, os espaços públicos e os espaços privados permitam e incentivem o convívio e as relações interpessoais. O uso sustentável do ambiente urbano depende de um sentimento de pertencimento do homem em relação a seu espaço. Logo, o espaço urbano precisa ser pensado para as pessoas, na escala humana.
> Um dos pontos mais debatidos no assunto é o uso que se faz da cidade, ou seja, a utilização dos espaços e do território: como e para o quê é feita a sua ocupação. Há um certo consenso de que a diversificação do uso dos espaços dentro de uma mesma zona está intimamente ligada à sustentabilidade. Isso porque se o planejamento urbano priorizar certos modelos de ocupação, e se tivermos as funções principais do espaço urbano, tais como moradia, serviços, educação, trabalho e lazer, concentradas em algumas zonas, acredita-se que haverá mais qualidade de vida. Assim, tanto a mobilidade urbana quanto a acessibilidade são mais eficientes e efetivas, e a cidade, no que lhe diz respeito, tende a ser mais segura, uma vez que ela é verdadeiramente ocupada pelos seus moradores, o que leva a um maior cuidado dela pela própria população que a habita.

Pode parecer absurdo a ideia de cidades inteligentes dentro de bairros mais afastados ou mais pobres, levando em consideração a falta de itens básicos como, por exemplo, asfalto e esgoto. Mas é nesse ponto que reside a relação

com a sustentabilidade: aproveitar o investimento em itens básicos acrescentando elementos que agregam valor e dão às cidades o poder de retorno de informações, que são essenciais para a população em si e também para a construção de políticas públicas específicas.

Uma das aplicações dessa associação do que é básico com aquilo que é avançado na construção de uma cidade inteligente, é a logística para que um bairro não receba simplesmente um asfalto novo, mas que ao mesmo tempo se estruture faixas, semáforos, ciclovias, transporte público e todo um modelo de mobilidade urbana que torne o processo de construção desse bairro mais sustentável.

Nesse cenário, os meios tecnológicos podem verificar quais são as ruas onde possuem os maiores índices de circulação dentro dessas localidades, a fim de construir novas rotas dentro do transporte urbano, seja ele público ou privado, além de planejar toda uma iluminação específica que traga mais segurança aos cidadãos ao circularem por esses locais em horários noturnos e de pouco movimentação. É importante reforçar que a inteligência construída por equipamentos e algoritmos sempre evolui, trazendo inovações e levando a novas implementações com o tempo. Diante dessa perspectiva, uma cidade inteligente é uma cidade viva que sabe se adaptar.

Outros diferenciais que podem ser agregados são a implementação de políticas públicas de saneamento básico, de coleta seletiva de lixo e de planos de reciclagem, concomitantes à implementação de sensores para verificar a qualidade da água e, por meio da pesquisa inteligente, investigar se há algo que pode ser melhorado em relação à alimentação e à saúde. Ademais, o investimento tecnológico em áreas de lazer pode agregar também valores positivos aos bairros garantindo a seus moradores um senso de pertencimento e orgulho.

Portanto, a bairrização não deveria ser vista com um olhar de desprezo, tendo em vista que também deve haver investimentos nesses lugares menos favorecidos atualmente. Segundo Junior, Amim, Braide e Cathedral (2021, p. 78), em relação à estruturação física e tecnológica de um lugar, deve-se pensar que:

> A coleta e o uso de informações, portanto, só faz sentido se for utilizada para algum benefício aos cidadãos, de modo que exista uma resposta às suas demandas e necessidades. Deve-se entender que, se por um lado há o agente “decisório”, na outra ponta há os equipamentos. Uso de tecnologias inteligentes e sensitivas finalísticos, os “atuadores”. Um semáforo inteligente, um poste inteligente, um chat bot ou um carro autônomo são exemplos de

> atuadores que só são viáveis pela combinação de coleta de grandes volumes de dados com o uso, ou não, de inteligência artificial para seu tratamento e uma resposta adequada, de acordo com condições e objetivos definidos, finalidades estas que podem atender a lógicas comerciais ou governamentais, mas que deveriam ser sempre em benefício do cidadão.

Assim, pensando nas demandas dos moradores desses bairros, considera-se a construção de cidades inteligentes a fim de garantir, por meio de políticas públicas juntamente com investimentos certeiros, um lugar melhor para toda a população.

1.3 Tecnologia Como Fator Fundamental para Cidades Inteligentes

Neste tópico, disserta-se sobre um fator primordial para a construção de cidades inteligentes que é a tecnologia. Primeiramente, é preciso compreender que o conceito de “inteligente” deve refletir o quanto a tecnologia impacta a construção dessas cidades. Em contrapartida, oposto ao termo “inteligente”, ressalta-se o conceito em inglês *dumb*, que pode significar burro, mudo ou estúpido, mas, de maneira menos ofensiva, a melhor tradução seria “não-inteligente”.

Para elucidar melhor o seu conceito dentro desta discussão, tem-se, por exemplo, uma cafeteira, que pode ser inteligente, ligada a um aplicativo, e abastecida de acordo com a rotina da casa, fazendo o café no tempo correto; ou ela pode ser não-inteligente, ou seja, não tem qualquer conexão e o morador é obrigado a colocá-la no fogão, esquentar a água e preparar o pó para fazer o seu café.

Observa-se que das duas maneiras é possível chegar ao resultado final, o café pronto, mas um dos modos exigiu apenas que um aplicativo configurado com inteligência artificial aprendesse a rotina da casa para preparar o café, e o outro exigiu tempo e esforço do morador para alcançar seu objetivo.

Assim, a tecnologia é um fator de otimização e ao transpor o seu efeito ao nível das cidades, ela é utilizada a fim de diminuir o esforço e o tempo dos agentes públicos e dos cidadãos, somados à redução de custos para se atingir uma meta.

Nesta quarta revolução industrial em que se vive atualmente, as cidades têm o poder de responder por meio de tecnologias, utilizando-se de dados que condicionam a tomada de decisão pelos próprios sistemas tecnológicos

(tecnologias embarcadas com inteligência artificial) ou auxiliam um agente na resolução de ações.

Vale constar também dois fenômenos importantes dentro dessa revolução, quando se trata de cidades inteligentes: miniaturização e barateamento de tecnologias. Na primeira, o uso de grandes equipamentos para executar uma tarefa não é mais necessário, dessa forma, a tecnologia passa a ser um fator mais orgânico e adaptável dentro de um centro urbano. Já com o barateamento das tecnologias, é possível expandir o seu uso e aprimorar a busca pela qualidade de vida de todos os cidadãos.

Apesar dos vários benefícios gerados a partir da tecnologia, não se pode cair na visão romântica que ela por si só se configura como a resolução de todos os problemas e deve ser implementada a qualquer custo em uma cidade. Todas as tecnologias possuem impactos bons e ruins que devem ser estudados.

A esse respeito, o Centro de Estudos e Debates Estratégicos da Câmara dos Deputados assim considera as consequências negativas em cidades inteligentes:

> Como a tecnologia tem a função de resolver problemas, as consequências negativas são, quase sempre, não intencionais, uma espécie de efeito colateral. Mas alguns desses efeitos daninhos são bastante profundos, podendo até suplantar os benefícios em alguns casos. Trazendo novamente o pensamento de Harari (2016), há uma série de desafios trazidos pela tecnologia para os próximos anos, o que torna praticamente impossível falar em tecnologia e não mencionar esses efeitos. Apenas para ilustrar a extensão dessas implicações, pode-se citar o impacto que os aplicativos de transporte compartilhado e outros relacionados à economia colaborativa trouxeram às relações de trabalho (JUNIOR; AMIM; BRAIDE; CATHEDRAL, 2021, p. 80).

Outro ponto de grande risco em relação à utilização de tecnologias para cidades inteligentes é a infraestrutura utilizada. Uma das preocupações é a falta de microprocessadores para atender a alta demanda tecnológica em carros, celulares, computadores, entre outros, presentes nas cidades inteligentes.

Observando o Projeto de Lei 3042/2021, que se tornaria a Lei Ordinária nº 14.302/22, auxiliando no incentivo do Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores (Padis), temos aqui uma grande preocupação no que diz respeito a falta de microprocessadores, inclusive no contexto dos automóveis atuais e futuros, que consequentemente impactam nos estudos sobre cidades inteligentes:

> Semicondutores estão em absolutamente tudo ao nosso redor. Exemplificativamente, dados da Associação Nacional dos Fabricantes de Veículos Automotores – ANFAVEA indicam que os veículos mais simples fabricados no Brasil já trazem cerca de 400 componentes semicondutores, ao passo que carros mais modernos empregam de 800 a 1000 chips, que são responsáveis por diversos sistemas de segurança, dirigibilidade, controle de manutenção, navegação assistida, entretenimento e rastreamento. O avanço tecnológico da indústria fará com que esse número cresça ainda mais, sobretudo com a adoção de veículos híbridos, elétricos e autoassistidos, que é um fenômeno crescente e irreversível.
> O momento vivido pelo mundo (e o cenário brasileiro não poderia ser diferente) justifica não apenas a manutenção, mas o fortalecimento de uma política robusta para semicondutores, a qual já se mostrou exitosa para a indústria e para o país, e que tem enorme potencial para catapultar a manufatura local para posição de destaque muito superior à que o Brasil, hoje, pode ostentar.
> A escassez mundial de chips é noticiada dia após dia nos mais diversos meios de comunicação. Indústrias de todos os setores vêm sendo impactadas pela falta de semicondutores, a ponto de se ver a redução (quando não a paralisação) de atividades de manufatura importantíssimas para a economia nacional, que terá reflexos relevantes nos curto e médio prazos nos preços de produtos, na inflação e no acesso da população aos mais diversos bens, de computadores a veículos, de bens da linha branca a telefones celulares (BRASIL, 2022, p. 6).

Diante desse cenário, cria-se a dependência de grandes empresas que podem subsidiar tais tecnologias; e não são muitas que possuem essa capacidade. Aqui ocorrem dois problemas: o primeiro é a caixa preta, criada ao se observar que o município não tem o poder de controlar totalmente o alto consumo de tecnologia, tornando-se totalmente dependente de contratos inflexíveis com terceiros para que seja respeitada a garantia de segurança e funcionamento.

Dentro da área de Engenharia de Software, o teste da caixa preta é assim nominado pois o usuário que irá testar o software somente tem controle da entrada de dados e consegue visualizar a saída destes dados em si, não conhecendo os processos que levaram a estes resultados. Sobre o teste de caixa preta, Pressman conceitua desta forma:

> O teste caixa-preta faz referência a testes realizados na interface do software. Um teste caixa-preta examina alguns aspectos fundamentais de um sistema, com pouca preocupação em relação à estrutura lógica interna do software. (PRESSMAN, 2011, p. 431).

Do ponto de vista problemático dentro de um município, podem ocorrer as mesmas situações: há o conhecimento de quais dados são coletados e qual a resposta dada a estes dados que foram coletados, mas não se sabe os cálculos feitos para se chegar a esta conclusão. A tecnologia é contratada e implementada,

mas a mão de obra não conhece o funcionamento e não consegue também dar os devidos reparos, ficando dependente do fabricante em eventuais falhas.

O segundo problema diz respeito à dificuldade em buscar outras empresas fornecedoras de tecnologia devido ao formato fechado que a maioria dos sistemas tecnológicos possuem. Assim, torna-se “refém” da instituição contratada a fim de dar continuidade às políticas públicas. Em resumo, há poucas empresas que possuem a capacidade de implementar as cidades inteligentes, e não há tecnologia nem capital intelectual suficiente para soluções internas.

Em nosso dia a dia, podemos visualizar tal situação na utilização de arquivos de formato fechado, como o *.docx da Microsoft em softwares para este fim diferentes do Microsoft Word, como O LibreOffice Writer, onde não há a total compatibilidade e ocorrem erros na visualização e utilização destes arquivos. Da mesma forma, em caso de necessidade, há aqui um problema de falta de compatibilidade entre equipamentos de fabricantes, caso não seja criado um padrão entre os fabricantes quanto as especificações dos equipamentos.

Diante desse embate, retoma-se o Centro de Estudos e Debates Estratégicos da Câmara dos Deputados que também reflete acerca desse ponto:

> Além disso, a imprescindibilidade cada vez maior da tecnologia para a vida em ambiente urbano, combinada com a concentração do desenvolvimento das soluções em um pequeno número de atores, leva a problemas de governança, dependência tecnológica e (sobre)simplificação dos problemas urbanos (MCNEILL, 2015). Essas externalidades devem ser consideradas tanto pelos cidadãos, como pela administração pública em suas necessárias reflexões sobre o uso das tecnologias. Tais ponderações, muitas das vezes imprecisas ou até inexistentes, devem ainda levar em consideração que, devido à aceleração dos ciclos inovativos, a obsolescência tecnológica tende a ocorrer também de maneira mais drástica, criando mais pressão sobre as finanças públicas e particulares (JUNIOR; AMIM; CRAIDE; CATHEDRAL, 2021, p. 82).

Por fim, analisando as questões tecnológicas, é preciso que toda a tecnologia dentro de uma cidade esteja acompanhada de uma previsão jurídica que dê embasamento a ela, buscando efetivar a finalidade de uma cidade inteligente. A partir dessa ponderação, Rech, Gullo e Scur (2019, p. 38) descrevem o Plano Diretor como um norte jurídico que deve auxiliar na implementação:

> A tecnologia deve diminuir as horas de trabalho e aumentar o tempo de lazer e convivência, mas não pode simplesmente ceifar os postos de trabalho, pois não haverá sustentabilidade, nem lazer nem conveniência, mas conflitos. O

> regramento inteligente de tudo isso é indispensável. [...] As cidades inteligentes apostam na inclusão compartilhada, em serviços públicos eficazes, que podem construir oportunidades de viver em uma sociedade ideal. A organização da cidade inteligente passa pelo Plano Diretor Inteligente, como instrumento jurídico de planejamento de cidades.

Em outras palavras, para se compreender melhor como efetivar uma cidade inteligente, é preciso entender o funcionamento de um Plano Diretor que conduzirá de forma organizada o planejamento idealizado.

1.4 PLANO DIRETOR DE UMA CIDADE INTELIGENTE

O Plano Diretor é a lei municipal que estrutura as políticas de uma cidade, dando os embasamentos necessários para o seu crescimento sadio, sempre respeitando os direitos fundamentais coletivos e individuais. Segundo o autor Araújo Júnior (2006, s.p.), pode-se defini-lo da seguinte maneira:

> Num primeiro momento pode-se definir o Plano Diretor como uma lei municipal, cuja elaboração está prevista na Constituição Federal de 1988, em seu artigo 182, § 1º, como sendo o instrumento básico da política de desenvolvimento e de expansão urbana.

O planejamento de uma cidade inteligente passa por um plano diretor responsável que consiga enxergar o macro, entendendo as demandas atuais e futuras, e a necessidade de crescimento. Mais uma vez, é preciso ressaltar que dentro do planejamento, a tecnologia nunca é um fim em si, mas um meio pelo qual os cidadãos possam ter uma melhora significativa em sua qualidade de vida. O Plano Diretor é uma obrigação constitucional dos municípios com mais de vinte mil habitantes, conforme o artigo 182:

> Art. 182. A política de desenvolvimento urbano, executada pelo Poder Público municipal, conforme diretrizes gerais fixadas em lei, tem por objetivo ordenar o pleno desenvolvimento das funções sociais da cidade e garantir o bem-estar de seus habitantes.
> § 1º O plano diretor, aprovado pela Câmara Municipal, obrigatório para cidades com mais de vinte mil habitantes, é o instrumento básico da política de desenvolvimento e de expansão urbana.
> § 2º A propriedade urbana cumpre sua função social quando atende às exigências fundamentais de ordenação da cidade expressas no plano diretor.
> § 3º As desapropriações de imóveis urbanos serão feitas com prévia e justa indenização em dinheiro.

> § 4º É facultado ao Poder Público municipal, mediante lei específica para área incluída no plano diretor, exigir, nos termos da lei federal, do proprietário do solo urbano não edificado, subutilizado ou não utilizado, que promova seu adequado aproveitamento, sob pena, sucessivamente, de:
> I - parcelamento ou edificação compulsórios;
> II - imposto sobre a propriedade predial e territorial urbana progressivo no tempo;
> III - desapropriação com pagamento mediante títulos da dívida pública de emissão previamente aprovada pelo Senado Federal, com prazo de resgate de até dez anos, em parcelas anuais, iguais e sucessivas, assegurados o valor real da indenização e os juros legais (BRASIL, 2022, s.p.).

Diante dessa obrigação, Araújo Júnior (2006) observa que antes mesmo da obrigatoriedade constitucional do Plano Diretor, este já era visto como um modelo de avanço urbano em busca de destaque arquitetônico entre os cidadãos, e de qualidade de vida. O autor define 4 (quatro) fases em relação à evolução dos planos diretores:

> A primeira, preocupada com o que chama de “desenho da cidade”, associada à ideia de estética urbana. A segunda, relacionada à distribuição das edificações sob a ótica econômica e arquitetônica. Num terceiro momento adota-se a ideia de um plano de desenvolvimento integrado, aplicando-se o conceito de planejamento, que integre vários setores da municipalidade. Uma Quarta etapa surge após a Constituição Federal de 1988 refletindo a ideia mencionada acima, constante do § 1º do art. 182 da Constituição Federal de 1988, voltada para a ordenação do pleno desenvolvimento das funções sociais da cidade e garantia do bem-estar da comunidade local (ARAÚJO JÚNIOR, 2006, s.p.).

Em uma análise técnica, pode-se considerar que atualmente a sociedade vive o avançar da quarta fase, em que a efetivação da função social da cidade, em conjunto com a garantida do bem-estar social passam pelo olhar tecnológico concomitantemente ao meio ambiente. É imprescindível entender que a concretização dessa realidade já deixou de ser apenas responsabilidade de engenheiros e de arquitetos, e hoje passam por uma grande multidisciplinaridade.

O recorte estabelecido neste trabalho se presta a observar o impacto do direito fundamental à privacidade e à proteção de dados dentro do gerenciamento de uma cidade, pautando-se nas ponderações de Araújo Júnior (2006, s.p.):

> O planejamento urbano deve então obedecer aos princípios constitucionais da dignidade da pessoa humana, inclusive garantindo-lhe o direito à moradia, a função social e o direito de propriedade, o meio ambiente ecologicamente equilibrado etc.

Embora atualmente já esteja na quarta etapa, relacionada à criação de planos diretores, é possível avaliar o projeto de cidades inteligentes a partir das fases anteriores, por meio de um olhar crítico social em busca dos melhores rumos para a efetivação do bem-estar comunitário.

A fase do “desenho da cidade” é primordial para o planejamento, deve-se levar em consideração todos os aspectos importantes, principalmente, a questão da qualidade de vida. É preciso planejar os lugares de lazer, de esporte, de moradia e as vias de acesso para chegar aos locais de forma rápida e segura; além do planejamento da saúde, da segurança e da educação.

Ademais, mas não menos importante, é preciso considerar e destacar, na construção de uma cidade, a cultura e a beleza. Ao acolher os mais diversos povos, deve-se respeitar os costumes e as tradições de cada grupo e colocar a beleza como um fator importante da cidade, trazendo satisfação e orgulho para aqueles que nela residem. SCRUTON (2013, p. 184), sobre a beleza, comenta:

> Nossa necessidade de beleza não é algo de que podemos prescindir sem que nos tornemos incapazes de nos contentar como pessoas. Ela é uma necessidade que surge de nossa condição metafísica de indivíduos livres que buscam seu lugar num mundo partilhado e público. Podemos vaguear alienados, ressentidos, desconfiados e receosos por este mundo ou podemos nos sentir à vontade nele, permanecendo em harmonia com os outros e com nós mesmos. A experiência da beleza nos orienta neste segundo caminho: ela nos revela que estamos à vontade no mundo, que o mundo está ordenado em nossas percepções como um lugar adequado à vida de seres como nós.

Além do mais, a busca pela beleza de uma cidade não se limita a sua qualidade meramente estética, mas envolve também o respeito ao meio ambiente, apostando em estratégias sustentáveis e ecológicas, como a arborização, que também é um sinônimo de beleza.

Ainda a exemplo da arborização, outro fator que reafirma a sua importância é a valorização imobiliária de locais mais arborizados ou próximos a esses espaços. Todos esses traços, culturais e arquitetônicos, valorizam a cidade e reforçam o sentimento de pertença dos cidadãos. Portanto, cidades inteligentes devem valorizar os traços da sociedade brasileira e fazer com que a tecnologia esteja presente de maneira orgânica dentro de diferentes realidades.

Dando continuidade, ao analisar a segunda fase, relacionada à distribuição das edificações sob a ótica econômica e arquitetônica, atualmente se tem

um fenômeno de bairrização, impulsionada principalmente pela pandemia e pelo trabalho remoto, onde casa e escritório se confundem. Esse fenômeno, que atingiu em especial as classes média e alta, modificou a forma de visualizar a cidade; já que não há o deslocamento até o trabalho, o bairro passou a ser o ponto mais importante para o cidadão.

No entanto, é crucial mencionar que com essa mudança de rotina, corre-se o risco de criar “bolhas” dentro das cidades, promovendo a falta de integração entre as pessoas de classes e culturas diferentes. Esse fechamento, até para a construção de cidades inteligentes, pode ser prejudicial, portanto, deve ser um fenômeno estudado e aprofundado com cuidado.

Na terceira fase, há uma análise mais ampla de como a cidade vai ser construída e se desenvolver. As duas primeiras fases podem ser vistas como etapas passivas, onde a criatividade, a carga de estudos e, principalmente, o conceito de uma cidade são primordialmente consideradas para a elaboração do planejamento. Já na terceira fase, inicia-se o estágio da tomada de decisão baseada em dados; é o momento em que as políticas públicas devem ser efetivadas, solucionando os problemas captados em número.

A essa altura, compreende-se que áreas como saúde, segurança, educação, lazer, saneamento básico, mobilidade urbana, entre outras não estão separadas, mas que cada uma delas contribui como um todo na construção da cidade.

Por fim, a quarta fase, determinada após 1988, com a Constituição Federal, a disposição de direitos ao cidadão e dos deveres do Estado. É a Constituição que determina quais são os deveres e as competências exclusivas e concorrentes que os municípios estão obrigados a contribuir e legislar como, por exemplo, a necessidade de um Plano Diretor.

É importante ainda recordar o foco deste trabalho, o qual se situa nessa quarta fase, e reflete sobre a efetivação da privacidade e da proteção de dados dentro das cidades, principalmente, no caso das cidades inteligentes.

O cumprimento dos direitos inscritos previstos pela Constituição Federal não pode ser aplicado de qualquer maneira. Ou seja, a segurança pública não pode ser exercida pura e simplesmente em um estado de vigilância; a saúde não pode ser efetivada em uma coleta massiva de dados sem o devido tratamento; a educação não pode ser ministrada cerceando as liberdades e retirando o conceito de privacidade; a mobilidade urbana não pode ser um sinônimo de rastreio em tempo real

de cada um dos cidadãos; e o saneamento básico não pode ser efetivado a partir de uma invasão à privacidade. A garantia da qualidade de vida não pode custar a liberdade e a privacidade dos cidadãos.

Um Plano Diretor inteligente cumpre sua função quando efetiva os direitos coletivos, levando em consideração os direitos individuais, colocando-os em um mesmo patamar e resolvendo da melhor forma possível os conflitos entre as partes. Assim, deve-se ter cuidado em relação à postura do Poder Público diante das exigências sobre as cidades inteligentes:

> Portanto, se isso impõe um reordenamento do direito urbanístico, com mudanças a postura da cidadania, com avanço para um Poder Público Municipal mais profissional, dotado de servidores técnicos, qualificados, capazes de superar a gestão burocrática, por uma gestão científica, inteligente, o planejamento exige cada vez mais normas de direito inteligente (RECH; GULLO; SCUR, 2019, p. 38).

Perante o exposto, encontra-se um grande problema dentro da administração de uma cidade, onde um sistema enrijecido pode não acompanhar as inovações, tornando-se ineficaz para os cidadãos. Felizmente, existem programas de fomento à resolução de problemas sociais e linhas de financiamento, os quais podem contribuir nesse tipo de situação.

Portanto, para a implementação de cidades inteligentes é necessário um avanço no poder executivo e legislativo do município, por meio de uma legislação e de um Plano Diretor bem fundamentado, que considere os princípios tecnológicos, inovadores, sociais e ambientais, a fim de que nas orientações legais e em outras resoluções municipais, tanto empresas públicas quanto parcerias público-privadas e iniciativas privadas atuem em prol do progresso social, conforme o descrito no capitulo III do Estatuto das Cidades (Lei Nº 10.257/01):

> Art. 39. A propriedade urbana cumpre sua função social quando atende às exigências fundamentais de ordenação da cidade expressas no plano diretor, assegurando o atendimento das necessidades dos cidadãos quanto à qualidade de vida, à justiça social e ao desenvolvimento das atividades econômicas, respeitadas as diretrizes previstas no art. 2o desta Lei.
> Art. 40. O plano diretor, aprovado por lei municipal, é o instrumento básico da política de desenvolvimento e expansão urbana.
> § 1o O plano diretor é parte integrante do processo de planejamento municipal, devendo o plano plurianual, as diretrizes orçamentárias e o orçamento anual incorporar as diretrizes e as prioridades nele contidas.
> § 2o O plano diretor deverá englobar o território do Município como um todo.
> § 3o A lei que instituir o plano diretor deverá ser revista, pelo menos, a cada dez anos.

> § 4o No processo de elaboração do plano diretor e na fiscalização de sua implementação, os Poderes Legislativo e Executivo municipais garantirão:
> I – a promoção de audiências públicas e debates com a participação da população e de associações representativas dos vários segmentos da comunidade;
> II – a publicidade quanto aos documentos e informações produzidos;
> III – o acesso de qualquer interessado aos documentos e informações produzidos. (Brasil, 2022, s.p.).

O Plano Diretor portanto, embasado no Estatuto das Cidades, é o alicerce fundamental para o avanço de uma cidade inteligente.

2 PRIVACIDADE E PROTEÇÃO DE DADOS

Tornar inteligente as cidades, faz parte da busca pelo bem-estar social, mas os direitos fundamentais, como privacidade e proteção de dados, não devem ser deixados de lado. Entender os seus pressupostos e implementá-los faz-se necessário em uma época em que dados pessoais valem ouro e o vigilantismo cresce.

Além disso, com a positivação desses direitos na Constituição Federal e a entrada em vigor da Lei Geral de Proteção Dados (LGPD), criou-se um momento favorável para a discussão dos efeitos do uso de dados, assim como, para a reflexão acerca de conceitos como a autodeterminação informativa e o empoderamento do titular quanto aos seus cuidados.

Esse “clima” de discussão sobre como os dados das pessoas são manuseados, vem crescendo tanto na iniciativa pública quanto privada, e é necessária para o entendimento da situação e, principalmente, para a sua aplicação.

2.1 PRIVACIDADE

Conceituar privacidade é um dos pontos dos mais complicados de se reunir em poucas palavras, visto a evolução e os diferentes conceitos adotados em diferentes épocas sobre o tema. Sobre privacidade, Doneda (2019, p.29) comenta assim a sua conceituação:

> É própria do nosso tempo a preocupação com a privacidade e como garanti-la. E a forma pela qual o direito a abordou durante muito tempo foi pela sua associação à busca de alguma forma de isolamento, refúgio ou segredo. A formação do conceito de privacidade, no entanto, aponta para elementos referentes a necessidades diversas, como a busca da igualdade, da liberdade de escolha, do anseio em não ser discriminado, entre outros. E, ainda, a privacidade está fortemente ligada à personalidade e ao seu desenvolvimento, para o qual é elemento essencial, em uma complexa teia de relações ainda a ser completamente vislumbrada pelo direito.
> Eventualmente, ocorre que nos encontremos em um dos momentos em que se verifica uma certa defasagem entre a carga semântica de um conceito e o que ele efetivamente representa. E é o exame dessa “defasagem” o ponto de partida que tomamos para verificar como a noção de privacidade se formou e, posteriormente, plasmou-se com outros elementos de forma a dar origem à proteção de dados pessoais.
> A noção de privacidade, em si, não é recente – com os diversos sentidos que apresenta, pode ser identificada nas mais variadas épocas e sociedades. Porém, a privacidade começou a ser concretamente abordada pelo

> ordenamento jurídico somente no final do século XIX para, enfim, assumir as suas feições atuais apenas muito recentemente.
>
> Praticamente não havia lugar para a tutela jurídica da privacidade em sociedades nas quais as condutas humanas estavam condicionadas a outra ordem de mecanismos – fosse uma rígida hierarquia social ou então uma determinada arquitetura dos espaços públicos e privados; fosse porque eventuais pretensões a esse respeito fossem neutralizadas por um ordenamento jurídico de caráter corporativo e patrimonialista; fosse, então, em determinadas sociedades nas quais a privacidade representasse não mais que um sentimento subjetivo que não poderia nem deveria ser tutelado. O despertar do direito para a privacidade ocorreu justamente num período em que muda a percepção da pessoa humana pelo ordenamento e ao qual se seguiu a juridificação de vários aspectos de sua vida cotidiana.

Em termos mais práticos, poderíamos adotar que a privacidade em si seria o direito de separar aquilo que a esfera pública da privada, e de escolher com autonomia com quem compartilhá-la. O desenvolvimento da personalidade de cada ser depende desse “direito de separar”, pois, em suma, os acertos e os erros cometidos por um sujeito dependem de um ambiente controlado, em que se há a confiança em poder errar, expressar ideias de maneira clara, escolher as pessoas certas etc.

Trata-se de um fenômeno em que o indivíduo demonstra tudo aquilo que guarda para si e não quer expor, como um histórico de doenças, uma situação embaraçosa, os motivos de um término de relacionamento etc. Por isso, em uma comparação banal, o fenômeno da privacidade é uma manifestação tão íntima que poderia ser classificada como algo pior que a nudez pública.

Pode ser observado nas amizades, visto que as pessoas selecionam os amigos para quem contar cada fato pessoal. Separa-se muitas vezes por camadas e por áreas, como trabalho, universidade, família etc., e há a liberdade de distinguir se determinado grupo vai ou não saber daquilo que ocorre em outro grupo.

Contudo o fenômeno da privacidade não se restringe às relações sociais, ele está presente também em lugares: a casa funciona como um guardião e uma espécie de espelho da personalidade e individualidade de cada pessoa; o carro pode guardar muitas informações e objetos pessoais; a mesa do escritório pode guardar um exame ou um atestado médico, entre outros casos.

Atualmente, todas essas realidades também precisam ser observadas no meio virtual. É importante compreender que no ambiente digital, essa privacidade é tão necessária para o desenvolvimento humano quanto na vida off-line.

Portanto, a privacidade é sem dúvidas algo que precisa ser defendido, principalmente, diante da postura antiética de disponibilizar publicamente conversas, fotos, documentos digitalizados etc. Embora haja posturas diferentes quanto a esse assunto, é inegável a necessidade de cuidados no que concerne ao uso de dados.

2.1.1 A Privacidade como Direito Fundamental

Sendo a privacidade um bem tão caro e importante, dentro do ordenamento brasileiro, ela está em alguns pontos do rol de direitos fundamentais. O primeiro ponto discute sobre o conceito amplo da dignidade da pessoa humana, conforme o artigo 1º da Constituição Federal, em seu inciso III (BRASIL, 2022). A partir dessa concepção, é possível afirmar que, dentro do quebra-cabeça da dignidade da pessoa humana, uma das peças diz respeito à privacidade e ao livre direito de escolha. Segundo SARLET, MARINONI e MITIDIERO (2020, p. 276):

> A dignidade da pessoa humana, nessa quadra, revela particular importância prática a partir da constatação de que ela (a dignidade da pessoa humana) é simultaneamente limite e tarefa dos poderes estatais e da comunidade em geral (portanto, de todos e de cada um), condição que também aponta para uma paralela e conexa dimensão defensiva (negativa) ou prestacional (positiva) da dignidade. Com efeito, verifica-se que na sua atuação como limite, a dignidade implica não apenas que a pessoa não pode ser reduzida à condição de mero objeto da ação própria e de terceiros, mas também o fato de que a dignidade constitui o fundamento e conteúdo de direitos fundamentais (negativos) contra atos que a violem ou a exponham a ameaças e riscos, no sentido de posições subjetivas que têm por objeto a não intervenção por parte do Estado e de terceiros no âmbito de proteção da dignidade. Como tarefa o reconhecimento jurídico-constitucional da dignidade da pessoa humana implica deveres concretos de tutela por parte dos órgãos estatais, no sentido de proteger a dignidade de todos, assegurando-lhe também por meio de medidas positivas (prestações) o devido respeito e promoção, sem prejuízo da existência de deveres fundamentais da pessoa humana para com o Estado e os seus semelhantes.

Continuando nessa via, deve-se refletir sobre o artigo 5º, especificamente, o descrito em seu inciso X:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 2022, s.p.).

Conforme reforçado, a privacidade é um bem inviolável, isto é, não deve ser forçado ou rompido; por conseguinte, é preciso ter um zelo e um cuidado especial, em especial, nos meios digitais. Essa inviolabilidade exige que o indivíduo que fornecer qualquer informação ou abrir alguma porta, esteja totalmente de acordo e ciente da ação tomada.

José Afonso da Silva, sobre esse direito fundamental, descreve:

> A tutela constitucional visa proteger as pessoas de dois atentados particulares: (a) ao segredo da vida privada; e (b) à liberdade da vida privada. O segredo da vida privada é condição de expansão da personalidade. Para tanto, é indispensável que a pessoa tenha ampla liberdade de realizar sua vida privada, sem perturbação de terceiros. São duas variedades principais de atentados ao segredo da vida privada, nota Kayser: a divulgação, ou seja, o fato de levar ao conhecimento do público, ou a pelo menos de um número indeterminado de pessoas, os eventos relevantes da vida pessoal e familiar; a investigação, isto é, a pesquisa de acontecimentos referentes à vida pessoal e familiar; envolve-se aí também a proteção contra a conservação de documento relativo à pessoa, quando tenha sido obtido por meios ilícitos. O autor ressalta o fato hoje notório de que o segredo da vida privada é cada vez mais ameaçado por investigações e divulgações ilegítimas por aparelhos registradores de imagem, sons e dados, infinitamente sensíveis aos olhos e ouvidos (SILVA, 1998, p. 211).

Há aqui uma clara preocupação do autor, principalmente, quanto aos dados, às imagens, aos sons e aos vídeos. Contudo, com o avançar tecnológico, além desses elementos, algo que deve ser levado em conta também são os metadados e os dados de pesquisa, que podem invadir ainda mais a privacidade, sem o conhecimento do usuário.

2.2 Proteção de Dados

Antes de adentrarmos no tema deste tópico, é preciso diferenciar a “privacidade” da “proteção de dados”. A grande diferença entre os dois conceitos deve ser vista sob dois aspectos: o da segurança da informação e o filosófico.

Do ponto de vista da segurança da informação, há um tripé composto pela disponibilidade, integridade e confidencialidade; e a privacidade estaria integrada no princípio da confidencialidade, mas sem excluir as outras opções. É nele que se define aquilo que é secreto, privado ou público. Nessa perspectiva, preservando inclusive dados públicos, a proteção de dados é abrangente quanto à disponibilidade,

isto é, se os dados estarão disponíveis sempre que precisar; e também quanto à integridade, assegurando que as informações estão corretamente disponibilizadas. Portanto, sob o ponto de vista da segurança da informação, a privacidade é uma constituinte da proteção de dados.

Já do ponto de vista filosófico, a situação se inverte; a proteção de dados possui um valor quase irrelevante nessa perspectiva, ela é vista como uma ferramenta do ramo da privacidade. Esta, por sua vez, é a fonte de discussão, desde os filósofos gregos Platão e Aristóteles. Segundo descrito por Arendt (2007, p. 38-39), Platão tinha uma posição abolucionista da esfera privada:

> Historicamente, é muito provável que o surgimento da cidade-Estado e do domínio público tenha ocorrido à custa do domínio privado da família e do lar.16 Contudo, a antiga santidade da lareira, embora muito mais pronunciada na Grécia clássica que na Roma antiga, jamais se perdeu inteiramente. O que impediu a pólis de violar as vidas privadas dos seus cidadãos, e a fez ver como sagrados os limites que cercavam cada propriedade, não foi o respeito pela propriedade privada tal como a concebemos, mas o fato de que, sem possuir uma casa, um homem não podia participar dos assuntos do mundo porque não tinha nele lugar algum que fosse propriamente seu.17 Até Platão, cujos planos políticos previam a abolição da propriedade privada e a expansão da esfera pública ao ponto de aniquilar completamente a vida privada, ainda falava com grande reverência de Zeus Herkeios, o protetor das fronteiras, e chamava de divinos os horoi, os limites entre os Estados, sem nisso ver qualquer contradição.

Já Aristóteles, em sua obra A Política, considera que a cidade está acima do privado, porém, mesmo abaixo, o privado deve ser respeitado:

7

> Sabemos que toda cidade é uma espécie de associação, e que toda associação se forma tendo por alvo algum bem; porque o homem só trabalha pelo que ele tem em conta de um bem. Todas as sociedades, pois, se propõem qualquer lucro — sobretudo a mais importante delas, pois que visa a um bem maior, envolvendo todas as demais: a cidade ou sociedade política. [...]
> Esta dupla união do homem com a mulher, do senhor com o escravo, constitui, antes de tudo, a família. Hesíodo disse, com razão, que a primeira família se formou da mulher e do boi feito para a lavra. Com efeito, o boi serve de escravo aos pobres. Assim, naturalmente, a sociedade constituída para prover às necessidades quotidianas é a família, formada daqueles que Carondas chama homos pyens (tirando o pão da mesma arca), e que Epimenides, de Creta, denomina homocapiens (comendo na mesma manjedoura).(Aristóteles, 2011, s.p)

Há, portanto, em Aristóteles a concepção de que a cidade era mais importante, mas que este bem mais importante deveria servir para prover as necessidades cotidianas das famílias.

Veja, a discussão do público e privado foi retratada desde a Grécia Antiga ali e persistiu, até os dias atuais, acompanhando as tendencias de cada época e culminando no tempo tecnológico atual.

Já proteção de dados é o conceito relacionado à metodologia de como proteger as informações, sejam pessoais ou não, e se entende que a sua natureza é como um tripé de cuidados jurídicos, tecnológicos e comportamentais.

A análise jurídica deve ser devidamente feita a partir de dois olhares: um sob o ordenamento jurídico e o outro sob aquilo que foi pactuado entre as partes. O olhar jurídico deve ser feito principalmente a partir do Código Civil e da LGPD. Do primeiro, deve-se tomar todas as observações necessárias relacionadas ao negócio jurídico, especialmente, no que se refere à celebração e à interpretação de cláusulas. Do segundo, extrai-se os direitos dos titulares de dados e os deveres dos controladores e operadores.

Sob a ótica da LGPD, os dois agentes de tratamento de dados são assim definidos:

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; [...]
> IX - agentes de tratamento: o controlador e o operador (BRASIL, 2018, s.p.).

Em vista do que foi citado, o controlador e o operador podem ser considerados como agentes de tratamento. Ao controlador, cabe a ele as decisões de como deve ser feito o tratamento de dados pessoais: se será de maneira física ou digital, onde serão armazenados, quem terá o acesso, se será utilizado serviços terceirizados, entre outros pontos relevantes. Já o operador é aquele que a mando do controlador, realiza um tratamento de dados específico como, por exemplo, um serviço contábil ou o fornecimento de um servidor para o armazenamento e o processamento de dados pessoais. É importante ressaltar que todos os dados que são tratados dentro da LGPD dizem respeito apenas à dados pessoais; já dados empresariais, que envolvam segredos industriais e outros pontos relevantes de uma empresa, não são protegidos pela lei, cabendo às instituições observar as leis correlatas e principalmente acordos contratuais.

Ainda em relação à análise jurídica, no segundo olhar, sobre aquilo que foi pactuado entre as partes, devem ser observados os itens anteriores descritos na lei, mas também, a vontade de proteção de dados, principalmente, a partir do vigor da LGPD. É preciso que as leis constem nos contratos, e buscar as garantias necessárias para que os requisitos mínimos de segurança sejam alcançados. A exigência da proteção de dados sempre vai depender daquele que é o responsável pela tomada de decisões: o controlador de dados. Este deve requerer dos fornecedores, de seus prestadores de serviço ou em qualquer interação que envolvam dados pessoais, o sigilo e o respeito à privacidade. Esse ponto está em conformidade com a LGPD e também com o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado da ANPD":

> Extrai-se dessa disposição legal que o tratamento não precisa ser realizado diretamente pelo controlador. Muito embora o controlador também trate dados pessoais, o elemento distintivo é o poder de decisão, admitindo-se que o controlador forneça instruções para que um terceiro ("operador") realize o tratamento em seu nome (art. 5º, VII; art. 39) (BRASIL, 2021, p. 10)

Com esse poder de decisão, o controlador de dados deve ter em seu alcance as garantias necessárias e as exigir. Aqui se encontra a importância de uma análise multidisciplinar do contrato, sendo os responsáveis pelos setores tecnológicos e de processos, além obviamente do jurídico, partes importantes para a exigência desses padrões de segurança, pois, sem o comprometimento de todos, corre-se o risco de acreditar que um acordo de não divulgação seria o suficiente para se resguardar dentro da LGPD. O "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado da ANPD" ainda discorre:

> O segundo ponto relevante é a desnecessidade de que todas as decisões sejam tomadas pelo controlador, bastando apenas que este mantenha sob sua influência e controle as principais decisões, isto é, aquelas relativas aos elementos essenciais para o cumprimento da finalidade do tratamento. De fato, especialmente quando há a contratação de um operador, é usual e legítimo que parte das decisões a respeito do tratamento, limitadas aos seus elementos não essenciais, fique sob a alçada do operador. A título de exemplo, podem ser mencionados a escolha dos softwares e equipamentos que serão utilizados e o detalhamento de medidas de prevenção e segurança (BRASIL, 2021, p. 10)

Portanto, não é necessário que o controlador exija nos mínimos detalhes, os parâmetros de segurança como, por exemplo, qual antivírus utilizar ou

qual o padrão de senha, mas ele pode exigir a existência de uma ferramenta antivírus e um padrão mínimo de segurança para a sua atuação.

Essa requisição pode ser uma determinação livre, pactuada contratualmente, ou feita por meio de *frameworks* de segurança da informação para que possam balizar os padrões mínimos. A ISO 27001, Framework NIST, Security+, são alguns exemplos importantes na área de segurança da informação.

2.2.1 A Proteção de Dados Pessoais como Direito Fundamental

Como visto anteriormente, a privacidade é um direito fundamental tutelado pela Constituição Federal, conforme o artigo 1º, inciso III e o artigo 5º, inciso X (BRASIL, 2022). Quanto à proteção de dados pessoais, em um primeiro momento, já estaria de acordo com o ordenamento constitucional, conforme a Ação Direta De Inconstitucionalidade 6.387 (ADI) (BRASIL, 2020).

Nela, como será visto detalhadamente em um segundo momento, o Supremo Tribunal Federal, em seus votos, entendeu que a proteção de dados pessoais estaria conjugada na leitura dos incisos X e XII do artigo 5º:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 2022, s.p.)

Conforme a ementa do ADI, é possível apontar que desde 1988 já havia salvaguardas a respeito da proteção de dados, mesmo que não estruturadas em forma de legislação, que só ocorreu após o Marco Civil da Internet e principalmente após a Lei Geral de Proteção de Dados Pessoais. Conforme a ementa do julgamento, pode-se ver explicito esse parâmetro:

> Na medida em que relacionados à identificação – efetiva ou potencial – de pessoa natural, o tratamento e a manipulação de dados pessoais hão de observar os limites delineados pelo âmbito de proteção das cláusulas

> constitucionais assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII), sob pena de lesão a esses direitos. O compartilhamento, com ente público, de dados pessoais custodiados por concessionária de serviço público há de assegurar mecanismos de proteção e segurança desses dados (BRASIL, 2020, p. 2)

Partindo desse princípio, já seria possível a interpretação da proteção de dados pessoais a partir de um direito constitucional, mas o legislador, exercendo sua autoridade de poder constituinte reformador, acrescentou um novo inciso dentro da Constituição Federal através de PEC 17/2019, que justamente tutela sobre dados pessoais.

No dia 10 de fevereiro de 2022, a Emenda Constitucional 115/2022, originada da PEC 17/2019, foi promulgada, alterando três artigos da Constituição Federal. O primeiro diz respeito ao direito fundamental da proteção de dados pessoais:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (BRASIL, 2022, s.p.)

Já as outras duas alterações dizem respeito as competências, que passam a ser privativas da União, tanto ao nível do executivo, quanto ao nível do legislativo, no que diz respeito a legislação sobre dados pessoais:

> Art. 21. Compete à União:
> [...]
> XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.
> [...]
> Art. 22. Compete privativamente à União legislar sobre:
> [...]
> XXX - proteção e tratamento de dados pessoais. (BRASIL, 2022, s.p.)

Esta solução dada auxilia uma uniformidade da legislação em todo o solo nacional, evitando que estados e municípios criassem leis especificas sobre o tema de proteção de dados pessoais.

Em vista do que foi exposto, está claro que tanto a privacidade quanto a proteção de dados pessoais são direitos fundamentais protegidos pela Constituição

Federal e ganham aqui uma importância e um seguro amadurecimento no futuro do Brasil.

2.2.2 Proteção de Dados no Poder Público

Neste tópico, é abordado um aspecto muito importante para a análise de como se comportam o tratamento de dados pessoais dentro de cidades inteligentes. Primeiramente, do ponto de vista técnico, elas devem ser vistas apenas como uma prefeitura, que pelo bem dos cidadãos, escolheu se equipar de tecnologias e processos que visam melhorar a dinâmica dentro dessa cidade, resolver problemas e dar mais qualidade de vida aos moradores.

Um erro que pode ser levado em consideração dentro do poder público, é conceituar os servidores como operadores de dados, enquanto a administração do munícipio é o controlador. No início dos estudos relacionados a LGPD, havia essa confusão, gerada por uma má interpretação da lei. O “Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado da ANPD” trata a gestão de dados neste sentido:

> Nesse cenário, empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta não devem ser considerados operadores, tendo em vista que o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos (BRASIL, 2021, p. 17)

Diante desse cenário, a gestão da proteção de dados é complexa, pois existe certa autonomia em todas as secretarias, além das sociedades de economia mista. Considerando esse fato, o “Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado” da ANPD, de acordo com a União, trata a gestão de dados da seguinte forma:

> Situação peculiar é a das pessoas jurídicas de direito público, cujas competências decisórias são distribuídas internamente entre diferentes órgãos públicos. É o que ocorre, por exemplo, com a União (pessoa jurídica de direito público) e os Ministérios (órgãos públicos despersonalizados que integram a União e realizam tratamento de dados pessoais conforme o previsto na legislação). Nesses casos, deve-se considerar dois aspectos centrais. De um lado, conforme o art. 5º, VI, da LGPD, o controlador é a União, pessoa jurídica de direito público que, em última análise, é a responsável

> pelas obrigações decorrentes da lei, de instrumentos contratuais ou de atos ilícitos praticados pelos seus órgãos e servidores (BRASIL, 2021, p. 8)

Como já elucidado, a União é considerada como a figura do controlador de dados, e os Ministérios são aqueles que integram a União e realizam o tratamento de dados conforme a legislação. Ressalta-se ainda que todas as secretarias municipais estão sob a legislação, logo também sob aquilo que é planejado pelo Município.

Ao se observar essa obrigação, é possível perceber a importância da dedicação dos setores designados à segurança da informação ao nível municipal e da criação de um Comitê Gestor de Segurança da Informação. É relevante frisar que, em última análise, a tomada de decisão será feita pelo executivo, mas esse Comitê, contando principalmente com o auxílio do setor de Tecnologia da Informação, de Segurança Pública, dentre outros, tem papel fundamental para o planejamento de proteção de dados dentro do munícipio.

Aqui, vale também observar a necessidade de nomear um encarregado de dados dentro do poder público. O conceito de encarregado é assim definido dentro da LGPD:

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); (BRASIL, 2018, s.p.).

Já o dever de nomeação de um encarregado está descrito dentro do artigo 41 da LGPD:

> Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> § 2º As atividades do encarregado consistem em:
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
> II - receber comunicações da autoridade nacional e adotar providências;
> III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.; (BRASIL, 2018, s.p.).

Observando o artigo 41 da LGPD, o controlador deve indicar um encarregado pelo tratamento de dados pessoais, sendo este o responsável por garantir a conformidade com a LGPD e as boas práticas de mercado. Além disso, a lei utiliza um termo amplo, sendo necessário observar que tanto organizações privadas quanto públicas devem nomear um encarregado de dados. Esse fato é confirmado dentro do “Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado” da ANPD que trata a gestão de dados da seguinte forma:

> O artigo 41 da LGPD não faz distinção quanto a instituições públicas ou privadas e por isso é importante que ambas estejam cientes da sua obrigação de indicar um encarregado de dados. A esse respeito, o art. 23, III, reforça a necessidade de um encarregado ser indicado por órgãos e entidades públicas (BRASIL, 2021, p. 22)

Outro ponto, considerando a complexidade da administração de um Município, seria a criação e a extensão de uma equipe que apoie o encarregado de dados nas diversas secretarias. A fim de efetivar o que está previsto pela LGPD, é importante se pensar em um encarregado para a gestão geral em conformidade com a legislação, e considerar, para cada uma das secretarias, o auxílio de um analista de proteção de dados. O “Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado da ANPD” confirma:

> Também é importante observar que a LGPD não proíbe que o encarregado seja apoiado por uma equipe de proteção de dados. Ao contrário, considerando as boas práticas, é importante que o encarregado tenha recursos adequados para realizar suas atividades, o que pode incluir recursos humanos. Outros recursos que devem ser considerados são tempo (prazos apropriados), finanças e infraestrutura (BRASIL, 2021, p. 22).

Por fim, não se pode subestimar os editais de licitações, os quais devem ter disposições que contemplem a proteção de dados. O encarregado deve sempre estar atento a todos os fornecedores dos municípios, pois o esforço em manter a conformidade dentro da própria administração pode ser perdido pelo descuido em relação aos fornecedores.

2.3 PRIVACY BY DESIGN

Dentro do contexto de criação de uma cidade inteligente, a fim de construir as ferramentas necessárias para se alcançar esse objetivo, não bastam somente os fatores tecnológicos ou o foco no meio ambiente, pois é um trabalho em conjunto com diversas áreas, dada a complexidade sobre o tema. Um dos campos onde há a necessidade de uma severa avaliação, é a área de proteção de dados pessoais. A grande preocupação é que, pelo bem maior, a proteção desses dados seja mitigada.

Em um primeiro momento, em projetos que já estejam em andamento, há uma importância em analisá-los me adequá-los à LGPD, sob a possibilidade deles sofrerem as sanções previstas na legislação. Agora, para projetos não iniciados, é preciso observar o conceito chamado *privacy by design* ou privacidade por *design*.

Ann Cavoukian (2011, p. 2) descreve que existem 7 (sete) princípios quando se fala nesse termo:

> a) proativadade antes de medidas reativas, prevenção antes de remediar as situações;
> b) Privacidade como padrão;
> c) Privacidade inserida no design;
> d) Funcionalidade completa, soma positiva e não soma zero;
> e) Segurança de ponta a ponta;
> f) Visibilidade e transparência; e
> g) Respeito pela privacidade do usuário.

Pensando em cidades inteligentes, o primeiro princípio diz respeito a antever todas as situações que possam ferir a privacidade de alguém. É um princípio que está totalmente de acordo com as diretrizes da LGPD, principalmente, a de responsabilidade e de prestação de contas. Construir cidades inteligentes requerem um forte conhecimento de proteção de dados pessoais.

O conceito de “privacidade por padrão” é uma concepção centralizadora dentro da privacidade por *design*, que diz respeito a todas as possibilidades de escolhas dentro de um tratamento de dados de acordo com as suas opções-padrão, trazendo as alternativas mais benéficas ao titular do dado, e caso ele escolha compartilhar as suas informações, fica sujeito a definir por si próprio novas funções. Um exemplo seria um carro inteligente que, por padrão, não compartilha informações com a cidade inteligente, mas deixa a escolha para o titular.

Dando continuidade, o terceiro conceito diz respeito à “privacidade inserida no *design*”, na qual as configurações por padrão, estão ajustadas para favorecer a privacidade, mas que a opção de as controlar seja facilmente identificada nos menus, assim como o contato com o encarregado.

A ideia de “funcionalidade completa” reflete-se na garantia de segurança da privacidade e de que os dados estão protegidos. Em tempos em que se há constantemente a suspeita de que as informações pessoais estão sendo espalhadas, essa relação completa de preservação e respeito cria um vínculo positivo de ambos os lados. Isto é, a empresa se fortalece com os pilares de respeito a dados dos titulares e com os princípios fundamentais da Constituição Federal, da LGPD e do Marco Civil da Internet, podendo inclusive utilizar esses pontos para se promover. Ao mesmo tempo, ganha também o titular de dados, que tem a garantia dos seus direitos enquanto cidadão de cidades inteligentes.

O conceito de “segurança ponta a ponta” é reconhecido em aplicativos de mensagens, em vários sites e também nos e-mails, mas dentro do contexto de cidades inteligentes, onde a rede pode ser compartilhada, a ideia ganha um status de extrema exigência, principalmente, nas comunicações entre titulares de dados e aplicações que exigem um alto nível de segurança.

Em relação ao princípio da “visibilidade e transparência”, é preciso que a linguagem seja acessível e clara, para que todos entendam o que está sendo processado com os dados fornecidos. Pode até existir uma segunda camada dos documentos que possuem uma maior profundidade técnica, na qual seja possível compreender todos os detalhes por meio de uma linguagem corriqueira, possibilitando a transparência e evitando-se inconsistências.

Por fim, dispõe-se sobre o princípio norteador do “respeito pela privacidade do usuário”, em que todos os conceitos demonstrados anteriormente são confirmados por este, sendo imprescindível a necessidade de ajustes a fim de acompanhar a tecnologia atual.

Por se tratar de um conceito estrangeiro, é preciso compreender se esse tipo de organização não é apenas harmônico com a LGPD, mas é explicitamente citado dentro do artigo 46 e devendo ser observada para o devido tratamento de dados pessoais:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2018, s.p.)

O texto como um todo não é claro em relação ao conjunto de cuidados que devem ser observados desde a concepção do projeto, mas é clara a necessidade de sua observância, conforme o parágrafo 2º do artigo 46. As medidas de segurança, técnicas e administrativas podem sim refletir esse conceito apresentado como uma boa prática, mas deve ser disposta pela ANPD, detalhando cada um desses pontos e cuidados.

3 SEGURANÇA PUBLICA

Um dos pontos mais polêmicos quanto ao tratamento de dados dentro de cidades inteligentes, refere-se à área de segurança pública. O cruzamento de informações em bancos de dados, o uso extensivo de monitoramento, o reconhecimento facial, o estado de animosidade política e o cerceamento de liberdade de expressão passam por essa discussão.

Observando o avançar tecnológico, é possível perceber o barateamento das tecnologias e o avanço na sua implementação. Diante de câmeras menores e mais precisas, da entrada da tecnologia 5G no Brasil e também do uso de inteligência artificial, é possível mapear boa parte dos cidadãos; contudo, é preciso refletir se toda essa vigilância é recompensadora, levando em consideração a possibilidade de diminuição nas taxas de criminalidade, ou se é prejudicial perante o eterno estado de alerta e a probabilidade de um governo mais autoritário que diminuirá as liberdades individuais.

É perceptível que a necessidade de discussão sobre o uso de dados dentro da segurança pública é urgente, a partir de reflexões sobre o ordenamento atual e as principais soluções.

3.1 MINORITY REPORT, PRECONIGÇÕES E ESTADO VIGILANTE

O livro “*Minority Report* - A nova lei” foi escrito por um dos maiores autores de ficção cientifica do século XX, Philip Kindred Dick (2002), que ao lado de Isaac Asimov, é um dos expoentes nas áreas em que a ficção cientifica é estudada na realidade para racionalizar possíveis problemas e soluções.

Philip Kindred Dick foi um escritor norte-americano de ficção científica, nascido em 16 de dezembro de 1928 em Chicago, e falecido no dia 2 de março de 1982 em Santa Ana. Suas obras trazem temas de suma relevância com fundos políticos, sociais e filosóficos, indo do autoritarismo e realidades alternativas, até estados alterados de consciência. Seus trabalhos mais conhecidos são “Ubik”, “Androids Sonham com Ovelhas Elétricas” e “*Minority Report* - A nova lei”.

Este último, principalmente no campo do Direito e da Criminologia, ganhou destaque pelo conceito de “precognição” e “livre arbítrio”. Em síntese, a

história acontece na capital dos Estados Unidos no ano de 2054, tendo como personagem principal John Anderton, um policial à frente da Divisão Pré-Crime, sendo que a sua função era a de impedir que homicídios ocorressem. Essa precaução era possível, pois a divisão policial contava com o trabalho de mutantes precognitivos que previam o futuro e conseguiam, graças as suas habilidades, precognizar um possível assassinato, trazendo ainda o nome do suposto criminoso e da vítima, e ainda fornecendo detalhes do crime como imagens, modo de operação e o horário.

John Anderton e sua equipe são os responsáveis pela análise dos casos, e por impedir o assassinato com base em todas as informações obtidas, prendendo o suposto culpado. A história muda de rumo quando os mutantes precognitivos, em um determinado dia, levantam a informação de que o próprio John Anderton cometeria um homicídio. Ele se recusa a acreditar que será um assassino e os seus próprios companheiros de equipe o levam até os fatos precognizados.

Para entender melhor esse ponto, este trecho da obra é bem claro quanto à atuação de mutantes precognitivos e a sua ação:

> — Você está a par da teoria da prevenção do crime, é claro. Suponho que isto seja ponto pacífico.
> — A informação que tenho é a que está disponível publicamente — replicou Witwer. — Com a ajuda de seus mutantes precognitivos, você conseguiu, audaciosamente, abolir o sistema punitivo pós-crime de cadeias e multas. Como todos sabemos, a punição nunca foi um grande impedimento, e provavelmente nunca ofereceu conforto à vítima já morta.
> Tinham chegado ao elevador. Enquanto este os levava rapidamente para baixo, Anderton disse:
> — Deve ter percebido o inconveniente legal básico da metodologia pré-crime. Prendemos indivíduos que nunca infringiram a lei.
> — Mas que certamente infringirão — afirmou Witwer com convicção.
> — Felizmente, não. Nós os pegamos primeiro, antes que cometam qualquer ato de violência. Desse modo a comissão do crime, em si mesma, é uma metafísica absoluta. Alegamos que são culpados. Eles, por sua vez, afirmam eternamente ser inocentes. E, de certa maneira, são inocentes (DICK, 2002, p. 28)

Como visto nesse diálogo simples, é possível perceber o tom filosófico que a obra carrega, principalmente, sobre questões de livre arbítrio e direito criminal.

Em nossa realidade não há mutantes precognitivos que podem prever crimes e evitá-los, mas por meio de análises de dados, pode-se monitorar comportamentos, apontar quando não estão de acordo com a ética social e recriminá-los.

Softwares munidos de inteligência artificial e de outras tecnologias poderiam catalogar, na melhor das hipóteses, dados abertos de *posts*, criar perfis de comportamento dos usuários e fazer medições quanto às possibilidades de manifestações contra o governo, por exemplo. Em um trecho de uma reportagem de 2013, o diretor da ABIN confirmou que utilizava os dados abertos de redes sociais para monitorar:

> No mês de junho, um reportagem publicada pelo jornal O Estado de S.Paulo apontou que a agência brasileira estava montando uma rede para monitorar internet. Dois meses após a notícia, a reportagem do Portal EBC conseguiu confirmar, via pedido pela Lei de Acesso à Informação (LAI), que a Abin realmente monitora redes sociais.
> De acordo com o documento de resposta da Agência, enviado no dia 27 de agosto, o Gabinete de Segurança Institucional da Presidência da República (GSI) esclareceu que a "Agência Brasileira de Inteligência quando necessário, realiza pesquisas em fontes abertas, incluindo mídias sociais, para eventuais subsídios aos seus trabalhos". Nenhum outro detalhe como é o trabalho da Abin em redes sociais foi repassado, inclusive se o monitoramento acontece por meio de uma rede ou ocasionalmente. A Abin já havia sido procurada pelo Portal EBC para falar sobre o assunto, mas não concedeu entrevista à época (MATSUKI; PEDROSA, 2013, s.p.).

Dados abertos são aqueles disponíveis na *internet*, postados voluntariamente (muitas vezes sem entender o impacto) e que podem ser lidos por todos. A catalogação dessas informações pode ser realizada ao cruzar dados de redes sociais com grupos e fóruns abertos, e também com grupos de mensageiros abertos com um “espião”, como *Whatsapp* e *Telegram*.

Entrando na seara de cidades inteligentes, os responsáveis pela segurança pública podem utilizar esses recursos a fim de evitar uma manifestação política, ou ainda cruzar informações coletadas em redes soais com dados de monitoramento para tentar evitar crimes. Mas, vale um questionamento: até que ponto, robôs alimentando banco de dados com materiais provenientes de fontes abertas, para predizer crimes ou evitar manifestações, é moral? É uma ponderação relacionada à tecnologia que passa pelas estruturas de cidades inteligentes.

3.2 VIGILÂNCIA AUTOMATIZADA

Como visto anteriormente, dados abertos de redes sociais eram monitorados pela ABIN, sem fornecer a segurança necessária dos motivadores nessa

coleta, sob a premissa de que esses dados estariam sendo utilizados para neutralizar manifestações e organizações livres de pessoas, caso necessário.

Além desse tipo de vigilância, outra forma de monitoramento hoje bastante utilizada é o uso de reconhecimento facial pela Administração Pública. Conforme o relatório do LAPIN, a usabilidade dessas tecnologias poderia ser colocada da seguinte maneira:

> Neste relatório, apresentamos alguns casos de uso dessas ferramentas pelo poder público voltadas a seis finalidades: segurança pública, transporte urbano, escolas, sistemas para gestão de benefícios sociais, controle alfandegário e validação de identidade. Essas aplicações foram mapeadas a nível federal e nas cinco regiões do Brasil, nas esferas municipal e estadual. Na segurança pública, a tecnologia tem sido utilizada principalmente para identificar pessoas desaparecidas ou procuradas pela polícia. Já para mobilidade urbana, a aplicação de tecnologia de RF tem a finalidade de identificar se a pessoa que está utilizando um benefício como o passe livre é aquela que realmente possui o direito à assistência. Esta hipótese é similar ao controle de presença escolar, acesso a benefícios sociais e verificação de identidade, em que se objetiva confirmar a identidade do estudante, do beneficiário e do cidadão, respectivamente (REIS; ALEMIDA; SILVA; DOURADO, 2021, p. 6)

É importante salientar que o objetivo não é demonizar o uso de reconhecimento facial no combate ao crime e no auxílio à segurança pública, mas respeitar o princípio da transparência, conforme o artigo 6º, inciso VI da LGPD (BRASIL, 2018). Diversas dúvidas surgem diante dessa realidade: quais são as empresas que fornecem os equipamentos de reconhecimento facial? Como a inteligência artificial foi construída? As imagens são tratadas em tempo real ou são realizadas gravações? As informações tratadas são armazenas em quais bancos de dados? Como é feito o supervisionamento humano? Há o compartilhamento desses dados? Essa tecnologia possui garantias quanto ao tratamento igualitário de pessoas de todas as raças, como brancos, negros, pardos, asiáticos, europeus, árabes, indígenas, etc.?

A própria LGPD, em seu artigo 20, dispõe sobre o tema, deixando claro que o tratamento automatizado deve dar o direito à revisão e também o dever ao controlador de fornecer informações claras sobre os procedimentos feitos:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (BRASIL, 2018, s.p.).

Ademais, dados pessoais que são manipulados dessa maneira, conforme a LGPD, são considerados informações sensíveis, de acordo com a definição do artigo 5º, inciso II:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural 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, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018, s.p.).

Conjugando todos esses fatores, o mínimo que deve ser feito é apresentar o relatório de impacto a proteção de dados, oportunizando que todos saibam a empresa dos equipamentos disponibilizados e como é feito o tratamento.

Contudo, o que preocupa são casos estarrecedores como o apresentado na reportagem do portal Band News, em que mais de uma prisão foi feita por engano no ano de 2019, no Rio de Janeiro, durante o uso de uma tecnologia experimental:

> Mais uma pessoa foi presa por engano pela Polícia Militar após ser identificada pelo sistema de reconhecimento facial implantado em Copacabana, na Zona Sul. Ele foi levado à delegacia, mas foi liberado quando constada a falha.
> Dias antes, uma mulher também foi confundida com a autora de um homicídio na Região dos Lagos. A verdadeira criminosa já estava presa, mas a informação não constava no banco de dados [...] (ALMEIDA, 2019, s.p.).

Utilizar uma tecnologia tão invasiva sem os cuidados necessários com a transparência de seus usos, deveria ser considerado uma grave ameaça à privacidade dos cidadãos. Rony Vainzof (2020, p. 22) comenta sobre as escolhas tecnológicas, incluindo o reconhecimento facial, da seguinte maneira:

> Qualquer iniciativa que se tenha nesse sentido – diga-se de passagem, irreversível –, por usualmente envolver coleta massiva de dados e, por vezes, com a possibilidade do tratamento de dados sensíveis, como o reconhecimento facial biométrico, deve ser beneficiada pelo estudo da própria LGPD, notadamente seus princípios, para mitigar riscos e avaliar a proporcionalidade do projeto, principalmente: (i) adequação, que é compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; (ii) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; (iii) qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; (iv) segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; (v) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e (vi) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

Em vista do que foi exposto, não é possível tratar de maneira superficial um problema que pode atingir negativamente toda a sociedade; que possui um potencial de não somente causar danos à privacidade, mas também à imagem de uma pessoa em caso de eventual engano.

Portanto, deve-se promover uma reflexão em relação à Segurança Pública, incluindo a proteção praticada por meio de tecnologias. Necessita-se de uma legislação própria, de modo que não poderia ser analisada sob o ponto de vista da LGPD, conforme será discutido a seguir.

3.3 Segurança Pública e LGPD

Diante da realidade da Segurança Pública dentro de cidades inteligentes, pode haver dúvida quanto à aplicação da LGPD nesse setor, visto o disposto no artigo 4º:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:
> [...]
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais (BRASIL, 2018, s.p.).

Ao observar rapidamente o artigo acima descrito, um leitor desatento poderia crer que os dados tratados dentro da Segurança Pública não estão inclusos na LGPD e que a sua secretaria continuaria a gestão sem a interferência da lei de proteção de dados. As respostas para esses pontos se encontram nos parágrafos subsequentes:

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

Dentro da Segurança Pública, todos os princípios presentes no artigo 6º da LGPD devem ser observados, como já destacado pelo Vainzof (2020).

Outro ponto importante diz respeito aos direitos assegurados aos titulares de dados quanto à requisição de informações de tratamento, como: a confirmação da existência de tratamento; o acesso, a correção, a anonimização, o bloqueio ou a eliminação de dados desnecessários, excessivos ou tratados em desconformidade; e a informação das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados.

Diante dessas obrigações destinadas aos controladores de dados dentro da área de Segurança Pública, mesmo que não haja menção direta sobre a necessidade de um encarregado, atendendo às obrigações de suporte aos titulares de dados, faz-se necessário também observar o artigo 23, inciso III da LGPD (BRASIL, 2018) que trata exatamente da necessidade de ser indicado um encarregado nas operações de tratamento de dados pessoais. Se uma de suas atribuições é justamente a resposta ao titular, então, dentro da Segurança Pública, é obrigatório a presença de pessoa para tal ato.

Como será visto adiante, mesmo que uma empresa de direito privado exerça o tratamento de dados a mando de uma empresa pública que trabalha com Segurança Pública, quem deve tutelar e responder pelos danos ocasionados desse tratamento é a empresa pública, em conformidade com a teoria da responsabilidade do agente público.

Um item importante a se observar é que ao implementar novas tecnologias a fim de otimizar os processos de Segurança Pública, como os itens que podem ser categorizados dentro da *internet* das coisas, o uso de robótica, a inteligência artificial ou outros artifícios tecnológicos, estes devem ser acompanhados de um relatório de impacto à proteção de dados, que pode ser requerido pela ANPD.

De forma geral, da mesma maneira que se vê em outros temas, como na saúde e em conflitos aparentes entre direitos fundamentais, é preciso respeitar a privacidade, não utilizar tecnologias que afetem o poder de escolha nem uma força de intimidação. Como se está sempre tratando de ganho de bem-estar em cidades inteligentes, deve-se evitar viver em um estado como imaginado por Orwell (1984, s.p.):

> Na fachada da casa logo do outro lado da rua, via-se um deles. o GRANDE IRMÃO ESTÁ DE OLHO EM VOCÊ, dizia o letreiro, enquanto os olhos escuros pareciam perfurar os de Winston. [...] Era a patrulha policial, bisbilhotando pelas janelas das pessoas. As patrulhas, contudo, não eram um problema. O único problema era a Polícia das Ideias.
> Por trás de Winston, a voz da teletela continuava sua lenga-lenga infinita sobre o ferro-gusa e o total cumprimento — com folga — das metas do Nono Plano Trienal. A teletela recebia e transmitia simultaneamente. Todo som produzido por Winston que ultrapassasse o nível de um sussurro muito discreto seria captado por ela; mais: enquanto Winston permanecesse no campo de visão enquadrado pela placa de metal, além de ouvido também poderia ser visto. Claro, não havia como saber se você estava sendo observado num momento específico. Tentar adivinhar o sistema utilizado pela Polícia das Ideias para conectar-se a cada aparelho individual ou a frequência com que o fazia não passava de especulação. Era possível inclusive que ela controlasse todo mundo o tempo todo. Fosse como fosse, uma coisa era certa: tinha meios de conectar-se a seu aparelho sempre que quisesse. Você era obrigado a viver — e vivia, em decorrência do hábito transformado em instinto — acreditando que todo som que fizesse seria ouvido e, se a escuridão não fosse completa, todo movimento examinado meticulosamente. Winston mantinha as costas voltadas para a teletela. Era mais seguro; contudo, como sabia muito bem, mesmo as costas de uma pessoa podem ser reveladoras.

Aqui deve ser alcançado o equilíbrio entre o combate do crime, considerando um estado de tranquilidade que se preocupa o bem estar do cidadão, em contrapartida ao estado de insegurança que também leva os extintos humanos em

um estado de desconforto e de sempre estar em profundo alerta sempre esperando um mal, nem entrando nos méritos relacionados aos danos causados por um crime; equilíbrio este que deve colocar do outro lado da balança o excesso de vigilantismo e um eterno estado de alerta, aí sim pelo poder estatal de segurança.

3.4 Segurança Pública em Cidades Inteligentes

Sobre as soluções relacionadas à segurança pública em cidades inteligentes, sejam elas implementadas por guardas municipais em nível municipal, ou pelas polícias militares, civis ou federais, todas elas devem observar o descrito anteriormente para um bom cumprimento da lei.

3.4.1 Georreferenciamento de Ocorrências

Dentro dessa solução, todas as ocorrências são mapeadas e estruturadas, classificando o local e o tipo de delito, buscando um padrão para que se possa agir contra as transgressões e propiciar uma maior segurança.

Como é visto em tópico futuro, nesse tipo de aplicação podem ser utilizadas técnicas de anonimização, principalmente, as relacionadas à generalização, sem especificar o endereço exato onde ocorreu o chamado, mas uma posição aproximada; ademais, pode-se investir na técnica de supressão, sem a necessidade do nome ou de qualquer outra informação que possa pessoalizar o caso.

As vantagens em obter padrões nessa situação são imensas, principalmente, na busca de quadrilhas e de crime organizado. O compartilhamento de informações entre guardas e polícias podem alimentar um banco de dados que auxilie em uma tomada de decisão conjunta, desde que, mais uma vez informando, respeite os direitos do titular de dados e os princípios da LGPD.

3.4.2 Monitoramento por Câmeras

O uso de câmeras em si não é ruim por natureza, principalmente em lugares públicos e de grande circulação. É justificado até mesmo a supervisão humana dessas filmagens em tempo real para verificar possíveis delitos ou perturbações que necessitam da intervenção da segurança pública.

Contudo, é preciso discutir o uso de tecnologias que captam e catalogam em tempo real pessoas e situações para referenciar o local ou o hábito de alguém, utilizando reconhecimento facial. Acrescenta-se ainda o uso indiscriminado de dados em casos políticos e sociais, como manifestações e identificação automática de protestantes.

Ademais, destaca-se que normalmente não é utilizada uma construção interna desse tipo de tecnologia, havendo a necessidade de contratação de ferramentas. Portanto, a garantia que esses equipamentos respeitam a LGPD é de suma importância nesses tipos de situações. Mais uma vez, ressalta-se a importância de um relatório de impacto à proteção de dados.

3.4.3 Sistemas Compartilhados de Controles de Ocorrências

Para ser criado um sistema de compartilhamento de controle de ocorrências, é necessário primeiramente verificar se a finalidade que se busca é efetiva: o combate à criminalidade e a busca pela paz social.

Nesse sentido, após análise do relatório de impacto à proteção de dados, os princípios da segurança da informação devem ser respeitados, principalmente, verificando o princípio da confidencialidade, quais agentes devem realmente ter acesso e a quais dados.

Ainda mais, pode ser adotado o sistema de aviso de checagem de informação, em que cada vez que o dado de um cidadão for acessado por algum agente da segurança pública, um aviso chega ao titular informando quem acessou, quando, e em que circunstâncias. Assim, dá a oportunidade de pedir maiores esclarecimentos ao encarregado de dados sobre as informações ali presentes, sobre o compartilhamento e também sobre a segurança do tratamento desses dados.

3.4.4 Gerenciamento de Frotas

Aqui se pode ter um grande gerenciamento de frotas de guardas e policiais, otimizando custos e buscando uma maior performance. Pensando no presente, é possível ter um maior controle sobre as necessidades, as ocorrências e a otimização de tempo.

Já pensando no futuro, ponderar a respeito da utilização de carros autônomos e não autônomos de maneira inteligente, de um maior gerenciamento de tráfego que facilite a ação das guardas e polícias, e de uma maior efetividade no cuidado dos equipamentos, podem auxiliar na segurança pública.

3.4.5 Controle de Eventos

Há aqui um bom exemplo de como as cidades inteligentes podem auxiliar no cuidado do cidadão. Eventos públicos, como exposições, shows, atrações esportivas, ou até mesmo, lugares públicos com grandes movimentações, como parques, podem ser efetivados com tecnologia. Além dos recursos citados anteriormente, pode-se apostar em drones, em um maior efetivo policial, no uso de informações privilegiadas, nos avisos inteligentes via celular de ocorrências, entre outras que facilitariam a segurança.

3.5 Muralha Digital e a Aplicação da Segurança Pública em Cidades Inteligentes

Visto a teoria sobre segurança pública em cidades inteligentes, é preciso observar na prática como se dá esse funcionamento, mesmo que com cautela. Um grande exemplo que ocorre nessa área é o que está sendo implementado na cidade de Curitiba, capital do Estado do Paraná. O anúncio feito no portal da prefeitura de Curitiba no ano de 2021 traz o seguinte parágrafo:

> A Muralha Digital é uma estrutura da Prefeitura de Curitiba que não dorme, é a contribuição de Curitiba, cidade inteligente, à segurança da Região Metropolitana. Serão 1.742 câmeras, 191 locais com 804 faixas de radares, 185 botões de pânico em escolas", resumiu o prefeito Rafael Greca ao

> ressaltar que parte das 488 câmeras já instaladas permite o reconhecimento facial (CURITIBA, 2021, s.p.).

Perante esse ostensivo monitoramento e do fato que a Lei Geral de Proteção de Dados Pessoais já está em vigor, espera-se um relatório de impacto a proteção de dados que lide com esses riscos à privacidade e com a proteção de dados.

Ademais, conforme o Instituto de Cidades Inteligentes, além do reconhecimento facial, é possível observar a utilização de tecnologia OCR para a identificação de placas, a análise de vídeo em tempo real do fluxo de pessoas, e a contagem de pessoas. Outro ponto importante de se destacar é o item “Tratamento das informações coletadas por dispositivos de videomonitoramento”, que consta nos “benefícios”, mas não há detalhes de como é as informações são tratadas, qual a metodologia utilizada, e se há a perfilização ou quaisquer outros riscos.

Percebe-se que há mais perguntas do que respostas, e a necessidade de um aprofundamento com soluções que contemplem a valorização da segurança pública e a proteção e privacidade de dados.

4 SAÚDE

Após verificar os avanços e os problemas que podem ser ocasionados com o progresso das tecnologias na área da Segurança Pública, aqui se encontra um outro problema que progrediu durante a pandemia do COVID-19.

Dentro da construção de cidades inteligentes, não se poderia pensar no bem-estar da população sem haver estudos e um gerenciamento de doenças. Garantir a saúde da população é também qualidade de vida. A Carta Brasileira de Cidades Inteligentes cita a necessidade de utilizar a tecnologia para promover a efetivação de direitos fundamentais e sociais, inclusive no campo da saúde:

> Ampliação do acesso a serviços públicos e direitos sociais por meio de TICs: Usar tecnologias de informação e comunicação (TICs) para promover **o direito à cidade e para ampliar os direitos sociais**. Focar em áreas urbanas com carências de serviços públicos e em pessoas e grupos sociais vulneráveis. Para realizar esses direitos, as TICs devem colaborar na simplificação o acesso a **serviços de saúde**, educação, moradia, transporte, saneamento básico (abastecimento de água potável, esgotamento sanitário, limpeza urbana e manejo de resíduos sólidos, drenagem e manejo das águas pluviais urbanas), telecomunicações (inclusive serviços de internet), lazer e cultura. (BRASIL, 2021, p. 61, negrito nosso).

Em vista do exposto pelo documento, observa-se a necessidade de um amplo caminho a fim de otimizar processos que tornem menos burocrático a administração da saúde. No entanto, ao se buscar desburocratizar algo, principalmente, na área da saúde, costuma-se relativizar a discussão sobre como os dados pessoais serão tratados. Ao observar novamente a Carta Brasileira de Cidades Inteligentes, encontra-se o conceito de cadastro técnico multifinalitário:

> O cadastro técnico multifinalitário pode ser entendido como um sistema de registro dos elementos espaciais que representam a estrutura urbana, constituído por uma componente geométrica e outra descritiva. Esses componentes lhe conferem agilidade e diversidade no fornecimento de dados para atender diferentes funções, inclusive a de planejamento urbano (Blachut et al, 1974). Segundo Blachut et al (1980), o cadastro urbano possui três funções básicas:
> Função fiscal, que se refere à identificação dos bens imóveis e de seus proprietários com a finalidade de regulamentar o recolhimento de impostos;
> Função jurídica, que se refere à determinação dos direitos de propriedade;
> Função de planejamento que, segundo os autores, “está deslocando-se rapidamente para o ponto central das operações cadastrais, e como resultado disso o cadastro está adquirindo uma certa característica multifinalitária” (Blachut et al, 1980).
> Dessa forma, o CTM torna-se uma base sobre a qual podem ser construídas diversas bases temáticas, tais como o cadastro tributário, a base de dados

> do sistema de saúde, o cadastro de áreas verdes e públicas, e assim por diante (BRASIL, 2021, p. 121).

O cadastro técnico multifinalitário, em outras palavras, quando mal elaborado, pode se tornar um mero catalogador de perfis pessoais, trazendo grandes riscos, por mais que exista uma finalidade e um bem a ser tutelado – a qualidade de vida dos cidadãos.

Sobre essas ameaças, talvez o exemplo mais claro para se compreender os problemas que podem ser ocasionados, seria a análise da Ação Direta De Inconstitucionalidade 6.387 (BRASIL, 2020), que tratou justamente de um conflito relacionado ao direito social à saúde e ao direito fundamental da privacidade e da proteção de dados.

4.1 Medida Provisória 954/2020 e o Direito Fundamental à Saúde em Conflito com o Direito Fundamental à Privacidade

Dentro do contexto de cidades inteligentes, já existem aplicações de inteligências artificiais e outros sistemas que poderiam mapear uma série de comportamentos sobre doenças que assolam os municípios. Além do contexto pandêmico do COVID-19, o Brasil, nos últimos anos, tem vivido um contexto de doenças sazonais como Dengue, Febre Amarela, Chicungunha, SARS, entre outras. O problema do uso extensivo de tecnologias para o auxílio ao combate de doenças, pode entrar em conflito com outros direitos fundamentais, como já visto, o direito fundamental à proteção de dados e à privacidade. Perante esse cenário, é importante analisar o julgamento da Ação Direta De Inconstitucionalidade 6.387 (BRASIL, 2020) e a Medida Provisória nº 954/2020 (BRASIL, 2020).

Para contextualizar esse conflito, diante da excepcionalidade da pandemia do COVID-19, foi aprovada a Lei nº 13.979, de 6 de fevereiro de 2020, que em sua ementa traz a seguinte redação: “dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019.” (BRASIL, 2019, s.p.).

Após ser outorgada, o presidente Jair Messias Bolsonaro editou a Medida Provisória nº 954/2020, que trata da produção estatística e do controle de

casos da doença. O então Ministro da Economia, Paulo Guedes, dentro da exposição dos motivos da mencionada Medida Provisória declarou:

> Para que seja viável uma adaptação metodológica dessa natureza, o IBGE necessita ter acesso a informações sobre o número de telefone e respectivo endereço residencial dos consumidores de serviços de telecomunicações, de pessoas naturais ou jurídicas. Tais informações possibilitarão a identificação dos domicílios (ou sede) que já constam na amostra da PNAD Contínua e o contato do respectivo responsável, ao qual aplicar-se-á a entrevista. Informações cadastrais adicionais, embora não sejam fundamentais, podem ser de grande valia para este processo, sem contudo o fornecimento ser revestido de caráter compulsório e, acaso fornecidas, guardarem o mesmo grau de sigilo e zelo (BRASIL, 2020, s.p.).

A ideia era clara: utilizar e cruzar os bancos de dados de todas as operadoras de telefonia com os dados daqueles que tiveram a doença, para rastrear a sua situação, se estavam respeitando a quarentena e as orientações transmitidas. A questão era: o que fazer com esses dados cruzados? Ou, mais do que isso: o que seria feito com esse grande banco de dados após a pandemia do COVID-19?

Diante dessas indagações, entende-se a necessidade de um ato inconstitucional e, assim, a Ordem dos Advogados do Brasil, o Partido da Social Democracia Brasileira (PSDB), o Partido Socialista Brasileiro (PSB), o Partido Socialismo e Liberdade (PSOL) e o Partido Comunista do Brasil (PC do B) entram, respectivamente, com as Ações de Declaração de Inconstitucionalidade nº 6387, 6388, 6389, 6390, 6393, concentradas e tendo como relatora a Ministra Rosa Weber.

Esta, em uma decisão monocrática, concedeu no dia 24 de abril de 2020, uma liminar *ad referendum* do Plenário do STF suspendendo a eficácia da Medida Provisória n. 954/2020. Diz o texto:

> Nesse contexto, e a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel, com o caráter precário próprio aos juízos perfunctórios e sem prejuízo de exame mais aprofundado quando do julgamento do mérito, defiro a medida cautelar requerida, ad referendum do Plenário desta Suprema Corte, para suspender a eficácia da Medida Provisória n. 954/2020, determinando, em consequência, que o Instituto Brasileiro de Geografia e Estatística – IBGE se abstenha de requerer a disponibilização dos dados objeto da referida medida provisória e, caso já o tenha feito, que suste tal pedido, com imediata comunicação à(s) operadora(s) de telefonia (BRASIL, 2020, s.p.).

Após concedida a liminar, nos dias 6 e 7 de maio de 2020, o Pleno, por maioria, referendou a medida cautelar deferida para suspender a eficácia da Medida Provisória nº 954/2020.

O aparente conflito entre o direito social à saúde, conforme descrito no artigo 6º da Constituição Federal (BRASIL, 2022), e os direitos fundamentais relacionados à intimidade e à vida privada, conforme o artigo 5º da Constituição Federal, inciso X (BRASIL, 2022), foi o responsável pelo embate que ocasionou todas as proposições de ADI. O Conselho Federal da Ordem dos Advogados do Brasil também acusa de violação direta aos artigos 1º, inciso III que asseguram a dignidade da pessoa humana, e 5º, inciso XII da Constituição Federal, que trata do sigilo dos dados e da autodeterminação informativa. Ao observar esse problema, o Ministro da Economia, Paulo Guedes, tentas justificar a escolha dessa metodologia a fim de defender o direito social à saúde e de reafirmar como o recolhimento dos dados das empresas de telefonia beneficiariam o controle do COVID-19. Segue a posição do Ministro, dentro da exposição de motivos da medida provisória:

> A garantia de realização da PNAD Contínua[1] reveste-se de especial relevância no presente momento, já que a pesquisa deverá ser veículo para a inclusão de quesitos relacionados ao monitoramento da pandemia de COVID-19 em todo o território nacional, orientando políticas públicas e o processo decisório nas mais distintas esferas. A capilaridade da pesquisa possibilitará o levantamento de dados representativos para diferentes níveis geográficos e de segmentos socioeconômicos (BRASIL, 2020, s.p.).

Portanto, diante dessa justificativa, entende-se que a metodologia realizada seria a de um cruzamento de dados da base interna do IBGE com os dados informados pelas empresas de telecomunicações a fim de promoverem as entrevistas. Conforme o que descreve o art. 2º da Medida Provisória 954/2020, parágrafo 1º:

> § 1º Os dados de que trata o **caput** serão utilizados direta e exclusivamente pela Fundação IBGE para a produção estatística oficial, com o objetivo de realizar entrevistas em caráter não presencial no âmbito de pesquisas domiciliares (BRASIL, 2020, s.p.).

É possível presumir que por meio dessas ligações, os dados a serem captados seriam em relação ao contágio da doença e também sobre os hábitos de ir e vir dentro da quarentena. Estendendo a possibilidade de cruzamento de dados com

[1] Pesquisa Nacional por Amostra de Domicílios Contínua.

a identificação das pessoas contaminadas, as informações fornecidas pelas empresas de telecomunicações poderiam facilitar o contato com os familiares, fazer o rastreio via entrevista dos lugares visitados e das pessoas com quem tiveram contato.

Em posse desses dados e ao analisa-los, o Governo Federal poderia criar políticas públicas com o objetivo de diminuir o grande impacto sanitário do COVID-19, e controlar de forma mais eficaz a doença e, diminuindo a superlotação dos hospitais e possibilitando a busca por outras soluções, temporárias ou permanentes, em relação ao tratamento da doença, consequentemente, diminuindo o número de mortos; sem esquecer dos outros atendimentos de saúde que também continuavam a acontecer durante a pandemia.

Diante disso, em resposta à possível gestão do Governo Federal decorrente do COVID-19, a Ministra Relatora, Rosa Weber, entende a importância da criação de políticas públicas, em conformidade com o dito no artigo 196 da Constituição Federal, efetivando o artigo 6º:

> Art. 196. A saúde é direito de todos e dever do Estado, garantido mediante políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário às ações e serviços para sua promoção, proteção e recuperação (BRASIL, 2022, s.p.).

Porém, para além desse entendimento, a Ministra Rosa Weber observa que a efetivação do direito social à saúde não pode ser feita de modo inconsciente, relativizando os outros direitos previstos na Constituição, como a proteção à vida privada e ao sigilo de dados. Diante disso, a Ministra escreve:

> Não se subestima a gravidade do cenário de urgência decorrente da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. O seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição (BRASIL, 2020, s.p.)

Diante dessa possibilidade de atropelos entre os direitos e reconhecendo o perigo do compartilhamento irresponsável de dados nas condições atuais da tecnologia, a Ministra Rosa Weber concedeu uma medida cautelar, que foi ratificada pelo Pleno, anulando o efeito da medida provisória. Contudo, dois pontos são importantes nessa análise: 1) utilizar uma “bala de canhão”, relativizando os graves problemas decorrentes desse compartilhamento de dados, inclusive, no âmbito

da saúde quando a privacidade não é respeitada e 2) a centralização da posse desses dados no Governo Federal.

O termo “bala de canhão” é derivado do ditado “matar mosca com bala de canhão”, e é utilizado quando uma medida para resolução de um problema cria um estrago maior do que o problema em si. Primeiramente, é preciso recordar que, por mais que os dados enviados pelas empresas de telecomunicações sejam cadastrais, eles ainda seriam cruzados com dados estatísticos do campo da saúde. Considerando esse fato, o banco de dados em si adquire o status de tratamento de dados sensíveis, conforme a LGPD, em seu artigo 5º, inciso II:

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> 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, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018, s.p.)

As diligências necessárias para administrar esse banco de dados, seriam de extrema complexidade, exigindo um alto grau de investimento em segurança da informação. Além disso, outra grave preocupação seria a necessidade de um planejamento para a observância da Seção IV da LGPD, que trata do término do tratamento de dados:

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada (BRASIL, 2018, s.p.).

Contudo, diante desse cenário, o grande ponto em questão é: ao decretar o término da pandemia e o fim da vigência da lei nº 13.979, de 6 de fevereiro de 2020 (BRASIL, 2020, s.p., que trata em seu artigo 8º: “esta Lei vigorará enquanto perdurar o estado de emergência internacional pelo coronavírus responsável pelo surto de 2019”; como será o término desse tratamento de dados ao perceberem que após o cruzamento das informações, juntamente com as novas pesquisas, o banco de dados em si se tornou algo novo e praticamente indistinguível?

Encontra-se aqui o segundo problema, derivado do primeiro, que é a centralização desses dados no Governo Federal, e o possível cruzamento desse

conteúdo sem uma boa justificativa para o seu tratamento, e principalmente, sem um relatório de impacto à proteção de dados.

Essas informações, futuramente, poderiam ser cruzadas com outros bancos de dados, como os policiais, os da Receita Federal, os do Denatran, entre outros. A plataforma gov.br já faz hoje essa junção de bancos, sob a justificativa de desburocratização, que com certeza é um item importante, porém, até o presente momento não foi disponibilizado um relatório de impacto à proteção de dados.

Diante desses problemas, pode-se traçar um paralelo com o que ocorreu na Alemanha. A Lei que organizou o senso de 1982 previa que cada cidadão deveria responder em torno de 160 perguntas, as quais teriam um tratamento de dados informatizado, podendo ser cruzados com o banco de dados de registros civis para retificação das informações; dados pseudoanonimizados poderiam ser enviados às autoridades federais e estavam sujeitos a uma alta multa. Doneda (2019, p. 167) expõe que essa legislação foi levada à Corte, pois havia um conflito com a *Bundesdatenchutzgesetz,* a lei de proteção de dados pessoais alemã, datada de 1977. Como resultado desse julgamento:

> Vários foram os motivos que levaram a Corte a reconhecer esta profunda incompatibilidade. Um deles foi a observação de que, caso os dados recolhidos fossem utilizados ao mesmo tempo para fins administrativos e estatísticos (Como na hipótese da retificação do registro civil a partir de dados do censo), estaria caracterizada a diversidade de finalidades, que impediria que o cidadão conhecesse o uso efetivo que seria feito de suas informações. Estas duas finalidades eram, além do mais, inconciliáveis, dado que o rigor estatístico não poderia coexistir com a necessidade dos órgãos administrativos de identificar os titulares destes dados. O Tribunal, desta forma, reconheceu a necessidade de se observar o princípio da finalidade na coleta de dados pessoais.

É possível fazer paralelos entre o julgamento da Ação Direta De Inconstitucionalidade 6.387 e a Medida Provisória nº 954/2020, com o censo alemão de 1982 e a sua incompatibilidade com a lei de proteção de dados pessoais alemã, e também com a possibilidade levantada de um cadastro técnico multifinalitário para a gestão de cidades inteligentes.

Perante o exposto, percebe-se que a única possibilidade desse banco de dados ser efetivo no auxílio à gestão de cidades inteligentes, seria uma total despersonalização das informações e o não cruzamento delas com os bancos de dados de cadastros civis. Contudo, esse feito só será alcançado por meio de uma boa anonimização de dados.

4.2 Anonimização de Dados

Diante dos problemas já destacados, pode-se pensar a solução de anonimização de dados a fim de termos estatísticas, de poder mapear doenças sazonais, epidemias e pandemias e, talvez, com muita diligência, de construir um cadastro técnico multifinalitário, conforme proposto pela Carta Brasileira de Cidades Inteligentes (BRASIL, 2021). A própria LGPD oferece essa opção dentro do seu artigo 12:

> Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
> § 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.
> § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada (BRASIL, 2018, s.p.).

Ter dados anonimizados por si só, segundo o artigo 12, afastaria a incidência da LGPD sobre eles, alcançando, assim, a finalidade pela qual é tratado: garantir estratégias relacionadas a saúde para um ganho na qualidade de vida.

Mesmo que se distancie a ocorrência da LGPD, o relatório de impacto à proteção de dados, além dos casos em que são utilizados o relatório de impacto à inteligência artificial, ainda são importantíssimos, efetivando o princípio da transparência, demonstrando os motivos em que a anonimização seria eficaz em afastar a atuação da LGPD e da publicidade, e também a eficiência em demonstrar os possíveis riscos que teríamos ao utilizarmos essas ferramentas.

Nesse sentido LIMA (2020, p. 234) pontua:

> Certamente sempre haverá “zona cinzenta” sobre essa questão, devendo determinado agente que desejar tratar dados como anonimizados ter extensa documentação acerca dos motivos pelos quais entende ter aplicado efetivamente técnicas de anonimização, diante da possibilidade de que outro controlador venha a “desanonimizar” determinados dados que, até então, eram entendidos como anônimos, especialmente na atual sociedade da informação tecnológica. Justamente por isso, já existem até mesmo manifestações acerca da impossibilidade de anonimizar dados atualmente.

Portanto, é preciso que mais de uma técnica de anonimização seja utilizada para alcançar os fins desejados. Abaixo serão apresentadas algumas opções que podem auxiliar nesse cadastro técnico multifinalitário, inclusive, para a gestão da saúde.

4.2.1 Anonimização por Supressão

A anonimização por supressão é uma das principais e mais brutas técnicas para a anonimização de dados. Nesse procedimento, retira-se uma coluna da tabela de dados para não fazer a identificação de algo.

Pode-se utilizar como exemplo, um cadastro de cidadãos que já testaram positivo para COVID-19, em que as colunas “NOME”, “ENDEREÇO” e “IDADE” são suprimidas, deixando exposto somente outras informações pertinentes para o mapeamento de informações. Esse tipo de coleta seria interessante, por exemplo, ao cruzar os dados totais de COVID-19 e separa-los por bairro, para uma visão mais ampla da disseminação. A *Personal Data Protection Commission Singapore* (Comissão de Proteção de Dados Pessoais de Singapura) trata essa técnica da seguinte maneira:

> 6.1. Description: Attribute suppression refers to the removal of an entire part of data (also referred to as “column” in databases and spreadsheets) in a dataset.
> 6.2. When to use it: When an attribute is not required in the anonymised dataset, or when the attribute cannot otherwise be suitably anonymised with another technique. This technique should be applied at the start of the anonymisation process, as it is an easy way to decrease identifiability at this point.
> 6.3. How to use it: Delete (e.g. remove) the attribute(s), or if the structure of the dataset needs to be maintained, clear the data (and possibly the header). Note that the suppression should be actual removal (i.e. permanent), and not just ‘”hiding the column”. Similarly, ‘redacting’ may not be sufficient if the underlying data remains somewhat accessible (PERSONAL DATA PROTECTION COMISSION, 2018, s.p.).[2]

[2] 6.1. Descrição: A supressão de atributo refere-se à remoção de uma parte inteira dos dados (também referido como "coluna" em bancos de dados e planilhas) em um conjunto de dados.
6.2. Quando usar: Quando um atributo não é obrigatório no conjunto de dados anônimos, ou quando o atributo não pode ser adequadamente anonimizado com outra técnica. Isto técnica deve ser aplicada no início do processo de anonimização, pois é uma maneira de diminuir a identificabilidade neste ponto.
6.3. Como usar: Excluir (por exemplo, remover) o(s) atributo(s), ou se a estrutura do conjunto de dados precisa ser atualizada, limpe os dados (e possivelmente o cabeçalho). Observe que a supressão deve ser a remoção real (ou seja, permanente), e não apenas “esconder a coluna”. Da

Como afirmado anteriormente, a “supressão de dados” é o modo mais bruto dentre as técnicas de anonimização, por deletar colunas e informar somente os dados necessários. O problema desse método é medir se somente as colunas deletadas têm o efeito de anonimizar os dados ou se é possível a reversão destes para pessoaliza-los, conforme o parágrafo 1º do artigo 12 (BRASIL, 2018).

4.2.2 Anonimização por Generalização

A anonimização por generalização junta os dados de uma coluna numa única definição mais genérica. Um exemplo dessa técnica seria a generalização de bairros próximos a partir de “zonas”, assim como no caso de referenciar os bairros Iguatemi, Itaquera, José Bonifácio, Mooca, Parque Ecológico, Penha, Sapopemba, Vila Carmosina, Vila Curuçá, Vila Ema e Vila Prudente de São Paulo/SP, e generalizá-los na coluna com o nome “Zona Leste”, parametrizando toda a região, e claro, retirando as referências de cada um dos bairros. A *Personal Data Protection Commission Singapore* (Comissão de Proteção de Dados Pessoais de Singapura) trata essa técnica da seguinte maneira:

> 10.1. Description: a deliberate reduction in the precision of data. E.g. converting a person’s age into an age range, or a precise location into a less precise location. This technique is also referred to as recoding.
> 10.2. When to use it: for values that can be generalised and still be useful for the intended purpose.
> 10.3. How to use it: Design appropriate data categories and rules for translating data. Consider suppressing any records that still stand out after the translation (i.e. the generalisation) (PERSONAL DATA PROTECTION COMISSION, 2018, s.p.).[3]

É perceptível o aumento do poder computacional no processamento de dados, generalizando-os e programando os padrões de generalização. Portanto,

---

mesma forma, 'editar' pode não ser suficiente se os dados subjacentes permanecerem um tanto acessível.

[3] 10.1. Descrição: uma redução deliberada na precisão dos dados. Por exemplo, a conversão de uma pessoa idade em uma faixa etária, ou um local preciso em um local menos preciso. Esta técnica também é referida como recodificação.
10.2. Quando usar: para valores que podem ser generalizados e ainda serem úteis para o objetivo pretendido propósito.
10.3. Como usar: Projete categorias de dados e regras apropriadas para traduzir dados. Considere suprimir quaisquer registros que ainda se destaquem após a tradução (ou seja, a generalização).

em um banco de dados robusto, essa técnica deve ser calculada para verificar o real poder computacional na resolução do problema apresentado.

4.2.3 Anonimização por Perturbação

Neste tipo de técnica, os dados são perturbados: inicialmente, seus valores são modificados e ao fim de uma análise, todas as informações permanecem semelhantes. Pode-se ilustrar esse método trocando, por exemplo, o nome “Ricardo” para “Pedro”, alterando o endereço, de “Rua das Águias” para “Rua das Andorinhas”, e trocando o número da casa, de 37 para 54. Ao perturbar o banco de dados como um todo, torna-se muito difícil pessoalizar as informações, porém não impossível. A *Personal Data Protection Commission Singapore* (Comissão de Proteção de Dados Pessoais de Singapura) trata essa técnica da seguinte maneira:

> 12.1. Description: the values from the original dataset are modified to be slightly different.
> 12.2. When to use it: for quasi-identifiers (typically numbers and dates) which may potentially be identifying when combined with other data sources, and slight change in value are acceptable. This technique should not be used where data accuracy is crucial.
> 12.3. How to use it: it depends on the exact data perturbation technique used. These include rounding and adding random noise. The example in this section shows base-x rounding (PERSONAL DATA PROTECTION COMISSION, 2018, s.p.).[4]

É possível observar que se cria uma situação em que os dados importantes são preservados, e aqueles que podem identificar alguém são perturbados. Contudo, há uma fragilidade: quando um atacante percebe que as informações foram perturbadas, pode começar um cruzamento de dados para os repessoalizar.

Por fim, ao observar três das principais técnicas de anonimização de dados, sem excluir o fato de que existem outras, nota-se a necessidade do estudo de

---

[4] 12.1 Descrição: os valores do conjunto de dados original são modificados para serem ligeiramente diferentes.
12.2. Quando usar: para quase-identificadores (normalmente números e datas) que podem potencialmente identificar quando combinado com outras fontes de dados, e pequenas alterações em valor são aceitáveis. Esta técnica não deve ser usada onde a precisão dos dados é crucial.
12.3. Como usar: depende da técnica exata de perturbação de dados usada. Esses incluem arredondamento e adição de ruído aleatório. O exemplo nesta seção mostra o arredondamento base- *x*.

cada uma delas, de sua viabilidade computacional e, principalmente, da possibilidade de combinação entre todas.

Em função do exposto, é necessário ressaltar mais uma vez o relatório de impacto à proteção de dados, a fim de assegurar que as técnicas de anonimização de dados não possibilitem a identificação das pessoas, recaindo novamente na incidência da LGPD.

4.3 Soluções para Cidades Inteligentes no Campo da Saúde

Abaixo são citadas algumas soluções que podem ser implementadas em cidades inteligentes, sempre reforçando a necessidade de o encarregado de dados supervisionar, entender as ferramentas, verificar as bases legais de tratamento de dados e oferecer a segurança necessária no momento em que as informações pessoais são tratadas.

4.3.1 Iluminação Pública e Poluição Luminosa

O ser humano tem se exposto cada vez mais a luzes artificiais, como telas de celulares, de computadores, de televisores etc. No contexto de cidades inteligentes, existem estudos que apontam que essa luminosidade, inclusive as que são utilizadas para a iluminação pública, pode ser uma das causas de distúrbios, principalmente, relacionados ao sono.

Um exemplo da interferência da luz artificial no ambiente natural, é a difícil observação do céu estrelado no meio urbano, devido ao excesso dessa iluminação; além dos postes, pode-se incluir os *outdoors* publicitários e outros meios luminosos. A Carta Brasileira de Cidades Inteligentes assim pontua sobre esse ponto:

> Sustentabilidade em iluminação pública: Elevar os padrões de eficiência energética e poluição luminosa (poluição gerada pelo excesso de luz artificial) em projetos de modernização e expansão da rede de iluminação pública. Promover a gestão eficiente do serviço por meio da adoção de soluções digitais integradas à rede. O objetivo é minimizar impactos da prestação do serviço de iluminação pública no meio ambiente e na saúde humana, assim como melhorar a qualidade de vida das pessoas nas cidades (BRASIL, 2021, p. 55-56).

É interessante mencionar que a medição de luminosidade pode ser feita por meio de drones, mas esse assunto será aprofundado em um capítulo específico sobre o tema. No momento, o mais importante é ter consciência de que na construção de cidades inteligentes, a qualidade de vida e o cuidado com o meio ambiente devem ser o ponto de partida para todos os tipos de planejamentos.

4.3.2 Intersetorialidade no Nível Local

No campo administrativo, a governança de processos e de dados é de suma importância para o gerenciamento de cidades inteligentes. Como já visto, nenhuma área é isolada; saúde e segurança caminham juntas, assim como, educação e lazer, e diversos outros campos. Logo, por meio da intersetorialidade, deve-se buscar um planejamento amplo para a gestão.

Quando se fala em saúde, por exemplo, sabe-se que a necessidade de atendimento não se restringe a apenas uma cidade, mas diz respeito a toda uma região metropolitana que depende desse sistema; daí advém o conceito de “hospital de referência”. Ao utilizar programas e, principalmente, processos que otimizem esses atendimentos, possibilita-se um grande avanço na qualidade de vida de toda uma região e ainda na otimização de espaço e tempo.

A Carta Brasileira de Cidades Inteligentes pontua da seguinte maneira:

> Intersetorialidade no nível local: Estabelecer espaços institucionais para cooperação e atuação intersetorial (cooperação entre as diferentes áreas de política pública), inclusive entre órgãos de municípios diferentes (escala supramunicipal). O objetivo é facilitar que as políticas, planos e programas de desenvolvimento urbano e de setores relacionados sejam implementados de forma integrada no território. Incluir ações de diferentes setores: por exemplo, habitação, saneamento básico (abastecimento de água potável, esgotamento sanitário, limpeza urbana e manejo de resíduos sólidos, drenagem e manejo das águas pluviais urbanas), mobilidade urbana, segurança hídrica, redução de desastres, meio ambiente, saúde, educação, segurança urbana. Adotar abordagem contínua e incremental para alcançar a integração (BRASIL, 2021, p. 72).

Sob o ponto de vista da LGPD, nesse sistema, não há a necessidade de comunicação com qualquer outro banco de dados, para alcançar a sua finalidade.

4.3.3 Gestão da Medicina da Família

Outro ponto a se considerar, quando se fala sobre saúde em cidades inteligentes, são as soluções para os médicos que visitam famílias. É preciso otimizar a logística de acordo com a prioridade, diminuindo custos e a tornando mais eficaz. Por meio de *software* treinado, uma boa solução seria a organização das casas de um bairro que precisam ser visitadas, em rotas logisticamente pensadas. A partir da lista de prioridades, o *software* poderia apontar as reais necessidades e calibrar um algoritmo que estabeleça uma rota de acordo com a urgência de cada caso.

Cabe ao controlador de dados a responsabilidade de entender como o *software* planeja essa logística e relatar ao titular de dados sempre que requisitado. É preciso ainda pensar em outros pontos de cuidado: os níveis de acesso e a disponibilidade das informações, além de uma forte tomada de decisão, investindo em segurança da informação e treinamento de todos os usuários.

Ademais, pode-se ainda adentrar na gestão de dados sensíveis, como os de anamnese e também os prontuários eletrônicos, que devem ser manuseados respeitando-se legislações específicas desses casos específicos.

4.3.4 Saneamento Básico, Coleta De Lixo E Outros Itens

Neste tópico, considera-se os pontos de intersecção entre saúde e infraestrutura. Por exemplo, o gerenciamento de saneamento básico digital pode auxiliar no controle de rotas de água e esgoto, assim como na sua criação, otimizando o acesso dos bairros a esses recursos. Dentro do planejamento de cidades inteligentes, todos os apontamentos apresentados ganham relevância, pois cada ação social, seja pequena ou grande, agrega valor à vida das pessoas e contribui na qualidade de vida, consequentemente, interferindo positivamente nos indicadores da área da saúde.

Em relação à coleta de lixo, pode ser considerada uma alternativa semelhante à introduzida no item anterior: construir gráficos que otimizem esse processo, coletando mais lixo em menos tempo. Com o avançar da tecnologia, o trabalho autônomo nesse recolhimento também pode ser incluído no planejamento, sem perder de vista que o despejo faz parte do hábito humano e é uma parte que

precisa ser estudada e pensada de forma conjunta com as outras estratégias sociais de melhoria da qualidade de vida dos cidadãos.

5 MOBILIDADE URBANA

A área de mobilidade urbana talvez seja a mais avançada no quesito de cidades inteligentes. A curva de inovação desse campo começa desde a evolução dos carros autônomos, caminhões, ônibus, drones e de outros meios de transporte, até o uso de semáforos inteligentes e de gestão de tráfego por meio de inteligência artificial; e tende a crescer muito mais perante o avanço do 5G e da diminuição do tempo de resposta quando solicitada uma informação.

Nesta seção, o propósito é visualizar as possibilidades de avanço em relação a mobilidades e de como os dados pessoais devem ser tratados, diante da intensa troca de informações entre os bens móveis e a própria cidade.

5.1 CARROS AUTÔNOMOS

Na década de 1980, a série “A Super Máquina” destacou-se ao trazer um carro como personagem principal. A história se pauta na dinâmica típica norte-americana da “dupla de agentes”, mas no seriado o parceiro de Michael Knight (David Hasselhoff) é um carro, o K.I.T.T., ou *Knight Industries Two Thousand*, resultado do projeto *Knight Automated Roving Robot* (Robô Cavaleiro Revolucionário Automático). O automóvel funciona a partir de uma inteligência artificial tão avançada ao ponto de praticamente possuir uma personalidade própria. Outros exemplos, como de “A Super Máquina”, em que se pode vislumbrar carros autônomos, não faltam: se utilizar bastante a imaginação, pode-se pensar em *Herbie*; o Batmóvel é quase um personagem dentro das histórias do Cavaleiro das Trevas; e em Os Jetsons, é possível admirar os carros voadores, que podem ser dirigidos sem a presença de um motorista – algo que, nos dias de hoje, assemelha-se aos drones tripulados autônomos. Essas tecnologias já são consideradas há muito tempo e conforme esse campo vai se desenvolvendo e evoluindo, pode-se contemplar resultados promissores e aplicações práticas.

Por definição, carros autônomos são automóveis totalmente conduzidos via algoritmos e sensores, levando algo ou alguém do ponto A ao ponto B. O Ministério da Infraestrutura conceitua o veículo autônomo como aquele que “pode executar suas funções de maneira automatizada, sendo capaz, inclusive, de percorrer

sozinho determinado trajeto, detectando obstáculos presentes no trânsito” (BRASIL, 2020, s.p.). Ademais, possuem níveis de automação, como o Departamento de Transportes Norte-americano (UNITED STATES, 2018, p. 8) trata:

> 0 - No Automation: The full-time performance by the human driver of all aspects of the dynamic driving task, even when enhanced by warning or intervention systems.
> 1 - Driver Assistance: The driving modespecific execution by a driver assistance system of either steering or acceleration/ deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task.
> 2 - Partial Automation: The driving modespecific execution by one or more driver assistance systems of both steering or acceleration/ deceleration using information about the driving environment and with the expectation that the human driver perform all remaining aspects of the dynamic driving task.
> 3 - Conditional Automation: The driving modespecific performance by an automated driving system of all aspects of the dynamic driving task with the expectation that the human driver will respond appropriately to a request to intervene.
> 4 - High Automation: The driving modespecific performance by an automated driving system of all aspects of the dynamic driving task, even if a human driver does not respond appropriately to a request to intervene.
> 5 - Full Automation The full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver.[5]

Contudo, diante desse tipo de abordagem em níveis de automação, é importante também confrontar o nível de autonomia e responsabilização de cada agente, seja ele o programador, a montadora, a cidade ou o consumidor. Perante esse impasse, Crivilim (2020, p. 78) discorre da seguinte maneira:

---

[5] Tradução nossa: 0 - Sem Automação: A direção é feita por um motorista humano em tempo integral, sendo este responsável por todos os aspectos da tarefa de condução dinâmica, mesmo quando aprimorado por sistemas de alerta ou intervenção.
1 - Assistência ao Condutor: A execução específica do modo de condução por um sistema de assistência ao condutor de direção ou aceleração/desaceleração usando informações sobre o ambiente de condução e com a expectativa de que o condutor humano realize todos os aspectos restantes da tarefa de condução dinâmica.
2 - Automação Parcial: A execução específica do modo de condução por um ou mais sistemas de assistência ao motorista tanto de direção quanto de aceleração/desaceleração usando informações sobre o ambiente de condução e com a expectativa de que o motorista humano realize todos os aspectos restantes da tarefa de condução dinâmica.
3 - Automação Condicional: O desempenho específico do modo de condução por um sistema de condução automatizado de todos os aspectos da tarefa de condução dinâmica com a expectativa de que o motorista humano responderá adequadamente a um pedido de intervenção.
4 - Alta Automação: O desempenho específico do modo de condução por um sistema de condução automatizado de todos os aspectos da tarefa de condução dinâmica, mesmo que um motorista humano não responda adequadamente a um pedido de intervenção.
5 - Automação Total: O desempenho em tempo integral por um sistema de condução automatizado de todos os aspectos da tarefa de condução dinâmica sob todas as condições da estrada e ambientais que podem ser gerenciadas por um motorista humano.

> Hipoteticamente, se temos um dano causado por uma inteligência artificial ou um autômato, no caso um veículo dotado de autonomia. Se houver um atropelamento, tal como já ocorreu na América do Norte (já citado neste trabalho), caso o proprietário do veículo seja responsabilizado pelo ressarcimento dos danos, pode, em regresso, exigir que o fabricante lhe ressarça pois, nesta hipótese, há uma clara e absoluta violação às leis básicas da robóticas (que devem ser positivas no ordenamento pátrio), pois o fabricante deve, sempre, criar mecanismos suficientes para que o autômato não cause, em nenhuma hipótese, danos à vida humana. Contudo, neste caso, excluindo eventual dano à um ser humano, teríamos que o fornecedor pode se eximir da responsabilidade civil, se conseguir demonstrar que não há nexo de causalidade entre sua criação e o dano e que ocorreu, em verdade, uma má-utilização do "produto" ou uma falha (ou até mesmo dolo) do ordenador do ato.

Em face desses questionamentos relacionados a potenciais danos, é que temos essa majoração de níveis de carros autônomos. Um nível 5, por exemplo, pode ser uma grande caixa preta, no sentido de não ter autonomia alguma quanto a qualquer manutenção, física ou de *software*, mas basta levar o carro até a concessionária para as devidas revisões mecânicas. Exigir do consumidor que ele entenda de programação para dirigir o seu carro a fim de evitar um dano é algo irreal e dificultará a reparação dos danos.

É preciso majorar no nível 0, exceto nos casos em que danos são ocasionados por falha na fabricação de um carro, da mesma forma que um nível 5 é quase impossível, o qual pode ser confrontado somente quando há uma falta de atualização ou por não levar o carro para as manutenções nos prazos corretos, cuja responsabilidade é do fabricante.

5.2 DRONES

A classificação de drone é realmente complicada. Como visto anteriormente, aquilo que encontramos na série "Os Jetsons" poderia ser considerado um drone, ou seja, um veículo autônomo, que voa e transporta passageiros. Em nosso dia a dia, o que normalmente nomeamos como drones são equipamentos, que possuem pás de hélice, controlados por controle remoto e que voam. Existem também exemplos que antes chamaríamos de barcos e, ainda, drones aquáticos que lembram submarinos.

Para facilitar a nomenclatura de cada um desses equipamentos, talvez fosse necessário utilizar os nomes que já estavam presentes em nosso

vocabulário e acrescentar um adjetivo próprio, como “barco por controle remoto”, “barco autônomo”, “submarino por controle remoto”, “submarino autônomo”, “mini-submarino” etc.

Neste trabalho, a definição de drone está centralizada no conceito já denominado como veículo aéreo, não tripulado, controlado remotamente ou de forma autônoma. Dentro do site da ANAC temos a seguinte categorização:

> A ANAC criou regras para as operações civis de aeronaves não tripuladas, também conhecidas como drones. [...]
> Pelo regulamento da ANAC, aeromodelos são as aeronaves não tripuladas remotamente pilotadas usadas para recreação e lazer e as aeronaves remotamente pilotadas (RPA) são as aeronaves não tripuladas utilizadas para outros fins como experimentais, comerciais ou institucionais.
> Os dois tipos (aeromodelos e RPA) só podem ser operados em áreas com no mínimo 30 metros horizontais de distância das pessoas não anuentes ou não envolvidas com a operação e cada piloto remoto só poderá operar um equipamento por vez (BRASIL, 2022, s.p.).

Ainda conforme a ANAC, nos Requisitos Gerais Para Aeronaves Não Tripuladas de Uso Cívil, Emenda 2 (RBAC-E nº 94), datado de 2021, o conceito é dado como “aeronaves não tripuladas de uso civil (doravante denominadas apenas de aeronaves não tripuladas) capazes de sustentar-se e/ou circular no espaço aéreo mediante reações aerodinâmicas” (BRASIL, 2021. p. 4). Há no Brasil, ao todo, o registro de 71.963 drones, sendo 65.765 de pessoas físicas e 6.198 de pessoas jurídicas.

Suas aplicações são diversas em cidades inteligentes, desde segurança pública até educação, mas o foco é o ganho dentro da área de mobilidade urbana. Cada vez mais, os drones serão utilizados para entregas de produtos, visto que são mais ágeis do que via trânsito terrestre. Ainda mais, aproveitando a verticalização das cidades, pode ser uma grande alternativa para entregas pela sacada do prédio ou por lugares mais acessíveis.

Um exemplo dessa aplicação seria o *delivery* de uma pizza diretamente na varanda de um apartamento, sem precisar que o morador desça do apartamento para recebê-la e com a garantia de que a comida chegará na temperatura ideal. Conforme reportagem do Globo.com, a empresa iFood já se prepara para a operação:

> Entregas comerciais poderão ser realizadas via drones no Brasil, inclusive de alimentos, autorizou a Agência Nacional de Aviação Civil (Anac) nesta sexta-

> feira (21). Com isso, o iFood, em parceria com a Speedbird Aero, será a primeira empresa das Américas a realizar delivery neste modal em todo o território brasileiro.
> A permissão, que é a primeira do tipo no país, se restringe ao modelo DLV-1 NEO, em rotas BVLOS, ou seja, além da linha visual do piloto. O drone deverá percorrer apenas distâncias de até 3 km, com cargas de até 2,5 kg (G1, 2021, s.p.).

No caso, a operação é iniciada por um entregador que retira o pedido de um local e, somente na etapa final, a entrega é feita pelos drones. As encomendas são levadas até um *droneport* (área específica e segura para pousos e decolagens de drones) e entregues ao consumidor.

5.3 Transporte Público

Uma categoria à parte do assunto discutido nesta seção, é a questão do transporte público movido em relação a dados estatísticos. É preciso verificar aqui a necessidade de mudanças quanto ao gerenciamento do transporte público sob o ponto de vista do bem-estar das pessoas.

Com o avançar do tempo, as cidades inteligentes deverão utilizar cada vez mais aplicativos de transportes, como Uber, 99, Lift, entre outros, em detrimento de ter carro próprio com todas as suas obrigações: manutenção, combustível, IPVA, estacionamento etc.

Ônibus e metrôs também podem aos poucos aperfeiçoar a logística dos itinerários e das rotas quanto à localidade dos moradores e também aos horários de maior circulação, distribuindo-os de maneira mais inteligente. Ainda mais, apenas frotas de ônibus e trens autônomos supervisionados pela central devem fazer parte do dia a dia.

Todos esses pontos compõem inovações importantes para a gestão da mobilidade urbana.

5.4 Há a Necessidade de uma Autoridade Reguladora de Novas Tecnologias?

Visto o cenário brasileiro, foi escolha do legislador criar uma Autoridade Nacional de Proteção de Dados, sendo um órgão da administração pública

federal ligado à Presidência da República. Foi dada à ANPD autonomia para editar normas relacionadas à proteção de dados e na tomada de decisões relacionadas a abusos ou a danos causados pelo tratamento indevido de dados.

Desde o início do vigor da LGPD havia uma previsão de uma revisão do papel e da autonomia da ANPD, conforme o artigo 55-A:

> Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.
> § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.
> § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD.
> § 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias (BRASIL, 2018, s.p.).

Com esta possibilidade, no dia 13 de junho de 2022, o presidente da república através da Medida Provisória nº 1.124/2022 transformou a Autoridade Nacional de Proteção de Dados em uma autarquia de natureza especial, dados assim mais autonomia, dando a ela uma maior estabilidade jurídica e promovendo proteção contra ingerências políticas dentro da autoridade. Posteriormente, a Medida Provisória foi convertida na Lei nº 14.460/2022.

Verificado todo este ganho de autônoma que a ANPD recebeu, é importante discutir todos esses pontos sob um ponto de vista técnico, pois pode-se abrir um caminho em direção à inovação possibilitando o uso da inteligência artificial, de estruturas baseadas na *internet* das coisas, dos carros autônomos e de outras novas tecnologias que vão surgindo com o tempo. A ANPD, conforme a evolução das tecnologias, deveria abarcar em seu escopo somente os pontos específicos relacionados a coleta e tratamento de dados pessoais ou deveria absorver outras demandas de regulações tecnológicas?

Para analisar esta pergunta, desde o princípio, já há a necessidade de um órgão supervisionando e regulando o que é criado e transformado por meio dessas tecnologias e o impacto que elas causam. Além disso, o conhecimento necessário para esse fim é específico, portanto, é imprescindível a criação de uma

autoridade gestora qualificada em gerenciar os danos, as faltas e também editar normas.

O problema dessa operação de supervisionar e regular dentro desta autoridade reguladora é a compatibilidade do controle dessas novas tecnologias com a velocidade da inovação. Sempre houve a preocupação dos juristas sobre como o direito se comportaria diante da agilidade com que as tecnologias têm evoluído.

Observando que as novas tecnologias, em sua maioria, se baseiam na massiva coleta de dados e de um tratamento especifico do mesmo, sejam estes dados pessoais ou não, dar ainda mais poderes a ANPD seria uma possibilidade de já utilizar uma estrutura que esta em fase inicial de ganhar um protagonismo para a proteção dos interesses do Brasil diante das novas tecnologias.

Existe ainda uma segunda alternativa, talvez mais assertiva em relação à primeira, na qual cada órgão específico deveria ser o responsável por editar as normas de suas áreas.

Um exemplo seria o Conselho Federal de Medicina editar as normas específicas sobre o uso de tecnologias dentro de suas competências, determinando se é admissível a criação de médicos digitais embarcados com inteligência artificial para a realização de casos mais simples, ou o uso de equipamentos como braços robóticos autônomos ou nanotecnologia para cirurgias e outros procedimentos.

A partir do momento que houver uma legislação aplicada na prática a respeito de determinada tecnologia, o INMETRO pode ser o órgão a executar políticas nacionais de qualidade, com uma metodologia adequada para analisar a capacidade de construção de uma inteligência artificial antes de ser disponibilizada. Em conformidade a isso, o próprio INMETRO, dentro do seu novo plano estratégico de 2021-2023 coloca essa perspectiva como um dos objetivos:

> O Inmetro, dentro desta realidade, tem um enorme desafio a superar para se reafirmar como uma organização que trabalha tecnologia, qualidade e confiança. Para isso, necessita se transformar. Não se trata de mudar por mudar, mas de realizar uma transformação planejada com objetivos bem definidos, sabendo aonde se quer chegar. Suas variadas formas de atuação podem ser resumidas em dois grandes grupos: o apoio tecnológico às organizações e o apoio ao funcionamento dos mercados. Verifica-se a necessidade da mudança nestes dois grandes campos: as organizações estão se transformando radicalmente e o mercado também. Portanto, o Inmetro precisa se transformar para atender as necessidades geradas por esta nova realidade. Conectividade, internet das coisas, biotecnologia, cibernética, robótica são necessidades fundamentais para o desenvolvimento do país, e o Instituto tem que responder estas novas demandas com uma atuação ousada, corajosa e voltada para gerar valor para a sociedade. O

> Inmetro deve ser uma caixa de ferramentas para o setor produtivo e para o mercado. Como caixa de ferramentas, tem que estar bem atento ao que este imenso público precisa para o momento. Em outras palavras, tem que se tornar o Inmetro 4.0.

Além do INMETRO, o Conselho Federal da Ordem dos Advogados do Brasil, o Conselho Federal de Engenharia e Agronomia, entre outros órgãos de classe, têm a possibilidade e a prerrogativa de criar normas específicas em suas áreas, focando em suas necessidades.

Como se sabe, para questões relacionadas à proteção de dados existe a ANPD, que pode, por meio do relatório de impacto à proteção de dados, requerer informações sobre o uso de decisões automatizadas e solicitar adequações a elas, como visto no artigo 20 da LGPD, antes do seu funcionamento e, adentrando no artigo segundo, poderia inclusive fazer uma auditoria, conforme o parágrafo 2º:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (BRASIL, 2018, s.p.).

Mas, em se tratando do conceito de mobilidade dentro de cidades inteligentes, o ponto principal seria verificar as possibilidades de gerenciamento de carros autônomos e também do uso de drones.

Já está presente dentro da Agenda Regulatória do Departamento Nacional de Trânsito (DENATRAN) para o biênio 2021-2022 (BRASIL, 2020), a regulamentação dos veículos autônomo, dentro da ótica da mobilidade e da engenharia, sob a responsabilidade da Coordenação-Geral de Segurança no Trânsito (CGST). Conforme pesquisa, não foram encontradas maiores informações, mas com o que foi exposto pode-se estabelecer um norte de como regularizar carros autônomos em nosso país.

Nenhum órgão regulamentador entende mais de veículos que o DENATRAN, o qual é responsável pelo estudo e pela escolha de como regulamentar cada sistema que compõe o complexo método de criação de veículos autônomos.

Outro ponto importante em relação à mobilidade urbana em cidades inteligentes é o uso de drones, principalmente, aqueles que devem ser utilizados para entregas. Atualmente, a responsabilidade por essa regulamentação é de três órgãos reguladores, conforme descrito por VARGAS (2021, p. 28):

> Quanto a esse último aspecto, salienta-se a atuação de três órgãos principais, são eles: a Agência Nacional de Aviação Civil (ANAC), a qual compete o cadastro de aeronaves, exploradores/operadores/pilotos, e observadores de aeronave não tripulada, a Agência Nacional de Telecomunicações (ANATEL), a qual compete a homologação das aeronaves não tripuladas a fim de evitar interferências não só em serviços de telecomunicações, como também em frequências destinadas a outras aeronaves, e o Departamento de Controle do Espaço Aéreo (DECEA), ao qual compete o acesso ao espaço aéreo.

Dessas três organizações, o mais importante, sob o ponto de vista de cidades inteligentes e da mobilidade urbana, seria o DECEA e o estabelecimento de como devem ser as áreas de voos dos dispositivos e qual a altura permitida, para que haja essas previsões dentro do plano diretor e de decretos municipais que possam regular essas manobras.

Também seria importante a regulação não somente dos drones controlados, mas também dos autônomos, para facilitar as questões relacionadas a entregas quando feitas em alta escala.

Seja a ANPD ganhando uma maior estrutura para poder supervisionar e regular novas tecnologias, seja cada órgão regulador, em sua área específica, trabalhar em conjunto com a ANPD quando as tecnologias envolverem dados pessoais, ou ainda, seja a criação de uma autoridade nacional específica que trate das evoluções tecnológicas e de sua regulação, articulando cada um dos interesses dos órgãos de classe em suas áreas de autonomia, será necessária uma mudança na legislação brasileira para evoluirmos as possibilidades quanto ao uso destas tecnologias.

5.5 O RESPEITO À LGPD DENTRO DA MOBILIDADE URBANA

Este é mais um caso de necessidade de cuidados relacionados à proteção de dados por meio do uso de tecnologias.

Segundo a engenheira Kathy Winter (2017, s.p.) da Intel Corporation, os carros autônomos produzem uma quantidade imensa de dados diariamente, estima-se em torno de 4 terabytes de dados por dia:

> Antes que nada, ¿por qué ese número? Cuatro terabytes es el volumen estimado de datos que va a generar un coche autónomo en aproximadamente una hora y media de conducción, la cantidad de tiempo que una persona típica pasa en su coche cada día. [...]
> Si lo interesante de los datos creados por un coche autónomo fuera simplemente la cantidad, 4 TB no sería del todo fascinante, sin embargo, lo que hace que los datos “sean el nuevo petróleo” para la conducción autónoma y lo que hace que sean un verdadero desafío, es nuestra necesidad de darles sentido para convertirlos en conocimiento práctico que permita los automóviles pensar, aprender y actuar sin la intervención humana. Los datos permiten a los coches autónomos conducir y evitar hasta en un 90% los accidentes causados por errores humanos, haciendo que sean cosa del pasado.[6]

Com essa quantidade de dados, há uma situação peculiar de um carro constituído praticamente de uma caixa preta, em que o dono possui quase nenhuma ingerência sobre os dados produzido, exceto sua rota. É uma proteção de dados pessoais executada de maneira diferente, mas que precisa ser feita pelo fabricante, pois o usuário não conseguirá controlar totalmente o sistema e ainda tem direitos conforme a LGPD, como a autodeterminação informativa.

Soma-se ainda à discussão outros questionamentos: quais dados serão geridos internamente pelos carros autônomos; quais dados serão enviados à nuvem do fabricante para o processamento de informações; quais dados deverão ser descartados após o seu uso; e também quais desses dados serão compartilhados

---

[6] Em primeiro lugar, por que esse número? Quatro terabytes é o volume estimado de dados que um carro autônomo gerará em cerca de uma hora e meia de condução, a quantidade de tempo que uma pessoa comum passa em seu carro todos os dias. [...]
Se o interessante sobre os dados criados por um carro autônomo fosse simplesmente a quantidade, 4 TB não seria tão empolgante, no entanto, o que torna os dados "o novo petróleo" para direção autônoma e o que o torna um verdadeiro desafio nossa necessidade de entendê-los para transformá-los em conhecimento prático que permita que os carros pensem, aprendam e ajam sem intervenção humana. Os dados permitem que os carros autônomos dirijam e evitem até 90% dos acidentes causados por erro humano, tornando-os coisa do passado

com os carros próximos, em especial, com os sistemas gestores de cidades inteligentes.

É previsível que haja a possibilidade dessas trocas de informações, principalmente, para que o controle da cidade possa calcular a quantidade de carros nas ruas e quais rotas estão sendo utilizadas, e também melhorar as vias de acesso.

Já em relação aos drones, é preciso atenção redobrada, pois podem realizar gravações e o rastreio de informações não somente do consumidor, mas de terceiros. Observando o caso anterior, sobre a entrega, levanta-se algumas indagações: um drone que faz um *delivery* no sétimo andar, captará as informações dos outros andares? Qual a capacidade de seus sensores quanto a isso? Qual o destino das gravações de vídeo? Como que fica o controle de privacidade de alguém do sexto andar, por exemplo, diante de uma requisição de dados e de um possível pedido de deleção dos arquivos relacionados ao voo realizado em seu andar, captando imagens, referenciamentos e mapeamentos daquele local? São perguntas necessárias de serem feitas e que as respostas devem estar no Relatório de Impacto de Proteção de Dados Pessoais.

6 UMA INTELIGENCIA ARTIFICIAL À FRENTE DE UMA CIDADE INTELIGENTE

Com o avançar da tecnologia, é muito improvável que um ser humano dê conta de todas as decisões feitas dentro de uma cidade inteligente, principalmente, observando o processo de barateamento e miniaturização dos sensores que avaliam os sistemas dentro de uma cidade inteligente. Portanto, o uso de inteligência artificial é uma medida viável, otimizando o gerenciamento.

6.1 UMA INTELIGÊNCIA ARTIFICIAL ÚNICA OU UM CONJUNTO DE IA'S

A inteligência artificial (IA) é um tema complexo dentro de seu campo de estudo, cuja engenharia tecnológica conjugada com saberes de neurociência é, do ponto de vista do presente e do futuro, extremamente necessária para sustentar toda a infraestrutura de uma cidade inteligente. Em vista disso, a fim de compreender a sua relação com a escolha desse sistema, é preciso adentrar a história da IA.

Para conceituar inteligência artificial, George Luger utilizou um conceito amplo, não como um sistema ou uma ferramenta, mas como campo de estudos. "Inteligência artificial (IA) pode ser definida como o ramo da ciência da computação que se ocupa da automação do comportamento inteligente." (LUGER, 2004, p. 24).

Stuart Russel e Peter Norwig utiliza um conceito misto, onde considera a inteligência artificial um campo da ciência, sendo a ferramenta resultado dos estudos neste campo dentro da ciência da computação.

> Durante milhares de anos, procuramos entender como pensamos; isto é, como um mero punhado de matéria pode perceber, compreender, prever e manipular um mundo muito maior e mais complicado que ela própria. O campo da inteligência artificial, ou IA, vai ainda mais além: ele tenta não apenas compreender mas também construir entidades inteligentes. (RUSSEL; NORWIG, 2004, p. 3).

De maneira compilada, poderíamos dizer que uma inteligência artificial é um sistema computacional criado para simular racionalmente a tomadas de decisão dos seres humanos, tentando traduzir em algoritmos o funcionamento do cérebro humano.

Um dos grandes responsáveis por pensar como seria uma máquina que simularia este agir de uma forma humana foi Alan Turing, o pai da Computação. Dentro do campo da inteligência artificial, o seu grande feito foi pensar em um teste em que uma máquina se passaria por um seria humano, abriria diálogo e o ser humano não descobrisse que estava conversando com uma máquina. Esse teste é até hoje base para a construção de uma inteligência artificial como aquelas utilizadas no chatbot ou interfaces humanizadas de voz, como assistentes digitais.

No início dos estudos de inteligência artificial, buscou-se na sua criação uma forma que poderia agir como um ser humano completo: escutando, entendendo e respondendo questões.

Como primeiro passo, objetivou-se que a IA entendesse o que lhe era descrito, e pudesse aprender e responder de forma escrita algo que fizesse sentido. No início, os retornos foram satisfatórios, porém, quanto mais complexo o conhecimento, maior era a dificuldade da IA realizar as ações, seja pelo poder de processamento ainda insuficiente, seja pela complexidade que era necessária na criação de algoritmos.

Diante desse impasse, os estudos em relação à inteligência artificial aos poucos esfriaram e passou-se a acreditar na inviabilidade de se construir uma inteligência complexa que comportasse todos os pontos desejados. A esse tipo de IA dá-se o nome de “Inteligência Artificial de Nível Humano”. Para elucidar a complexidade desse tipo de sistema, Norvig e Russel (2013, p. 52) descrevem a forma que alguns dos fundadores tentam reatar essa ideia, observando o avanço tecnológico:

> Apesar desses sucessos, alguns fundadores influentes da IA, incluindo John McCarthy (2007), Marvin Minsky (2007), Nils Nilsson (1995, 2005) e Patrick Winston (Beal e Winston, 2009), expressaram descontentamento com a evolução da IA. Achavam que a IA deveria colocar menos ênfase na criação de versões cada vez melhores de aplicações eficientes para tarefas específicas, tal como dirigir um carro, jogar xadrez ou reconhecer fala. Em vez disso, acreditam que a IA deveria retornar às suas raízes esforçando-se para obter, nas palavras de Simon, “máquinas que pensam, que aprendem e que criam”. Chamam o esforço de IA de nível humano ou HLAI; o primeiro simpósio foi em 2004 (Minsky et al., 2004). O esforço necessitará de grandes bases de conhecimento; Hendler et al. (1995) discutem de onde essas bases de conhecimento poderiam vir.

Trazendo esse problema para o contexto deste trabalho, é difícil conceber apenas uma inteligência artificial a cargo de gerir todas as funções de uma

cidade inteligente. Por isso, pensa-se na ideia de criar uma série de inteligências artificiais que possam ser conectadas entre elas por meio de uma engenharia capaz de atribuir sentido de unidade nas tomadas de decisão. Esse é o momento de se conceber sistemas especialistas a partir de uma construção única e voltadas para um propósito. A inteligência artificial evolui nessa direção e pode trazer muitos ganhos para as cidades inteligentes, conforme Norvig e Russel (2013, p. 737) tratam sobre sistemas especialistas e tomadas de decisão:

> As primeiras pesquisas de sistemas especialistas se concentravam em responder a perguntas, e não na tomada de decisões. Esses sistemas, que recomendavam ações em vez de fornecer opiniões sobre as questões em geral, faziam isso utilizando regras de condição-ação, em vez de empregarem representações explícitas de resultados e preferências. O surgimento das redes bayesianas, no final da década de 1980, tornou possível a construção de sistemas em grande escala que geravam inferências probabilísticas consistentes a partir da evidência. A adição de redes de decisão significa que podem ser desenvolvidos sistemas especialistas que recomendem decisões ótimas, refletindo as preferências do usuário, bem como a evidência disponível.

Pensar em uma estrutura que permita a associação de vários sistemas especialistas embarcados com inteligência artificial para a construção de uma cidade inteligente, é uma possibilidade concreta de executar com maior eficiência a gestão de recursos e os cuidados com o meio ambiente.

Um exemplo claro em que se utiliza a inteligência artificial para resolver problemas, é o seu uso no gerenciamento de um sistema de semáforos inteligentes. Uma reportagem da Veja Rio de 2021 (MAIA, 2021) noticia uma parceria firmada entre o Google e a cidade do Rio de Janeiro, levando a alguns locais um sistema que gerencia os semáforos, trazendo o conceito de semáforos inteligentes, cuja ideia é controla-los de uma maneira que os carros fiquem o menor tempo possível parados, contribuindo para a fluidez do trânsito da cidade.

Seu fundamento é de se buscar uma calibragem em relação ao tráfego de automotores em tempo real, sem a necessidade de uma pesquisa humana em campo, para depois criar uma programação específica destinada à cada um dos cruzamentos, interligando-os.

Estruturalmente, cada semáforo tem o seu próprio sensor de presença, computando a quantidade de carros e de motos que trafegam pelo cruzamento, assim, é possível gerenciar o tempo em cadeia e calcular o tempo necessário para que o trânsito flua.

Tal abordagem é capaz de trazer diferentes benefícios, como a otimização do tempo, a melhoria na qualidade de vida e do meio ambiente, conforme constatado em Israel, no qual foi utilizado um modelo semelhante ao do Rio de Janeiro, e houve uma diminuição de 10% a 20% no consumo de combustível e no tempo de atraso nos cruzamentos (MAIA, 2021).

Além disso, em períodos noturnos, os semáforos conseguem detectar a presença de carros e de motos, e agilizar o processo de abertura de passagem, atribuindo mais segurança ao evitar que o condutor fique parado em um semáforo, exposto a eventuais riscos.

Tudo isso pode ser exponenciado com a evolução das tecnologias. Pode-se imaginar, por exemplo, a massificação do uso de carros autônomos que podem conversar com semáforos inteligentes por meio de uma conexão 5G e do sistema especialista de gerenciamento de semáforos. Assim, além de conseguir detectar a presença do semáforo, a IA do carro pode determinar qual a velocidade ideal para ficar o menor tempo possível parado.

Ao observar o cenário apresentado sob um olhar do Direito e de um sistema de responsabilização, julga-se que, diante de um acidente causado por um erro na performance do semáforo inteligente, a culpabilidade recai sobre o sistema de responsabilidade objetiva do estado; sendo que é assegurado ao município o direito de regresso contra quaisquer responsáveis nos casos de dolo, ou de culpa contra a empresa responsável no caso de um erro na programação da inteligência artificial. Além do mais, pode ser proporcionado um plano de seguro em que o próprio município delega um fundo para a restituição financeira desses danos.

Focando no problema deste trabalho, sabe-se que, com o aumento exponencial da tecnologia na construção de cidades inteligentes, mais dados serão utilizados, inclusive os pessoais. Qualquer carro autônomo está passível de ser localizado pela cidade e em tempo real, principalmente, diante do conceito de semáforos inteligentes. Ao obter a identificação do carro, as chances de detectar o condutor, os passageiros e os hábitos são muito grandes, tornando-se possível até predizer para onde vai cada automóvel de acordo com a rotina.

Nessa circunstância, há a possibilidade de coleta desses dados, contudo deve ser analisada pelo analista de privacidade, junto ao encarregado de dados, a necessidade dessa coleta e do tratamento, conforme o artigo 6º, inciso I da LGPD: “finalidade: realização do tratamento para propósitos legítimos, específicos,

explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018, s.p.); pode ainda ser analisado conforme o artigo 7º, parágrafo 3º da LGPD: "O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização" (BRASIL, 2018, s.p.). Em suma, a finalidade deve ser o norteador dessa coleta e, principalmente, do armazenamento e do tratamento de dados.

Portanto, embora a aplicação da IA pareça simples, percebe-se que existem problemas complexos em relação a sua utilização e conexão com a construção de cidades inteligentes.

6.2 A Necessidade de um Relatório de Impactos à Inteligência Artificial na Construção de Cidades Inteligentes

Em conformidade com o exemplo visto anteriormente, sobre os semáforos inteligentes, pode-se constatar a complexidade alcançada por um sistema especialista embarcado com inteligência artificial. Diante disso, reconhece-se a necessidade de cada um dos sistemas apresentar um "Relatório de Impacto à Inteligência Artificial", de acordo com os princípios da impessoalidade, moralidade, publicidade e eficiência, e conforme o caput do artigo 37 da Constituição Federal (BRASIL, 2022).

Em texto aprovado pelo Parlamento Europeu no ano de 2020, o Regime relativo aos aspetos éticos da IA, da robótica e das tecnologias conexas, consagra inovações pertinentes a respeito do uso desses recursos, que poderiam ser implementadas em solo nacional quando o assunto se tratar de inteligência artificial. Conforme o item 13, dentro do capítulo relacionado à avaliação de riscos:

> 13. Considera que, pare determinar se a inteligência artificial, a robótica e as tecnologias conexas devem ser consideradas de alto risco e assim estar sujeitas ao cumprimento obrigatório das obrigações jurídicas e dos princípios éticos estabelecidos no quadro regulamentar para a IA, é conveniente realizar sempre uma avaliação *ex ante* imparcial, regulamentada e externa assente em critérios concretos e definidos (UNIÃO EUROPEIA, 2019, s.p.).

A partir desse item, obtém-se um norte para a criação de uma avaliação de riscos relacionados ao uso de IA. Sob o ponto de vista técnico, todo o texto do Parlamento Europeu parte do princípio de que toda inteligência artificial, principalmente, aquela acompanhada pela robótica, possui um alto grau de risco prejudicial. Logo, essas condições recairiam sobre os semáforos inteligentes, por ser um sistema robótico construído a partir da IA, conforme citado anteriormente. É importante reforçar que o fato de o sinaleiro não possuir mobilidade não impede que seja compreendido como um instrumento da robótica. Matarić (2014, p. 19-20) assim denomina um robô:

> Um robô é um sistema autônomo que existe no mundo físico, pode sentir o seu ambiente e pode agir sobre ele para alcançar alguns objetivos. [...] Existir no mundo físico – o mesmo mundo no qual existem pessoas, animais, objetos, árvores, o clima e muitas outras coisas – é uma propriedade fundamental dos robôs. Lidar com esse mundo físico e suas irredutíveis leis e desafios é o que faz da robótica o que ela é: um desafio real. Os robôs que existem no computador são simulações. Eles não têm realmente de lidar com as verdadeiras propriedades do mundo físico, porque simulações nunca são tão complexas quanto o mundo real. Portanto, embora haja uma grande quantidade de robôs simulados no ciberespaço, um robô de verdade existe no mundo físico.

Portanto, um semáforo é considerado um robô, visto que existe no mundo físico, possui suas programações e seus objetivos, lendo o ambiente por meio de sensores. Desse modo, perante um robô dotado de inteligência artificial, admite-se que ele possui um alto grau de risco danosos e, por meio de uma avaliação, verifica-se se esse nível de ameaça pode ser mitigado com soluções tecnológicas e comportamentais, como por exemplo, com a supervisão de um observador ou mediador.

O próprio Parlamento Europeu cita uma abordagem ampla de como medir os riscos e incluir entre eles a avaliação de impacto sobre a proteção de dados, prevista no Regulamento Geral sobre a Proteção de Dados em seu item 16.

> 16. Considera que esta abordagem baseada no risco deve ser desenvolvida de forma a limitar os encargos administrativos para as empresas e, em particular, as PME, utilizando, tanto quanto possível, os instrumentos existentes; refere que tais instrumentos incluem, entre outros, a lista de avaliação de impacto sobre a proteção de dados prevista no Regulamento (eu) 2016/679 (UNIÃO EUROPEIA, 2016, s.p.).

Pode-se presumir que, diante de uma categorização entre os níveis de exigência para a criação de inteligências artificiais, o Município, pelo seu dever estatal, deve ser o mais transparente possível, demonstrando os riscos e os seus atos para mitigar as ameaças.

Ao mencionar a avaliação de impacto sobre a proteção de dados e observar o seu equivalente em solo nacional – o relatório de impacto à proteção de dados –, é possível ter um documento em paralelo dentro da área de uso da inteligência artificial, nomeado como “relatório de impacto à inteligência artificial”. Os relatórios de impacto à proteção de dados, possui em sua descrição, pelo menos, os tipos de dados coletados, a metodologia utilizada na coleta e na garantia da segurança das informações, e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação dos riscos adotados.

Em relação ao relatório de impacto à inteligência artificial deve-se ter a descrição de um projeto, a metodologia feita no treinamento da máquina (se utilizou um banco de dados pré-formatado ou não), a análise dos programadores, o mapeamento de riscos e de possíveis consequências, e por fim, a criação de um seguro para cobrir potenciais danos. Esses deveriam ser o mínimo necessário para se criar um relatório dentro das diretrizes expostas, inclusive, para uma prefeitura implementar uma cidade inteligente.

6.3 Uma Taxa para o Seguro Relacionado a Cidades Inteligentes

Ao planejar uma cidade inteligente, principalmente, aquela que embarca inteligências artificiais, enfrenta-se a problemática dos possíveis danos e de quais as melhores possibilidades de ressarcimento dessas avarias.

No ano de 2017, o Parlamento Europeu aprovou um texto a ser remetido à Comissão, sobre as Disposições de Direito Civil sobre Robótica. Dentro desse contexto, um dos pontos mais aclamados está relacionado aos danos que podem ser ocasionados e a criação de um seguro obrigatório para a implementação de instrumentos robóticos dotados de IA. No item 57 das disposições, traz-se a seguinte redação:

> 57. Destaca que uma possível solução para a complexidade de atribuir responsabilidade pelos danos causados pelos robôs cada vez mais autónomos pode ser um regime de seguros obrigatórios, conforme acontece já, por exemplo, com os carros; observa, no entanto que, ao contrário do que acontece com o regime de seguros para a circulação rodoviária, em que os seguros cobrem os atos e as falhas humanas, um regime de seguros para a robótica deveria ter em conta todos os elementos potenciais da cadeia de responsabilidade (UNIÃO EUROPEIA, 2014, s.p.).

Conforme destacado no texto, a cobertura desses seguros obrigatórios passa pela programação, construção do equipamento, instalação dos sensores e pelo funcionamento, e deve cobrir falhas humanas durante a instalação e a manutenção, como também outros tipos de avarias mecânicas e de programação. Diante dos riscos que são assumidos com o uso desses recursos, o amparo precisa cobrir toda a cidade, principalmente, os lugares em que mais se usufrui de tecnologias para o bem-estar do cidadão.

A implementação de uma taxa para garantir o seguro de uma cidade inteligente, talvez seja o caminho e o norte necessário para efetivar o uso de tecnologias inovadoras, visto que, nas situações em que os danos atentam principalmente contra a matéria, é possível ressarcir de maneira rápida.

Pode-se, inclusive, valer do princípio da isonomia, por meio da qual se verifica os lugares que estão mais avançados na implementação de cidades inteligentes, e se cobra os custos do seguro de acordo com o nível desse avanço.

7 RESPONSABILIDADE CIVIL NO AMBIENTE DIGITAL

Nesta seção, chega-se a um ponto importante relacionado às cidades inteligentes. Diante da multiplicidade de relações presente nesse sistema, é necessário elencar quais os tipos de danos que podem ocorrer nas cidades inteligentes, e delimitar quais são as responsabilidades de cada um e quais os regimes de responsabilidade.

Neste estudo, verifica-se três pontos: a responsabilidade de um agente público, a responsabilidade nas relações de consumo e a responsabilidade geral que incide na LGPD. Por fim, é importante analisar o relatório de impacto à proteção de dados; item que está atrelado à responsabilidade geral que recai sobre a LGPD.

7.1 CIDADÃO X CONSUMIDOR

Para se entender qual a responsabilidade que incide na proteção de dados dentro de cidades inteligentes, é vital fazer a distinção entre “cidadão” e “consumidor”.

O conceito de “cidadão” é bem amplo; em algumas situações pode ser representado como aquele que reside em solo nacional ou aquele que exerce seu papel de cidadania, como voto, pagamento de impostos e taxas, e respeito à legislação. Mas, nesta pesquisa, a definição que interessa é: aquele que está localizado dentro de uma cidade, considerando principalmente as cidades inteligentes.

É um cidadão que usufrui da estrutura criada a partir de políticas municipais e aproveita dos serviços e dos espaços. Dentro de uma cidade inteligente, busca-se oferecer a esse cidadão um padrão de vida melhor e um bem-estar otimizado. Portanto, é preciso defini-lo pensando nos casos em que um dano incidir sobre ele.

Já o “consumidor” é assim definido dentro do artigo 2º da lei nº 8.078 (CDC, ou Código de Defesa do Consumidor):

> Art. 2° Consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final.

> Parágrafo único. Equipara-se a consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo (BRASIL, 2018, s.p.).

Perante o exposto, deve-se considerar que todo consumidor é um cidadão, que possui direitos e deveres dentro de uma cidade, mas pertencente a uma categoria única e especial, sendo que só adquire o adjetivo “consumidor” quando efetua a compra de um bem ou serviço não-estatal.

Uma cidade não pode ser considerada um bem ou serviço a ser comprado ou consumido. Por mais que o conceito mercantil cresça a cada dia, inclusive, oferendo vantagens a fim de atrair empresas e pessoas com grande capital intelectual, uma cidade é um fenômeno social de vivência e de bem-estar. Assim, busca-se em uma cidade, um lugar onde seja seguro o desenvolvimento pessoal em todas as áreas, físicas, psíquicas, materiais e espirituais, refletindo a coletividade.

Portanto, conclui-se que a cidade, por mais que ela possua aplicações tecnológicas, proporcione um maior grau de qualidade de vida aos cidadãos e seja considerada uma cidade inteligente, ainda assim, não deve ser considerada um bem de consumo. Dessa forma, a possibilidade da “responsabilidade objetiva” incidir sobre a gestão de uma cidade, deve ser afastada, visto que esta trata-se de uma gestão pública.

7.2 A Responsabilidade do Município, Seus Agentes e Empresas Estatais dentro das Cidades Inteligentes

Neste tópico, entra-se em uma seara já pacificada, visto que a responsabilidade dos danos causados pelo Município está situada dentro da classificação da responsabilidade objetiva, e que todas as avarias, materiais e morais, independentes de culpa, são ressarcidas pelo Estado, conforme o caput e o parágrafo 6º do artigo 37 da Constituição Federal:

> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:
> [...]
> § 6º As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa

> qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa (BRASIL, 2022, s.p.).

José Afonso da Silva (1998, p. 651), em sua obra clássica do Direito Constitucional, diante da responsabilidade dos agentes públicos, aponta:

> A obrigação de indenizar é da pessoa jurídica a que pertencer o agente. O prejudicado há que mover a ação de indenização contra a Fazenda Pública respectiva ou contra a pessoa jurídica privada prestadora de serviço público, não contra o agente causador do dano. O princípio da impessoalidade vale aqui também.
> O terceiro prejudicado não tem que provar que o agente procedeu com culpa ou dolo, para lhe correr o direito ao ressarcimento dos danos sofridos. A doutrina do risco administrativo isenta-o do ônus de tal prova, basta que comprove o dano e que este tenha sido causado por agente da entidade imputada. A culpa ou dolo do agente, caso haja, é problema das relações funcionais que escapa à indagação do prejudicado. Cabe à pessoa jurídica acionada verificar se seu agente operou culposa ou dolosamente para o fim de mover-lhe ação regressiva assegurada no dispositivo constitucional, visando a cobrar as importâncias despendidas com o pagamento da indenização. Se o agente não se houve com culpa ou dolo, não comportará ação regressiva contra ele pois nada terá de pagar.

Portanto, segundo o autor, os agentes municipais devem responder diante dos danos causados. A fim de confirmar esse ponto, Sarlet, Marinoni e Mitidiero (2020, p. 294-295) descrevem:

> A responsabilidade do Estado e de seus agentes por atos (comissivos ou omissivos) ilícitos e que afetam o patrimônio e posições jurídicas do cidadão é outra característica central do Estado de Direito. Por tal razão – de acordo com a lição de Gomes Canotilho – tal responsabilidade implica não somente a existência de um sistema jurídico-público de responsabilidade estatal (implicando um dever de reparação dos prejuízos causados pelos órgãos estatais), mas também um dever de indenização de determinados sacrifícios impostos aos cidadãos, como é o caso da previsão de uma indenização justa por conta de expropriações levadas a efeito pelo Poder Público. Tal responsabilidade, seu fundamento e abrangência, bem como os meios de controle e suas respectivas consequências, encontra-se regulada na própria Constituição Federal e no plano da legislação infraconstitucional, com destaque para a consagração da responsabilidade objetiva do Estado como regra no texto constitucional de 1988, que, ademais, contempla expressamente a responsabilidade por erro judiciário, ademais de normas dispondo sobre a desapropriação e correspondente indenização, sendo particularmente problemática a responsabilidade do Estado por conta da omissão legislativa, esta última assumindo caráter excepcional.
> Também a indenização por erro judiciário assume relevância nesse contexto, estando, todavia, sujeita a um regime jurídico próprio (que apresenta algumas particularidades) especialmente quando em causa eventual responsabilização por ato de natureza jurisdicional, tendo a Constituição Federal inclusive assegurado um direito fundamental específico para a hipótese de erro judiciário em caso de condenação e mesmo quando alguém quedar preso por tempo superior ao determinado na sentença condenatória (art. 5.º, LXXV, da CF). Por outro lado, a adoção irrestrita da teoria de

> responsabilidade objetiva do Estado e do assim chamado risco integral deve ser compreendida e aplicada de modo responsável e não absoluto, especialmente quando se tratar de danos decorrentes de fenômenos da natureza ou por fato de terceiros.

Apoiando-se no que foi exposto, vale ressaltar duas situações muito importantes dentro da gestão de cidades: a responsabilidade objetiva não é absoluta e os danos causados por desastres naturais não devem ser automaticamente reparados pelo estado. Em outros pontos deste trabalho, discute-se sobre os efeitos negativos do uso de dados para fazer predições. Contudo, quando se trata de desastres naturais, os dados relacionados à natureza, que em sua maioria não podem ser classificados como dados pessoais, tem o poder de auxiliar na prevenção de desastres e de planejar maneiras de evitar tais riscos; essa é a capacidade de predição das cidades inteligentes.

Quanto mais se avança nos termos tecnológicos, menor deveria ser a possibilidade do estado se ausentar da responsabilidade de danos diante de desastres naturais, justamente por essa capacidade de predizer riscos. As cidades inteligentes devem auxiliar nas tomadas de decisões para que o estado assuma as suas responsabilidades perante os cidadãos.

7.2.1 A Responsabilidade do Município diante de um Incidente de Dados

Conforme observado anteriormente, a responsabilidade do município, de seus agentes públicos e de empresas prestadoras de serviço são de categoria de responsabilidade objetiva, em que ao ser comprovado o dano, independente de culpa, o estado deve ressarcir o prejuízo.

Diante disso, automaticamente, espera-se que, diante de um incidente de dados que afeta um cidadão, a responsabilidade do município seja objetiva. Porém, há a necessidade de se observar na LGPD o artigo 43:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro (BRASIL, 2018, s.p.).

Os elementos descritos nesse artigo, demonstram que a responsabilidade pode ser afastada, levando em consideração o inciso II: quando não houver violação à LGPD e às considerações lançadas pela ANPD e por outras instituições regulatórias.

Ainda, é preciso retornar ao descrito do artigo 23 da LGPD:

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, [...] (BRASIL, 2018, s.p.).

Ao analisar o ponto apresentado acima sobre o "objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público", identifica-se um afastamento do regime geral de responsabilidades da LGPD, em que a sua obrigatoriedade em si é proativa e recai sobre a regra da responsabilidade civil objetiva do poder público; vale relembrar a preferência que a Constituição Federal tem sobre a legislação corriqueira.

Nesse sentido, Faleiros Júnior (2019, p. 22) pontua da seguinte maneira:

> A Lei Geral de Proteção de Dados trouxe institutos curiosos para a formação deste raciocínio, definindo por exemplo, grande abertura para a discussão causal ao prever, no artigo 43, II, o afastamento do nexo pela demonstração da não violação às disposições da lei. Este parâmetro aberto, pelo que se explorou, não deve conduzir ao raciocínio de que 'subjetivização' da responsabilidade civil do Estado aparece no horizonte como uma solução viável às dificuldades advindas da complexidade de cognição, fiscalização e controle dos algoritmos em Big Data, voltando, com isso, a se cogitar da culpa administrativa ('faute du service'). Seria um retrocesso.

Portanto, o tratamento de dados em um órgão público é uma categoria à parte, devendo respeitar as suas particularidades, não incidindo aqui a regra geral do artigo 43. Somado a isso, reforça-se o descrito na Lei de acesso à informação, em seu artigo 34:

> Art. 34. Os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso (BRASIL, 2011, s.p.).

Observando todos esses pontos, confirma-se que a responsabilidade civil de agentes públicos dentro da LGPD, é a objetiva. Assim, os cuidados que esses servidores devem ter em relação ao tratamento de dados, devem ser de um alto investimento capital e intelectual, para que essas informações estejam dentro de um plano de segurança da informação.

7.3 O Dano Enquanto Consumo e o Dano ao Cidadão

Neste momento, é preciso fazer a distinção entre os dois tipos de danos relacionados à responsabilização de prejuízo dentro de uma cidade inteligente.

Para exemplificar, supõe-se que um consumidor entrou em um site de compras, adquiriu um livro e, no transporte feito de maneira remota via drone, ocorreu indevidamente uma gravação; ainda, devido a um incidente de dados, estes perderam a sua confidencialidade. Essa situação hipotética ainda é um caso de dano não decorrente do consumo, mas está de acordo com as subresponsabilidades criadas do trabalho. Logo, nesse cenário, o bem a ser tutelado seria a privacidade dos cidadãos em relação a esse incidente de dados.

Portanto, recairia a responsabilidade subjetiva, em que deve ser investigado se houve a má-fé do operador, da empresa ou, até mesmo, se foi consequência de uma má ingerência. Ainda assim, observando as bases legais de tratamento de dados da LGPD, em nenhuma delas, exceto no legítimo interesse, poderia recair o transporte de bens por drone controlado remotamente.

Diante da responsabilidade subjetiva em casos como o exemplificado, os quais envolvem vias públicas, programação, robótica e preparo do piloto, deve-se exigir o disposto no artigo 38, caput e parágrafo único, da LGPD:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (BRASIL, 2018, s.p.).

Executar um trabalho com tamanha complexidade exige um Relatório de Impacto à Proteção de Dados e, nos casos que embarcam inteligências artificiais, deve ser solicitado um documento paralelo, nos moldes do Relatório, podendo ser nomeado como Relatório de Impacto à Inteligência Artificial.

7.4 A Responsabilidade Civil nas Relações de Consumo dentro das Cidades Inteligentes

Quando se observa as relações de consumo que ocorrem dentro das cidades inteligentes, como transporte, entregas, produtos e invocações, é preciso observar a regra geral das relações de consumo e o Código de Defesa do Consumidor. A análise deste tópico deve ser feita a partir da leitura do artigo 45 da LGPD:

> Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente (BRASIL, 2018, s.p.).

Ao analisar esse ponto, tem-se a remissão para o artigo:

> Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos BRASIL, 2018, s.p.).

Não há muito o que dizer sobre as relações de consumo dentro das cidades inteligentes, sendo que no caso de danos dentro desse sentido, a responsabilidade objetiva incidiria.

Serviços relacionados ao aluguel de bicicletas, a aplicativos de transporte de passageiros e de objetos, entre outras situações, entram nesse rol. Contudo, não se pode extrapolar tudo o que existe dentro de uma cidade inteligente e cruzar as linhas, tentando estabelecer que todos os danos são provenientes de consumo.

No transporte público, por exemplo, ainda que a frota seja autônoma e haja um dano decorrente dessa relação, ainda assim, deve ser considerada como

um dano consequente de um serviço prestado por um agente público e não resultante de consumo.

7.5 A Regra Geral sobre a LGPD e a sua responsabilidade Dentro das Cidades Inteligentes

Se por um lado há uma forte relação entre o cidadão e o município, o qual possui regra própria, e também entre o consumidor e os produtos/serviços dentro das cidades inteligentes, o restante dos negócios jurídicos configura-se como o que se pode chamar de “regra geral da responsabilidade civil em cidades inteligentes”.

Essa regulamentação ainda gera inúmeras controvérsias sobre qual é o seu regime; se é responsabilidade objetiva ou subjetiva dentro da LGPD. De um lado, existem aqueles que a consideram como responsabilidade subjetiva, pois a culpa é um fator fundamental dentro da responsabilidade civil na LGPD. Sobre esse ponto, GUEDES e MEIRELES (2019, p. 230-231) comentam:

> Segundo o art. 6º, inciso X, da LGPD, os agentes deverão demonstrar a “adoção de medidas eficazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". Do ponto de vista do controlador, do que adianta "prestar contas", se, ao final, se houver incidente, por mais diligente que tenha sido, ele será responsabilizado da mesma forma e independentemente de culpa? Ao criar verdadeiro standard de conduta, a LGPD se aproximou mais do regime de responsabilidade fundado na culpa ... A culpa passou a ser analisada a partir da ideia de desvio de conduta, que leva em conta apenas o comportamento exigível diante das especiais circunstâncias do caso concreto.

Ao considerar a culpa na não proteção de dados, ainda que pregressa, buscando investir em segurança da informação e criando uma cultura de privacidade e de proteção de dados, entra-se em uma seara completamente nova; exceto em casos especiais.

Para se observar esse tipo de responsabilidade é preciso retornar ao que trata o descrito na LGPD, no caput do artigo 6º e nos incisos VIII e X:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> [...]
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

> [...]
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018, s.p.).

Diante desses 3 (três) itens, a responsabilidade pelo dano incide, independente de culpa ou não, se não houver uma prevenção ativa dentro da empresa e também um processo interno de responsabilização e prestação de contas. Percebe-se que é diferente da responsabilidade objetiva ou subjetiva. É como se a culpa, ao contrário dos dois pontos anteriores, estivesse qualificada de uma maneira abaixo do que a prevenção e a prestação de contas em si. Essa ideia é discutida pelos professores Maria Celina Bodin de Moraes e João Quinelato de Queiroz (2019, p. 129):

> A nova lei, porém, introduz, secundando o regulamento europeu, uma mudança profunda em termos de responsabilização. Trata-se da sua união ao conceito de "prestação de contas". Esse novo sistema de responsabilidade, que vem sendo chamado de "responsabilidade ativa" ou "responsabilidade proativa" encontra-se indicada no inciso X do art. 6º, que determina que às empresas que não é suficiente cumprir os artigos da lei; será necessário também "demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas. Portanto, "não descumprir a lei, não é mais suficiente".

Utiliza-se o termo "proativa", no sentido de ter a proatividade em ações, levando em conta o tripé citado anteriormente: tecnológico, jurídico e de processos. A segurança da informação deve sempre ser respeitada. Ao fazer um tratamento de dados, é preciso ter em mente o investimento necessário para proteger devidamente as informações, levando em consideração a tecnologia atual e os dados que serão tratados.

Da parte jurídica, Moraes e Queiroz (2019, p. 118) lembram o seguinte:

> As cada vez mais criativas formas de coleta e tratamento de dados pessoais na atualidade renovam o direito à autodeterminação informativa como instrumento de promoção da pessoa, sendo premente que se abandone a lógica proprietária que ainda recai sobre os dados pessoais – no sentido de que os dados pessoais podem ser objeto de apropriação tal qual bem móveis – para uma lógica protetiva das relações pessoais e dos direitos subjetivos. A proteção da intimidade por vias da mera não interferência na esfera individual cede espaço à tutela positiva e proativa, isto é, que garanta ao titular o conhecimento pleno das formas de tratamento, finalidade e destino

> de seus dados. Na lição de Rodotà, é muito fraca a concepção meramente negativista sobre os dados pessoais segundo a qual se lançam proibições de coletas de dados pessoais, proibições essas que, na verdade, são o ponto de partida e não de chegada.

Além da questão da autodeterminação informativa, é preciso sempre lembrar da necessidade de transparência máxima, reforçando que o usuário, mesmo não possuindo o conhecimento tecnológico necessário, precisa saber claramente como os dados são tratados. O ponto da escolha da base legal e da finalidade do tratamento são imprescindíveis como justificativas dos atos de tratamento.

Ademais, é essencial a reflexão acerca da questão dos processos de gerenciamento das relações humanas, extremamente primordiais dentro de uma organização. É nessa discussão que entra a cultura, o treinamento, os avisos, as travas tecnológicas, contratuais e de processos. Tudo para que se efetive essa responsabilidade proativa.

7.6 Os Princípios da LGPD Como Norteadores da Responsabilidade Proativa.

A compreensão da distinção entre a responsabilidade subjetiva e proativa se faz presente na leitura principiológica da Lei Geral de Proteção de Dados Pessoais. A efetivação desses princípios, em quaisquer tratamentos de dados, exige uma compreensão mais profunda da constante atualização dos parâmetros de segurança e de interpretação da lei, sempre condizente com os direitos dos usuários.

Utilizando-se a classificação do Bruno Bioni (2022), pode-se agrupar esses princípios em três grandes fases, e em cada uma deve-se fazer uma análise detalhada de como tem que ser o tratamento de dados. São nomeadas como: de monólogo, de diálogo e de salvaguardas. Em cada uma dessas fases, os agentes de tratamento de dados devem ter um olhar diferente para cada diagnóstico; e estão coroadas pelo princípio de responsabilidade e de prestação de contas.

7.6.1 Fase de Monólogo e os Princípios da LGPD

A primeira fase, conforme a classificação de Bioni (2022), é chamada de “Fase de Monólogo”, cuja leitura está compreendida nos três primeiros princípios dispostos dentro do artigo 6º da LGPD, sendo estes o princípio da finalidade, da adequação e da necessidade:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; (BRASIL, 2018, s.p.).

O conceito de monólogo indica que as tomadas de decisão dos agentes de tratamento devem ser voltadas para um planejamento interno, verificando a viabilidade do manuseamento antes mesmo de seu início ou de alguma grande alteração; ainda, evidenciando a finalidade dessa operação adequação desse tratamento diante das finalidades, e a necessidade da coleta de cada dado pessoal em específico; e, por fim, transparecer como são processados essas informações.

O princípio da finalidade está disposto como o primeiro princípio e o início do planejamento do tratamento de dados pessoais em uma empresa. Cada dado coletado precisa ter um propósito específico, claro de ser explicado e não ambíguo. Essa finalidade precisa ser explicada e entendida pela maioria dos titulares de dados. O Aviso de Privacidade deve divulgar esse princípio ao titular e atentar àa armadilha da mudança de rota, onde os dados já coletados são utilizados como coringas, que podem ser reaproveitados em novas funções e finalidades. Um dado coletado para um determinado objetivo não deve ser utilizado para outro fim.

Já o princípio da adequação é aquele em que, observando a finalidade dos dados coletados, são criadas estruturas equivalentes às expectativas para a proteção desses dados pessoais, adequando-se não somente à LGPD, mas também a outras legislações, como os atos administrativos, as boas práticas de mercado e a Constituição Federal. A proporcionalidade aqui é dada ao observar a quantidade de

dados que são coletados, a sua importância e os riscos que podem ser gerados diante de um incidente.

O princípio da necessidade diz respeito à mínima coleta de dados. Por se tratar de princípios qualitativos, medir a abrangência das informações pertinentes, sendo estas proporcionais e não excessivas, deve estar alinhada à boa fé e à maturidade do controlador de dados diante desse princípio. O equilíbrio entre satisfazer os requisitos para alcançar a finalidade e não abusar na coleta de dados, só poderá ser alcançado com uma equipe técnica que trabalhe lado a lado com os desenvolvedores e administradores no que diz respeito a processos. A necessidade em si não diz respeito somente ao modelo de negócio, mas também às legislações e às regulações, onde também o jurídico deve apontar as demandas.

7.6.2 Fase de Diálogo e os Princípios da LGPD

A segunda fase é nomeada como a “Fase de Diálogo”, cujos princípios englobados são os de livre acesso, de qualidade dos dados e de transparência, dispostos no artigo 6º:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; (BRASIL, 2018, s.p.).

O termo “diálogo”, que nomeia esta fase, expressa que as tomadas de decisão dos agentes de tratamento de dados devem, após verificar a viabilidade dentro da primeira fase, estar voltadas ao contato com o titular, transmitindo toda a confiança necessária de que os seus direitos estão sendo respeitados.

Considerar, por exemplo, o princípio do livre acesso é constatar que os dados de um titular podem ser acessados a qualquer momento, a pedido do

mesmo. Aqui ainda é preciso destacar dois itens importantes sobre a metodologia desse livre acesso: consulta facilitada e integralidade. Do primeiro ponto, destaca-se o *design* do produto ou o processo para que um usuário possa ter acesso a essas informações. Se for um formato digital, a plataforma, em que se comporta esses dados, deve ser de fácil acesso e segura, comportando, por exemplo, uma autenticação em duas instâncias como um dos itens de segurança. Depois de entrar na plataforma, deve ser respeitado o acesso facilitado a informações de cadastro, de compras, de acessos, financeiras, de comportamento etc.

Quanto à integralidade, as plataformas devem não somente observar os dados que são descritos em informações pessoais quantitativas e exatas, como os dados fornecidos diretamente por seus titulares, mas ainda, observar também as informações coletadas por *cookies*, por mapeadores de calor e por outras tecnologias de telemetria que também devem estar acessíveis aos seus usuários, informando o que foi coletado e como esse dado, após o seu processamento, transforma-se na utilização da plataforma.

Na pior das hipóteses, deve-se ter um canal facilitado com o encarregado de dados para que ele possa fornecer essas informações que não estão presente no sistema. Considerar a integralidade tem que ser um ponto relevante, que na maioria dos casos não é levado em conta nas plataformas, principalmente, por não serem considerados dados exatos, mas qualitativos e de tendência, que auxiliam e norteiam ações para o negócio. É preciso considerar também que o tratamento de dados off-line precisa ter o seu *design*, observando uma metodologia em que o livre acesso seja respeitado, e o encarregado cumpra o papel de contato com o titular de dados, conforme o artigo 41, § 2º, inciso I da LGPD: “aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências” (BRASIL, 2018, s.p.. Portanto, um fluxo de acesso de dados pelo titular deve ser criado atentando-se a esse princípio como um norteador.

Já sobre a qualidade dos dados, é preciso compreender que, pelo bem do controlador ou do operador de dados, assim como, pelo bem do titular, quanto mais exatos os dados são, maior é o resguardo e a conformidade com a lei, e também é melhor para se alcançar a finalidade descrita na fase anterior. Garantir a exatidão, a clareza, a relevância e a atualização dos dados é um dever do controlador ou do operador de dados ao desenvolver, por exemplo, uma plataforma ou um processo de uso, de edição ou de atualização desses dados. Ainda mais, dentro do rol de direitos

do titular, está a correção de dados incompletos, inexatos ou desatualizados, como descrito no artigo 18, inciso II da LGPD (BRASIL, 2018).

Por fim, dentro da “Fase do Diálogo”, a transparência para com o titular de dados, demonstrando como está sendo tratado seus dados pessoais, é de suma importância para a conformidade com a lei. Aqui deve ser observado o papel do Aviso de Privacidade, os Contratos firmados, inclusive os de relações de trabalho, as Políticas internas e externas, as relações com os fornecedores e a simplificação das informações para com o titular, divulgando como é feito o tratamento de dados, quais informações são coletadas de maneira direta ou indireta, com quem são compartilhados e quais as garantias de segurança que foram implementadas pelo controlador. Se conjugado com o princípio do livre acesso, observando principalmente a consulta facilitada dos dados pessoais e a maneira com que é tratada, é preciso aqui admitir uma forma em que esses documentos possam ser construídos em camadas, constituídas de uma maneira que o homem médio, isto é, o usuário mais comum, possa compreender de forma clara e sucinta o que está ocorrendo com os seus dados, evitando assim que o titular não compreende o que ocorre durante o tratamento. Ainda mais, deve ser considerada uma outra camada mais técnica, demonstrando com exatidão o que acontece dentro da plataforma, dando os subsídios necessários para uma tomada de decisão mais técnica de um titular de dados.

7.6.3 Fase de Salvaguarda e os Princípios da LGPD

A terceira fase é a “Fase de Salvaguarda”, cujos princípios englobados são os dde segurança, e prevenção e de não discriminação, dispostos dentro do artigo 6º:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (BRASIL, 2018, s.p.).

O termo “salvaguarda”, conforme o dicionário Michaelis (2021, s.p.), no seu item 5, é conceitado como a “ação que visa preservar a integridade e a perenidade de uma obra, de um patrimônio etc.”. Dito isso, dentro da LGPD, a salvaguarda visa implementar os meios técnicos necessários para preservar a legislação tanto na questão normativa quanto na principiológica.

O princípio da segurança diz respeito às ferramentas e às técnicas que devem ser implementadas em uma organização para proteger os dados pessoais de um titular. Aqui, conforme descrito na lei, a segurança deve proteger os “acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão” (BRASIL, 2018, s.p.), e aproximar os princípios norteadores da matéria de segurança da informação, em que há a confidencialidade, a integridade e a disponibilidade das informações. Vale reforçar que não se trata somente de proteção de dados pessoais em meios digitais, mas também em espaços físicos, utilizando recursos, como por exemplo, salas fechadas, trancas e cadeados, como fator de segurança.

O princípio da prevenção diz respeito à adoção de medidas para prevenir incidentes de segurança. Se a proteção em si são as ferramentas e as metodologias utilizadas, a prevenção é a medida que deve ser utilizada diante do tipo de informação que é tratada. Por exemplo, prevenir um incidente de dados em uma padaria localizada numa cidade do interior. Os dados tratados contidos em um caderno são diferentes de um tratamento feito por um grande partido político em uma capital. O primeiro necessita, em boa medida, de uma gaveta com chaves que possa proteger esse caderno; já o segundo necessita de aparatos técnicos, como sistemas apropriados, computadores com proteções compatíveis, servidores com um alto grau de segurança, posto que uma informação relacionada à política partidária é classificada como um dado sensível, onde o grau de segurança deve ser amplificado.

Por fim, o princípio da não discriminação diz respeito a um tratamento para fins discriminatórios ilícitos ou abusivos. A leitura desse princípio deve ser ainda mais amplificada; mesmo que o fim não seja discriminatório, mas se a consequência gerada por essa finalidade for, esse objetivo não deve ser alcançado ou deve haver uma mudança de rota, levando em consideração essa análise. Vale destacar que a discriminação em si não é um problema, mas as que envolvem discriminações ilícitas ou abusivas sim. Em sua maioria, mas não deve ser observado com um rol taxativo, todos os dados que de alguma maneira diferenciam, são itens discriminatórios,

conforme os itens descritos dentro do artigo 5º, inciso II, que trata de dados pessoais sensíveis:

> Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural 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, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018, s.p.).

A discriminação de um candidato a uma vaga, por ter acesso abusivo a dados referentes a genética de uma pessoa ou por questões raciais, possuem uma conotação abusiva, onde justamente o princípio visa proteger. Pode acontecer ainda que, , devido a uma má programação ou um mal treinamento, essas tecnologias passem a ter um comportamento ruim, imitando os problemas da humanidade. Diante desse fato, deve-se ter dentro da equipe de desenvolvimento, profissionais com maturidade para detectar possíveis problemas e evitar que cheguem ao consumidor final *softwares* mal construídos.

7.6.4 A Efetivação da Proatividade Observando os Princípios da LGPD

Recordando que a LGPD é um emanharado complexo de situações em que simplesmente se pode verificar se uma organização está em conformidade com a lei ou não. Observar esses princípios, que já estão na lei, promovem a segurança jurídica necessária para analisar todas as outras obrigações dentro da legislação. As tomadas de decisão feitas a partir desses princípios, tornam a proatividade em cumpri-los como um fator de prova da conformidade com a LGPD. O 10º princípio do artigo 6º, que é apresentado mais à frente, é o princípio que coroa todos os itens anteriores, pelo seu fator de demonstração.

7.7 Segurança da Informação Como Fator de Proatividade

Não é possível tratar sobre a responsabilidade proativa sem abordar a segurança da informação e os investimentos necessários para tal. A proatividade

dentro do tratamento de dados está intrinsicamente ligada com o quanto foi investido em segurança da informação, não somente do ponto de vista financeiro, mas também de tempo, de treinamentos, de tecnologias e no estabelecimento de uma cultura de privacidade.

Como visto anteriormente, dentro do texto da LGPD há um preceito descrito como o princípio da segurança, em que, diante de um tratamento de dados pessoais, deve-se considerar ferramentas e técnicas que visem a proteção dos dados.

Vale destacar que o contexto da Segurança da Informação é mais amplo do que somente a proteção de informações particulares. Ao referi-la, está se trabalhando uma matéria em que todas as informações de uma empresa devem possuir um plano de proteção e não somente os dados pessoais. Segredos comerciais, o balanço financeiro, o estoque, os fornecedores, os equipamentos e as informações relevantes também estão embarcadas.

Os princípios da segurança da informação podem ser divididos em três preceitos: confidencialidade, disponibilidade e integridade, sendo que todas as tarefas relacionadas à segurança da informação estão calcadas nesses três princípios, e todos os processos e as contramedidas relacionadas a incidentes, como *spywares* e ataques de negação de serviço (ataques DDoS).

O princípio da confidencialidade é daquele que norteia a privacidade dos dados e dos acessos dentro e fora das organizações. É dentro desse princípio que se verifica os cuidados relacionados aos acessos dos sistemas, à complexidade de senhas, à proteção de papeis e aos relatórios nas mesas e impressoras, justificando que cada colaborador ou terceiro deve ter um acesso específico e mínimo conforme a complexidade de suas atribuições. Há ainda os cuidados relacionados às ações tomadas, os quais visam assegurar que as informações confidenciais e críticas não sejam acessadas, de maneira bruta (ataques em geral) ou planejada (fornecimento inapropriado de informações para aqueles que não possuem acesso), protegendo assim os dados da empresa.

O princípio da disponibilidade é aquele que norteia os acessos aos dados nos momentos requisitados dentro de uma organização. É dentro desse princípio que se verifica os cuidados relacionados à estruturação dos servidores, dos aplicativos, do acesso à rede, das regras de acesso e das manutenções. Estar disponível é uma habilidade essencial dentro de uma organização. Um exemplo da falta de disponibilidade dos arquivos e sistemas são os ataques denominados

ransomwares, os quais, por meio de um *malware*, criptografam os arquivos de um determinado local, retirando a sua disponibilidade e exigindo o pagamento de valores para que esses documentos possam ser descriptografados e acessados novamente. Outros exemplo são os servidores indisponíveis por motivos de manutenção ou a rede fora do ar, onde não é mais possível ter o acesso aos arquivos e sistemas. Aqui vale recordar que é preciso ter regras específicas relacionadas à disponibilidade: em uma central de atendimento que atende das 8 horas da manhã até às 18 horas, caso um colaborador queira acessar o sistema às 22h, ele conseguirá ter esse acesso? Devem os servidores serem desligados no período fora do trabalho?

Ter uma disponibilidade 24 horas por dia, nos 7 (sete) dias da semana, não necessariamente reflete os planejamentos e os desejos de uma organização, devendo, assim, todas essas decisões, serem inseridas em políticas específicas e aprovadas pela alta direção.

Por fim, o princípio da integridade é daquele que norteia a veracidade e a confiabilidade das informações dispostas. É dentro desse princípio que se verifica se as informações dispostas ali condizem com a realidade. Por exemplo, se um colaborador, tendo acesso ao balanço financeiro dentro de uma empresa, forja as informações, escondendo um caso de corrupção. Arquivos corrompidos, informações adulteradas, digitação errada na inserção de informações, coleta errada de dados por sensores e tantos outros pontos podem minar a integridade de um sistema, o tornando dispensável.

Os princípios de segurança de informação e suas tarefas agregadas, como controle de acessos, *backups*, simulação de violações e ataques, gestão de incidentes, entre outras são importantíssimas para a adequação à LGPD e para o controle de conformidade. Somando os princípios da segurança da informação com os esforços da efetivação dos princípios da LGPD do artigo 6º, alcança-se a efetivação de uma busca proativa. A ratificação dessa proatividade está assegurada graças ao último princípio do artigo 6º da LGPD e a importação do termo *accountability*.

7.8 ACCOUNTABILITY E PROATIVIDADE

Conforme salientado anteriormente, ao se discutir sobre responsabilidade proativa, é imprescindível sua relação com investimentos na área da

segurança da informação. Além disso, é necessário um esforço ainda maior quando considerada a LGPD para a finalidade de, além de investir em segurança, provar a conformidade com a legislação e a implantação dos requisitos de segurança.

Considerando que a LGPD teve inspiração na legislação de proteção de dados europeia (General Data Protection Regulation - GDPR), o artigo 5º possui princípios próximos com o que temos em âmbito nacional. Mesmo não sendo iguais aos preceitos brasileiros, destaca-se os princípios da licitude, da lealdade, da transparência, da minimização dos dados; mas o grande intuito aqui é verificar o princípio que ficou em destaque no parágrafo segundo do artigo 5º, conhecido como *accountability*. A tradução portuguesa da lei, utilizada em Portugal, traz como o princípio da responsabilidade; contudo, a responsabilidade em si não traz como um todo o significado de *accountability*. Já a LGPD, em seu artigo 6º, inciso X apresenta uma redação diferente para esse mesmo princípio: “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.” (BRASIL, 2019, s.p.).

O conceito brasileiro traduz melhor o significado de *accountability*, sendo não somente uma simples responsabilização por todas as fases da classificação dos princípios (monólogo, diálogo e salvaguardas), mas uma profunda importância para prestar contas a quem precisar. Bioni (2022), em sua classificação, coloca o princípio da responsabilização e da prestação de contas como o preceito coroador de todos os princípios anteriores. Ele protege, amplia e publiciza todos os atos, tomados de maneira proativa, para alcançar os patamares necessários, não somente para estar em conformidade com a LGPD, mas também a fim de ter como norteadora uma cultura de privacidade, onde o modelo de negócio se utiliza de todo o trabalho feito para amplificar a segurança de uma organização.

No tópico anterior, que tratava da segurança da informação, foi explicitado a necessidade de uma adequação como um todo e dos investimentos necessários diante do mercado. O princípio da responsabilização e da prestação levanta bandeiras ao comércio e aos clientes dos seus negócios, sendo favoráveis nas mesas de negociação, cem ontratações de seguros e em outros momentos decisivos importantes. Em muitas consultorias para se avaliar o valor de mercado de

uma organização também se considera os pontos de segurança de uma empresa, inclusive a dos dados.

Todas as políticas (Política de Segurança da Informação, Política de Backups, Política de Acessos etc.), os procedimentos (Rotinas de backups de um sistema específico por exemplo), a comprovação de treinamentos, as mudanças em contratos e os estímulos para a criação de uma cultura de privacidade são alguns dos itens relacionados ao princípio da responsabilização e da prestação de contas.

A responsabilidade proativa não se configura na propagação de todos esses documentos, o que em tese é uma má administração e pode ser utilizada por atacantes para acessar informações indevidas. Ela caracteriza-se na não estagnação em um patamar, dizendo que está de acordo com a lei e que a sua conformidade se encerrou; mas sim que a proatividade deve ser continua, pois os riscos também evoluem com o tempo. Para exemplificar esse fato, basta verificar o número de atualizações em sistemas operacionais, aplicativos, sistemas bancários etc. para entender que o risco é constante e evolutivo, e que só a conformidade momentânea não basta. A responsabilização e a prestação de contas, portanto, devem evoluir com o avançar do tempo, atentando-se a todas as fases e aos princípios, às evoluções tecnológicas, às boas práticas de mercado e também aos informes e às regulações da Autoridade Nacional de Proteção de Dados.

7.9 Relatório de Impacto à Proteção de Dados Dentro de Cidades Inteligentes

A partir do que é estabelecido pela União Europeia, apresenta-se um norte do que pode representar esse relatório, juntamente com a Avaliação de Impacto à Proteção de Dados. De início, é preciso observar o Considerando 84 do Regulamento Geral sobre a Proteção de Dados:

> A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. Sempre que a avaliação de impacto sobre a proteção de dados

> indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais (UNIÃO EUROPEIA, 2016, s.p.).

Dado o impacto de uma inteligência artificial, é necessária uma avaliação equivalente, pois, uma má implementação ou até mesmo uma omissão pode ser revisada nesse processo de avaliação. Se no texto, o impulsionador para a necessidade da avaliação, é o elevado risco para os direitos e as liberdades das pessoas singulares, quando se trata de inteligência artificial embarcando sistemas para cidades inteligentes, a visão deve ser mais ampla, sendo os direitos da coletividade como os direitos que devem ser salvaguardados. O item 7 do artigo 35º do Regulamento Geral sobre a Proteção de Dados trata dos requisitos mínimos para a produção da avaliação de impacto sobre a proteção de dados:

> A avaliação inclui, pelo menos:
> a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;
> b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;
> c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos a que se refere o n.o 1; e
> d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa (UNIÃO EUROPEIA, 2016, s.p.).

Portanto, a produção do relatório de impacto à proteção de dados pelo controlador, a sua revisão pelo encarregado de dados e, se preciso, o envio à ANPD, são necessários para a transparência de uma cidade inteligente quanto ao cuidado dos dados de seu cidadão. Já a LGPD conceitua o relatório de impacto à proteção de dados da seguinte maneira:

> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (BRASIL, 2018, s.p.).

Observado o descrito dentro do artigo 5º, inciso XVII da LGPD, é possível verificar as necessidades da produção de um relatório de impacto à proteção de dados pessoais sob o ponto de vista brasileiro, bem parecido com o que ocorre em solo europeu. Para dar profundidade à demanda desse documento, Filipe Fonteles CABRAL (2019, p. 5) dispõe sobre o relatório de impacto à proteção de dados pessoais:

> Um dos instrumentos mais importantes para a abordagem de gerenciamento de riscos é o chamado Relatório de Impacto à Proteção de Dados (RIPD). O RIPD é uma declaração elaborada pela organização que realiza a coleta e/ou o processamento de dados pessoais e que deixa consignadas as particularidades dessa atividade. O documento tem a dupla função de auxiliar a entidade a identificar e mitigar riscos à privacidade dos indivíduos e de constituir prova de que a atividade de processamento de dados está em conformidade com a lei.

Para que o RIPD seja efetivo, ele deve ser combinado com uma avaliação de impacto à proteção de dados pessoais. A referida avaliação é uma tarefa complexa, que congrega análises técnicas e jurídicas, e deve ser realizada por profissionais experientes, com metodologia, sob pena de tornar-se ineficaz para os seus propósitos de auxiliar a organização no gerenciamento de riscos. Compreendendo a importância desse documento, verifica-se a necessidade de que cada uma das secretarias municipais e ainda, de que todos os outros setores que envolvem dados pessoais, tenham detalhadas todas as informações particulares e a sua forma de tratamento.

Deve constar no relatório de impacto à proteção de dados pessoais, de maneira geral, a finalidade do tratamento, o ciclo de tratamento de dados, as medidas de segurança adotadas pelo controlador, as possibilidades de minimização, a anonimização e a pseudoanonimização, os fatores de segurança e quais as outras formas de prevenção de riscos e de atitudes diante de um incidente de dados.

Ainda mais, a cada inovação feita ou serviço implementado na cidade, principalmente, aqueles envolvendo tomadas de decisão por algoritmos, devem ser levados em conta os dados pessoais e como é feito o aprendizado para mitigar os riscos.

Recaindo a responsabilidade objetiva ao se tratar de agentes públicos, esses investimentos são contrapartidas ao que poderia ser gasto diante dos

danos causados por falta de investimento técnico e financeiro na proteção desses dados.

8 CONCLUSÃO

O conceito das cidades inteligentes irá chegar aos grandes centros urbanos, independentemente da agilidade com que será introduzida. Já se tem exemplos de aplicativos disponibilizados pelos municípios referentes à mobilidade urbana e à segurança pública.

Portanto, é preciso aplicar de forma eficiente conceitos importantes, como o *privacy by desing*, desde o início do projeto, concebendo todas as fases de implementação a partir de um pensamento de privacidade e de proteção de dados; bem como o *etichs by desing*, cuidando dos parâmetros éticos nas construções de soluções e de algoritmos que tenham um controle quanto ao resultado final em cidades inteligentes.

Ademais, dentro de todo esse processo, uma das peças mais importantes para a efetivação de cidades inteligentes que preservam os direitos fundamentais, como o direito à privacidade, é o Relatório de Impacto à Proteção de Dados.

Esse relatório precisa ser mais difundido e exigido pela ANPD em implementações passadas e presentes, e como um documento padrão das futuras aplicações. É por meio dele que se tem as garantias necessárias que afetam a vida de todos os cidadãos como, por exemplo, a implementação de monitoramento eletrônico com reconhecimento facial.

Quanto à inteligência artificial, é necessária a criação de um relatório de impacto à IA, via lei e oferecido por órgão responsável, como OAB, INMETRO, ANAC, CFM, entre outros, o qual determinará as medidas de segurança e as garantias quanto a sua construção e distribuição.

Sob o ponto de vista da segurança pública, o risco de um vigilantismo que traga uma sensação de sempre estar sendo observado e identificado, não pode ser um ônus diante do monitoramento urbano. A implementação de tecnologias nessa área, deve preservar a privacidade das pessoas tanto em ambientes abertos quanto no tratamento massificado da localização de todos os sujeitos.

Sob o ponto de vista da saúde, devido aos riscos ao tratar dados pessoais sensíveis, deve-se ter um maior cuidado quanto à segurança da informação, principalmente, levando em consideração o princípio da confidencialidade.

Dentro de sistemas de cadastro, seja na rede pública ou privada, o respeito à proteção de dados pessoais deve ser amplo, inclusive, devendo o município estar preparado para uma requisição de dados pessoais por meio do responsável.

Além disso, sob o ponto de vista da mobilidade urbana, é preciso uma posição urgente do DENATRAN sobre como será a implementação de carros autônomos em nosso país, diante da sua chegada via importação sem dispor de uma regra específica. Outro ponto a se destacar é como uma cidade inteligente vai se comportar quanto ao gerenciamento de tráfego urbano por inteligência artificial, e como será a comunicação entre os carros e a cidade.

É importante pensar também sobre como será o tratamento de dados pessoais em relação ao tráfego urbano, sob a perspectiva de que, no gerenciamento desses veículos, a sua identificação pode mapear os hábitos dos motoristas e dos passageiros dentro de suas rotas.

Há ainda os cuidados necessários na utilização de drones, verificando tanto as rotas urbanas, devido aos mesmos problemas citados anteriormente sobre as rotas e a troca de informações, quanto as filmagens que podem extrapolar os limites da privacidade. Em relação a este último apontamento, deve-se ter um cuidado especial na manipulação dos dados, principalmente em cidades inteligentes verticalizadas, onde as filmagens podem registrar o interior dos prédios. É claro que não se deve esquecer as casas, pois as gravações podem registrar áreas externas, como piscinas, quintais, garagens etc.

Quanto aos danos – com ênfase ao suporte do relatório de impacto a proteção de dados –, temos três possibilidades de incidências de responsabilidade dentro de cidades inteligentes: o dano sob o ponto de vista de consumo, onde incide a responsabilidade objetiva conforme o Código de Defesa do Consumidor (BRASIL, 1990); a responsabilidade objetiva a respeito do agente público quando os próprios gestores de cidades inteligentes cometem danos como, por exemplo, em um acidente ocorrido com um ônibus autônomo; e a responsabilidade proativa quando envolver dados pessoais – fora os pontos acima –, cuja proatividade terá um peso maior ao proteger os dados sob o ponto de vista tecnológico, jurídico e de processos.

Por fim, vale dizer que o respeito ao meio ambiente e a uma cidade inteligente plural, em que todas as regiões recebam o seu devido cuidado, deve constar no planejamento e na implementação das cidades inteligentes. E com o avançar dessa efetivação, a criação de elementos, como taxas, que subsidiem os

seguros relacionados a cobertura de danos nessas cidades e o uso de imposto para cobrir todas as regiões será necessária para efetivar as garantias fundamentais previstas na Constituição Federal (BRASIL, 1990).

REFERÊNCIAS

ALMEIDA, Emily. Homem é preso por engano em Copacabana. **Band News FM Rio**, 2019. Disponível em: https://bandnewsfmrio.com.br/editoriasdetalhes/homem-e-preso-por-engano-em-copacabana. Acesso em: 13 mar. 2021.

ARENDT, Hannah. **A condição humana.** 10ª ed. Rio de Janeiro: Forense Universitária, 2007.

ARISTÓTELES. **A Política.** 1ª ed. Rio de Janeiro: Nova Fronteira, 2011.

ARAÚJO JÚNIOR, Miguel Etinger de. Algumas considerações sobre o Plano Diretor dos municípios e sua importância no processo de construção da cidadania e da democracia. **Revista de Direito Público Universidade Estadual de Londrina**, Londrina, v. 1, n. 1, p. 45-62, jan./abr. 2006.

BIONI, Bruno. **Aula 1 – Privacidade e Proteção de Dados:** Desafios Atuais e Tendências. 32. ed. São Paulo: Data Privacy Brasil, 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 dez28. 2022.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Direito do Consumidor. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L8078compilado.htm. Acesso em: 23 jan. 2022.

BRASIL. **Lei nº 10.257, de 10 de julho de 2001**. Regulamenta os arts. 182 e 183 da Constituição Federal, estabelece diretrizes gerais da política urbana e dá outras providências. (Estatuto das Cidades). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10257.htm. Acesso em: 03 dez. 2022.

BRASIL. **Lei nº 12.527, de 18 de novembro 2011.** Lei de Acesso à Informação. Brasília, DF: Presidência da República, 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 23 jan. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 23 jan. 2022.

BRASIL. **Lei nº 13.979, de 6 de fevereiro de 2020.** Dispõe sobre as medidas para enfrentamento da emergência de saúde pública de importância internacional decorrente do coronavírus responsável pelo surto de 2019. Distrito Federal, 2020a. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Lei/L13979.htm. Acesso em: 11 ago. 2020.

BRASIL. Câmara dos Deputados. **Projeto de Lei Nº. 3042 DE 2021.** Dispõe sobre a prorrogação do prazo de vigência de incentivos do Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores – PADIS, instituído pela Lei nº 11.484, de 31 de maio de 2007, e dá outras providências.. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2067122&filena. Acesso em: 11 dez. 2022.

BRASIL. **Exposição de Motivos da Medida Provisória nº 954, de 17 de abril 2020.** Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020b. Distrito Federal, 2020. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Exm/Exm-MP-954-20.pdf. Acesso em: 11 ago. 2020.

BRASIL. Supremo Tribunal Federal. **Medida Cautelar na Ação Direta De Inconstitucionalidade 6.387, de 24 de abril de 2020.** Requerente: Conselho Federal da Ordem dos Advogados Do Brasil. Intimado: Presidente Da República. Relatora: Ministra Rosa Weber. Distrito Federal, 2020c. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15342959350&ext=.pdf. Acesso em: 05 ago. 2020.

BRASIL. **Portaria nº 2.663, de 31 de dezembro de 2020**. Institui a Agenda Regulatória do Departamento Nacional de Trânsito (DENATRAN) para o biênio 2021-2022, com o objetivo de indicar temas de cunho regulatório a serem estudados no período. Distrito Federal, 2020d. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n%C2%BA-2.663-de-31-de-dezembro-de-2020. Acesso em: 5 dez. 2021.

BRASIL. Supremo Tribunal Federal. **Pleno**: compartilhamento de dados de usuários de telefonia. 2020e. 39m10s. Disponível em: https://www.youtube.com/watch?v=qnU5UV5wmkE. Acesso em: 5 ago. 2020.

BRASIL. Autoridade Nacional de Dados Pessoais. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília, DF: Presidência da República, 2021a. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 5 dez. 2021.

BRASIL. Ministério do Desenvolvimento Regional. **Carta Brasileira Cidades Inteligentes**. Brasília, DF: Presidência da República, 2021b. Disponível em: https://www.gov.br/mdr/pt-br/assuntos/desenvolvimento-urbano/carta-brasileira-para-cidades-inteligentes/20201208_carta-brasileira-para-cidades-inteligentes_final.pdf. Acesso em: 5 dez. 2021.

BRASIL. Agência Nacional de Aviação Civil. **Drones**. Distrito Federal, 2022. Disponível em: https://www.gov.br/anac/pt-br/assuntos/drones. Acesso em: 5 jun. 2022.

CABRAL, Filipe Fonteles. **Proteção de Dados Pessoais na Atividade Empresarial:** gerenciamento de riscos e o relatório de impacto à proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2019.

CAVOUKIAN, Ann. **Privacy by design:** the 7 foundational principles – implementation and mapping of fair information practices. Toronto: Information and Privacy Commissioner of Ontario, 2011. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em: 5 abr. 2022

CRIVILIM, Hugo. **Os Reflexos da Inteligência Artificial na Responsabilidade Civil**. 2020. 198 p. Dissertação (Mestrado em Direito Negocial) – Universidade Estadual de Londrina, Londrina, 2020.

CURITIBA. Prefeitura Municipal de Curitiba. **Centro de Controle Operacional da Muralha Digital de Curitiba começa a funcionar**. Curitiba, jan. 2021. Disponível em: https://www.ici.curitiba.org.br/noticias/centro-de-controle-operacional-da-muralha-digital-de-curitiba-comeca-a-funcionar/2263. Acesso em: 13 dez. 2021.

DICK, Philip Kindred. **Minority Report:** A Nova Lei. 2. ed. São Paulo: Record, 2002.

DONEDA, Doneda. **Da privacidade à proteção de dados pessoais:** elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2019.

FALEIROS JÚNIOR, José Luiz de Moura. O Estado entre dados e danos: Uma releitura da teoria do risco administrativo na sociedade da informação. In: FALEIROS JÚNIOR, José Luiz de Moura; LONGHI, João Victor Rozatti; GUGLIARA, Rodrigo. **Proteção de Dados Pessoais na Sociedade da Informação**. Indaiatuba: Editora Foco, 2019.

G1. Ifood será a 1ª empresa a realizar delivery com drones no Brasil após permissão da ANAC. **Tecnologia**, 2021. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/01/21/anac-permite-uso-de-drones-para-entregas-no-brasil.ghtml. Acesso em: 23 jan. 2022.

GUEDES, Gisela Sampaio da Cruz; MEIRELES, Rose Melo Vencelau. Término do tratamento de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**, São Paulo: Editora RT, 2019.

INMETRO. **Plano Estratégico do INMETRO 2021-2023**. Distrito Federal: INMETRO, 2021. Disponível em: https://asmetro.org.br/portalsn/wp-content/uploads/2021/03/PlanoEstrategicoInmetro_Aprovado_revFinal-100221-PDF.pdf. Acesso em: 23 jan. 2022.

JUNIOR, Francisco; AMIM, Angela; BRAIDE, Eduardo; CATHEDRAL, Haroldo. **Cidades inteligentes:** uma abordagem humana e sustentável. Brasília: Edições Câmara, 2021. Disponível em: https://www2.camara.leg.br/a-camara/estruturaadm/altosestudos/pdf/cidades_inteligentes.pdf. Acesso em: 15 jun. 2021.

LIMA, César Carvalho Lima. Do Tratamento de Dados Pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

LUGER, George F. **Inteligência Artificial**. 4. ed. Porto Alegre: Bookmann, 2004.

MAIA, Luiza. Recursos de inteligência artificial do Google serão usados nos sinais de trânsito. **Veja Rio**, 2021. Disponível em: https://vejario.abril.com.br/cidade/inteligencia-artificial-google-semaforos-rio/. Acesso em: 08 jan. 2022.

MATARIĆ, Maja J. **Introdução à robótica**. São Paulo: Editora Unesp e Blucher, 2014.

MATSUKI, Edgard; PEDROSA, Pedrosa. Abin admite monitorar dados de redes sociais para investigações. **Portal EBC**, 2013. Disponível em: https://memoria.ebc.com.br/tecnologia/2013/08/abin-monitora-dados-de-redes-sociais. Acesso em: 13 dez 2021.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa. **Cadernos Adenauer**, Rio de Janeiro, ano 20, n. 3, p. 113-135, 2019.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

PRESSMAN, Roger S. **Engenharia de software: uma abordagem profissional**. Porto Alegre: AMGH, 2011.

PERSONAL DATA PROTECTION COMMISION. **Guide to Basic Data Anonymisation Techniques**. Singapura, 2018. Disponível em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf. Acesso em: 28 dez. 2022.

RECH, Adir Ubaldo; GULLO, Maria Carolina; SCUR, Luciana. **Plano Diretor Inteligente:** Pressuposto Para Cidades Inteligentes. [s.l]: Educs, 2019.

REIS, Carolina; ALMEIDA, Eduarda; DA SILVA; Felipe; DOURADO, Fernando. **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil.** Brasília: Laboratório de Políticas Públicas e Internet, 2021. Disponível em: https://lapin.org.br/download/4136/. Acesso em: 5 dez. 2021.

RUSSEL, Stuart; NORVIG, Peter. **Inteligência Artificial**. 3. ed. Rio de Janeiro: Elsevier, 2013.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de Direito Constitucional**. 9. ed. São Paulo: Saraiva Educação. 2020.

SCRUTON, Roger. **Beleza**. São Paulo: É Realizações, 2013.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 15. ed. São Paulo: Malheiros, 1998.

UNIÃO EUROPEIA. Parlamento Europeu. **Disposições de Direito Civil sobre Robótica.** Estrasburgo**,** 2014.Disponível em: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.pdf. Acesso em: 12 nov. 2021.

UNIÃO EUROPEIA. Parlamento Europeu. Conselho. Regulamento (UE) 2016/679 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia.** Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em: 12 nov. 2021.

UNIÃO EUROPEIA. Parlamento Europeu**. Regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas**. [s.l.], 2019. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_PT.pdf. Acesso em: 15 dez 2021.

UNITED STATES. Department of Transportation. **Preparing for the Future of Transportation**: Automated Vehicles 3.0. Washington, 2018. Disponível em: https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320656/av-30-web-version.pdf. Acesso em: 5 dez. 2021.

VAINZOF, Rony. Disposições Preliminares. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

VARGAS, Isadora Formenton. **Drones e direitos de personalidade**. Indaiatuba: Editora Foco, 2021.

WINTER, Kathy. Para los coches autónomos 4 terabytes es más que um número. Newsroom. [s.l.], 2017. Disponível em: https://newsroom.intel.la/news-releases/para-los-coches-autonomos-4-terabytes-es-mas-que-un-numero/#gs.n9351l. Acesso em: 1 set. 2022.