UNIVERSIDADE CATÓLICA DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

GABRIEL DE OLIVEIRA CAVALCANTI NETO

CIDADES INTELIGENTES E PROTEÇÃO DE DADOS: UMA ANÁLISE DO CASO DA CIDADE DO RECIFE PARA OTIMIZAÇÃO DO MARCO REGULATÓRIO ATUAL

RECIFE – PE
2024

GABRIEL DE OLIVEIRA CAVALCANTI NETO

CIDADES INTELIGENTES E PROTEÇÃO DE DADOS: UMA ANÁLISE DO CASO DA CIDADE DO RECIFE PARA OTIMIZAÇÃO DO MARCO REGULATÓRIO ATUAL

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Católica de Pernambuco (UNICAP), como requisito parcial para obtenção do título de Mestre em Direito.

Linha de pesquisa: Cidadania Digital

Orientador: Prof. Dr. Alexandre Freire Pimentel

RECIFE – PE

2024

C376c Cavalcanti Neto, Gabriel de Oliveira.
Cidades inteligentes e proteção de dados : uma análise do caso da cidade do recife para otimização do marco regulatório atual / Gabriel de Oliveira Cavalcanti Neto, 2024.
134 f.

Orientador: Alexandre Freire Pimentel.
Dissertação (Mestrado) - Universidade Católica de Pernambuco. Programa de Pós-graduação em Direito. Mestrado em Direito, 2024.

1. Proteção de dados - Recife. 2. Cidades inteligentes 3. Brasil. [Lei geral de proteção de dados pessoais (2018)]. 4. Direito à privacidade - Recife. I Título.

CDU 34:004.738.5(81)

Pollyanna Alves - CRB/4-1002

GABRIEL DE OLIVEIRA CAVALCANTI NETO

CIDADES INTELIGENTES E PROTEÇÃO DE DADOS: UMA ANÁLISE DO CASO DA CIDADE DO RECIFE PARA OTIMIZAÇÃO DO MARCO REGULATÓRIO ATUAL

Dissertação apresentada ao Programa de Pós-Graduação em Direito da Universidade Católica de Pernambuco (UNICAP), como requisito parcial para obtenção do título de Mestre em Direito.

Aprovada em 12 de novembro de 2024.

BANCA EXAMINADORA

ALEXANDRE FREIRE PIMENTEL:1677578
Assinado de forma digital por ALEXANDRE FREIRE PIMENTEL:1677578
Dados: 2025.01.29 23:13:03 -03'00'

Prof. Dr. Alexandre Freire Pimentel
(Presidente da Banca Examinadora)

Documento assinado digitalmente
gov.br
JOAO PAULO FERNANDES DE SOUZA ALLAIN TE
Data: 31/01/2025 15:49:01-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. João Paulo Allain Teixeira
(Titular Interno)

Documento assinado digitalmente
gov.br
THERESA CHRISTINE DE ALBUQUERQUE NOBRE
Data: 31/01/2025 09:13:05-0300
Verifique em https://validar.iti.gov.br

Prof.ª Dra. Theresa Christine de Albuquerque Nóbrega
(Titular Interno)

Documento assinado digitalmente
gov.br
DIOGO RAIS RODRIGUES MOREIRA
Data: 31/01/2025 14:37:07-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Diogo Rais Rodrigues Moreira
(Titular Externo)

Recife
2024

AGRADECIMENTOS

Agradeço a minha família e amigos por terem me apoiado durante todos esses anos nos quais estive em busca dessa conquista. Finalmente chegou o grande dia e mais uma etapa da minha vida foi concluída, depois de uma árdua caminhada onde tive momentos de dificuldade e de alegrias. Ela foi finalizada com sucesso e irei guardar na memória os aprendizados, que me tornaram uma pessoa melhor.

Posso dizer que adquiri muita experiência ao longo desses 2 anos de trajetória e não poderia deixar de agradecer, primeiramente à Deus, pelo dom da vida, pois ele me auxiliou em momentos marcantes em minha jornada.

Ao meu pai, Gabriel Filho, pelo companheirismo, valores ensinados e por não medir esforços para que meus sonhos e objetivos fossem realizados. À minha mãe, Ângela Lins, pelo carinho e incentivo incondicionais, sempre torcendo para o meu sucesso. Ao meu irmão, Daniel Cavalcanti, pela irmandade, amizade, preocupação e cuidado.

Pelo exemplo de vida, sabedoria e atenção, agradeço aos meus avós paternos, Gabriel Cavalcanti (in memoriam) e Júlia Barros (in memoriam), que nunca se ausentaram espiritualmente do meu coração. Agradeço aos meus avós maternos Waldemir Lins (in memoriam) e Silvia Lins, que sempre estiveram presentes na minha formação prestando todo auxílio e sempre me incentivando com exemplos de ética, probidade e moralidade.

Pela ajuda incansável e compreensão, agradeço amigo Hélio André. Além disso, cabe ressaltar o apoio incondicional do meu orientador, Alexandre Freire Pimentel, que me proporcionou discutir, evoluir e pensar a frente da nossa realidade. Agradeço a Catarina Oliveira por toda atenção, carinho e pela maravilhosa oportunidade dos 12 meses de estágio docência. E, em especial, a minha namorada, Mylena, por todo o amor, carinho, paciência e dedicação. Obrigado pela colaboração de todos e espero que seja apenas o início! Essa vitória é de todos nós!

RESUMO

O conceito de *smart city* (cidade inteligente) está relacionado à existência de sistemas de tecnologia da informação e comunicação para o desenvolvimento de ações inovadoras e para a criação das novas cidades. Contudo, o fenômeno traz implicações no campo jurídico não devidamente analisadas até o presente, como a privacidade e proteção de dados. Diante disso, a dissertação analisa se a LGPD é capaz de controlar possíveis ameaças à privacidade pessoal em cidades inteligentes, bem como o tratamento de dados na cidade do Recife. Para tanto, o estudo busca a legislação pertinente às políticas públicas e proteção de dados na cidade de Recife, realizar uma revisão sistemática multi/transdisciplinar sobre o tema cidades inteligentes, a fim de apontar possíveis caminhos para melhoramento da proteção de dados dos cidadãos em razão das ameaças à privacidade provocadas pelas cidades inteligentes. Metodologicamente, trata-se de um estudo de caso único na cidade do Recife-PE, de natureza qualitativa, com dados coletados por meio de pesquisa documental e bibliográfica. São analisados documentos legais que contribuem para as políticas públicas de governança inteligente em Recife-PE, experiências envolvendo atores e práticas na cidade e como a Gestão da Informação garante a proteção de dados dos cidadãos.

Palavras-chave: proteção de dados; consentimento; LGPD; privacidade; cidades inteligentes.

ABSTRACT

The concept of smart city is related to the existence of information and communication technology systems for the development of innovative actions and the creation of new cities. However, the phenomenon has implications in the legal field that have not been properly analyzed to date, such as privacy and data protection. Given this, the dissertation analyzes whether the LGPD is capable of controlling possible threats to personal privacy in smart cities, as well as data processing in the city of Recife. To this end, the study seeks legislation pertinent to public policies and data protection in the city of Recife, carrying out a multi/transdisciplinary systematic review on the topic of smart cities, in order to point out possible ways to improve citizens' data protection due to of privacy threats caused by smart cities. Methodologically, this is a single case study in the city of Recife-PE, qualitative in nature, with data collected through documentary and bibliographic research. Legal documents that contribute to smart governance public policies in Recife-PE, experiences involving actors and practices in the city and how Information Management guarantees the protection of citizens' data are analyzed.

Keywords: data protection; consent; LGPD; privacy; smart cities.

LISTA DE ABREVIATURAS E SIGLAS

ADI	Ação Direta de Inconstitucionalidade
AEPD	Autoridade Europeia para a Proteção de Dados
AIP	Avaliações de Impacto de Privacidade
ANPD	Autoridade Nacional de Proteção de Dados
ANS	Agência Nacional de Saúde Suplementar
ARPA	*Advanced Research and Projects Agency*
Arpanet	*Advanced Research Projects Agency Network*
CAE	Comissão de Assuntos Econômicos
CCPA	*California Consumer Privacy Act*
CDC	Código de Defesa do Consumidor
CFTV	Circuito Fechado de Televisão
CGPDP	Conselho Gestor de Proteção de Dados Pessoais
CIX	*Commercial Internet Exchange*
CNJ	Conselho Nacional de Justiça
CNPD	Conselho Nacional de Proteção de Dados Pessoais e da Privacidade
CNPJ	Cadastro Nacional da Pessoa Jurídica
CPF	Cadastro de Pessoa Física
CPSI	Contratação Pública para Solução Inovadora
CRFB/88	Constituição da República Federativa do Brasil de 1988
EMPREL	Empresa Municipal de Informática
FCRA	*Fair Credit Reporting Act*
FTC	*Federal Trade Comission*
GDPR	*General Data Protection Regulation*
GIX	*Global Internet Exchange*
HTTP	*Hypertext Transfer Protocol*
IA	Inteligência Artificial
IBGE	Instituto Brasileiro de Geografia e Estatística
ICTs	Instituições Científicas, Tecnológicas e de Inovação
IDEC	Instituto Brasileiro de Defesa do Consumidor
IoT	*Internet of things*
ISO	*International Organization for Standardization*

ITU	*International Telecommunication Union*
KDD	*Knowledge Discovery in Databases*
LAI	Lei de Acesso à Informação
LAN	*Local Area Network*
LGPD	Lei Geral de Proteção de Dados Pessoais
LNCC	Laboratório Nacional de Computação Científica
MPF	Ministério Público Federal
MSN	*Microsoft Network*
NIRE	Número de Identificação do Registro de Empresas
NSF	*National Science Foundation*
NSFNET	*National Science Foundation Network*
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
ONU	Organização das Nações Unidas
PDA	Plano de Dados Abertos
PDAPF	Política de Dados Abertos do Poder Executivo Federal
PDC	Privacidade Desde a Concepção
PIA	*Privacy Impact Assessment*
PM	Polícia Militar
PPP	Parceria Público-Privada
RG	Registro Geral
RIPD	Relatório de Impacto à Proteção de Dados Pessoais
RNP	Rede Nacional de Ensino e Pesquisa
SEI	Secretaria Especial de Informática
Serpro	Serviço Federal de Processamento de Dados
SPC	Serviço de Proteção ao Crédito
SUS	Sistema Único de Saúde
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
WWW	*World Wide Web*

SUMÁRIO

INTRODUÇÃO

Em termos de governança e Direito Digital, o tema “Cidades inteligentes” (CI) tem ganhado destaque no cenário jurídico. Nada obstante, as discussões acadêmicas em geral investigam a matéria do ponto de vista urbanístico, ambiental ou sociológico, negligenciando a sua dimensão jurídica e o seu aspecto regulatório. Comumente, as análises focam nos benefícios sociais das *smart cities* e esquecem de elaborar críticas para aperfeiçoamento do fenômeno. Diante disso, urge investigar a questão da ambivalência entre privacidade e vigilância dos cidadãos no contexto das cidades inteligentes.

Questões relevantes precisam ser tratadas, como a ausência de mecanismos de consentimento para o processamento de dados pessoais coletados em espaços públicos ou através do Estado, a “privatização” da infraestrutura e dos dados coletados nas cidades, a redefinição de “*Big Data*” extraídos da Internet das Coisas (*Internet of Things* – IoT) em cidades inteligentes e o armazenamento desses dados na nuvem. O reflexo jurídico desse quadro é a discussão sobre privacidade e cidades inteligentes, privacidade e Internet das coisas, também privacidade e *Big Data*, o que desagua no debate sobre privacidade e a crise da demarcação do que é público e do que é privado.

Diante do quadro, a dissertação investiga eventuais ameaças que as cidades inteligentes trazem aos direitos constitucionais à privacidade e à personalidade, bem como a eficácia da regulamentação da Lei Geral de Proteção de Dados (LGPD) em torno da Internet das Coisas (IoT), “computação ubíqua”, “*Big Data*” e a nuvem. A proposta é discutir como a LGPD protege a privacidade nos casos das cidades inteligentes, tendo a cidade do Recife como marco.

O estudo pretende responder à seguinte indagação: partindo da análise da cidade do Recife, pode-se afirmar que a LGPD é capaz de controlar possíveis ameaças à privacidade pessoal presentes nas cidades inteligentes?

Parte-se da hipótese de que a LGPD tende a proteger uma zona ou “bolha” de privacidade individual, ignorando ou protegendo deficientemente a privacidade no espaço público e que o esquema de consentimento da LGPD não serve para salvaguardar a privacidade do cidadão no espaço público.

A empreitada se justifica, porque, de acordo com a Organização das Nações Unidas (ONU) (2019), atualmente, 55% da população mundial vive em cidades,

número que chegará a 70% em 2050. Esse processo de urbanização se tornou tão grande que, em alguns países (e.g., Coréia do Sul), a capital chega a gerar até metade do seu Produto Interno Bruto (PIB).

Globalmente, a alta densidade urbana causa problemas relacionados ao tráfego, água, energia, emissão de gases poluentes, desenvolvimento não planejado, resíduos, criminalidade. A necessidade política e social de combater essas mazelas, combinada com o potencial lucrativo para empresas de tecnologia e telecomunicações, provocou o desenvolvimento de soluções digitais e em rede, dando origem ao conceito de cidade inteligente (Dameri; Cocchia, 2013).

Conforme a Câmara dos Deputados, 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 [...] estima-se que o tamanho do mercado global de cidades inteligentes alcançou US$ 312,4 bilhões, em 2018, e atingirá aproximadamente US$ 1,56 trilhões até o final do ano de 2025, segundo dados da consultoria Frost & Sullivan (2019). No Brasil, também os números impressionam. O estudo conduzido pelo BNDES (2018), Plano Nacional de IoT (Internet das coisas ou Internet of things), estimou, para 2025, que apenas no âmbito da IoT poderiam ser adicionadas entre $50 e 200 bilhões de dólares à economia brasileira, sendo entre 0,9 e 1,7 bilhões referentes a cidades inteligentes (Brasil, 2021, p. 15).

Conforme o *Ranking Connected Smart Cities* (Urban Systems, 2023), o Recife é o 21º município mais inteligente do País. Tal ranking é composto por 74 indicadores em 11 eixos temáticos: mobilidade, urbanismo, meio ambiente, tecnologia e inovação, empreendedorismo, educação, saúde, segurança, energia, governança e economia. A edição coleta dados e informações de todos os municípios brasileiros com mais de 50 mil habitantes.

Ainda, a cidade do Recife foi eleita como base para o desenvolvimento desta pesquisa por ser considerada referencial na área do turismo e desenvolvimento tecnológico, em virtude do Porto Digital.

O Porto Digital é um dos principais parques tecnológicos e ambientes de inovação do Brasil e é um dos representantes da nova economia de Pernambuco. Instalado na área central do Recife, atua na produção de *software* e serviços de Tecnologia da Informação e Comunicação (TIC), economia criativa e foco no futuro das cidades por meio de prototipação com base em fabricação digital e Internet das coisas.

Conforme dados de 2022 (Moraes, 2023), o parque tecnológico é composto por mais de 350 empresas, cujo faturamento gira em torno de R$ 4,75 bilhões, empregando mais de 17.000 pessoas

Além disso, o Recife possui cerca de 1.653.461 de habitantes e uma escala territorial de 218,843 km², de acordo com o Instituto Brasileiro de Geografia e Estatística (IBGE) (2020). Traz consigo questões intimamente ligadas às cidades inteligentes e à privacidade, como a mobilidade urbana e a segurança pública, tornando-se um desafio para gestores e cidadãos.

Dentre os problemas que serão discutidos, está a falta de padrões universais abertos para a troca de dados, o que se relaciona em como os dados coletados pelo Estado vão para repositórios privados.

Os dados abertos são uma questão fundamental para a participação das pessoas em cidades inteligentes. Na pior das hipóteses, uma cidade inteligente pode se tornar o feudo de dados privados nas mãos de um monopólio de tecnologia ou telecomunicações (Ribeiro, 2017). Essas questões integram as preocupações e incertezas contínuas sobre quem é o proprietário e como controlar o "*Big Data*".

Assim, a pesquisa irá auxiliar a população para que identifique e participe da construção da cidade, bem como possibilitará aos governos melhor enfrentamento dos desafios e aproveitamento de oportunidades tecnológicas sem que gerem danos à privacidade.

Como demonstrado, o tema ganha relevo pelo aumento de investimento em tecnologias de governança e isso demanda regulamentação para que não ocorra uma exploração predatória dos dados dos cidadãos, dotados de grande valor econômico.

Por fim, o trabalho ainda contribuirá para a formação de uma necessária literatura que examine as cidades inteligentes e a privacidade em termos do contexto social no Brasil e das regras obrigatórias da legislação brasileira.

O objetivo geral é analisar, a partir do caso da cidade do Recife, se a LGPD é capaz de controlar possíveis ameaças à privacidade pessoal de cidades inteligentes. Especificamente, o estudo visa: a) elaborar revisão sistemática multi/transdisciplinar sobre as cidades inteligentes; b) identificar atores e ações relacionados a projetos de cidade inteligente no Recife; c) levantar a legislação sobre políticas públicas relacionadas ao tema cidades inteligentes em Recife-PE; d) apontar possíveis caminhos para melhoramento da proteção de dados dos cidadãos em razão das ameaças à privacidade provocadas pelas cidades inteligentes, a partir do Recife.

O trabalho é dividido em 5 capítulos, além desta introdução e da conclusão. No primeiro capítulo, é tecido um apanhado histórico acerca do desenvolvimento da Internet e o surgimento da era da informação, como pressuposto para as implicações desse fenômeno com a privacidade. Aborda-se a evolução da Internet e a emergência da sociedade da informação, fundamentais para compreender a interação entre tecnologia e privacidade. Também se demonstra como o avanço tecnológico remodelou as interações sociais e as implicações disso para a privacidade individual, destacando o papel crescente da informação como recurso valioso na era digital.

No segundo capítulo, aborda-se o papel da legislação sobre privacidade na atualidade, tendo em vista a popularização da Internet e dos meios computacionais se tornou um ponto central nas sociedades contemporâneas. A partir da revisão da literatura sobre legislações referidas à proteção de dados, no Brasil e na União Europeia, compara-se os dois documentos, a fim de encontrar semelhanças e diferenças entre a *General Data Protection Regulation* (União Europeia, 2016) e a Legislação de Proteção de Dados do Brasil (Lei n.º 13.709/2018).

O terceiro capítulo detalha a provisão de Internet e os serviços de aplicativos, enfatizando a necessidade de neutralidade da rede e a responsabilidade dos provedores na proteção de dados. Discute-se o papel do Marco Civil da Internet e da LGPD na regulação do tratamento de dados, pontuando o impacto dessas leis no cenário nacional de proteção de dados.

O terceiro capítulo também se aprofunda na tutela da privacidade pelo direito pátrio. A análise se volta para o contexto das contratações públicas e parcerias para inovação tecnológica, observando a ausência de disposições claras sobre privacidade e proteção de dados, critica-se a falta de mecanismos legais para garantir a privacidade desde a concepção em projetos desenvolvidos em parceria com o setor público.

O quarto capítulo explora o conceito de cidades inteligentes e sua interseção com a Lei Geral de Proteção de Dados no Brasil, usando a cidade do Recife como um estudo de caso. Aborda como a tecnologia da informação e comunicação (TIC) promove o desenvolvimento de cidades inteligentes e examina as implicações jurídicas relacionadas à privacidade e à proteção de dados que surgem nesse contexto.

Delineia o conceito de cidades inteligentes, que são promovidas por autoridades nacionais e municipais, grandes corporações globais de tecnologia, e

organizações internacionais como a Comissão Europeia, a *Organisation for Economic Co-Operation and Development* (OECD) e a *International Organization for Standardization* (ISO) e destaca as preocupações sobre a influência das empresas privadas nos espaços urbanos e na governança democrática, os riscos de vigilância em massa, vazamentos de dados e a falta de consentimento informado.

O quinto e último capítulo trata da a evolução histórica, urbanística e tecnológica da cidade do Recife, contextualizando-a no âmbito de uma cidade inteligente que busca integrar avanços tecnológicos à gestão urbana. Identifica, por fim, desafios que ameaçam a integridade deste desenvolvimento: a falta de transparência e abertura dos dados municipais.

Por fim, conclui-se pela importância da transparência e do acesso igualitário à informação como pilares para a proteção de dados e a promoção de uma governança inclusiva e democrática, apontando para a necessidade de revisões normativas e práticas que alinhem a cidade com os princípios da LGPD.

1 CONSIDERAÇÕES PRELIMINARES SOBRE A INTERNET E A SOCIEDADE DA INFORMAÇÃO

No século XXI, os direitos da personalidade, bem como os direitos ditos fundamentais ou humanos, precisam ser interpretados em consonância com as pluralidades de personalidade e com as diferenças culturais. Isso implica, também, considerar as transformações sociais trazidas pelo desenvolvimento das tecnologias da informação e seus princípios, como o compartilhamento, a liberdade de acesso, comunicabilidade, participação, dentre outros, além da análise das subculturas surgidas com este amadurecimento.

Alguns autores nomeiam o atual estágio da civilização ocidental como sendo a “era da informação”, a “sociedade informacional” ou qualquer expressão semelhante que represente o redimensionamento do valor da informação e do conhecimento em qualquer mercado ou ciclo de produção. O acesso à informação é uma característica da chamada cibercultura, expressão que representa uma série de impactos socioculturais das tecnologias digitais na sociedade.

Nesse sentido, Pierre Lévy usa a expressão “dilúvio da informação” na contemporaneidade, defendendo inclusive que se trata de um caminho sem volta, característica a qual os tradicionais institutos sociais devem ficar acostumados e assim saber conviver (Lévy, 2010).

Dentre as tecnologias da informação, inclui-se todo o conjunto de tecnologias em microeletrônica, computadores, telecomunicações e ainda aspectos tecnológicos da engenharia genética (Castells, 2002). Nesse estágio civilizacional, o conhecimento se torna uma espécie de moeda, ou, pelo menos, uma espécie de fator real de influência nos negócios, no mercado e em qualquer setor produtivo.

Tanto é assim que empresas, artistas, desenvolvedores, pensadores etc., estão permanentemente buscando proteção para seus conhecimentos ou para os resultados destes. A informação vira objeto da tecnologia, que por sua vez se torna a causa de uma verdadeira revolução, da mesma forma como fora a energia elétrica para a revolução industrial (Saldanha *et al.*, 2017).

Com pressuposto para compreensão do conceito de privacidade e Internet no âmbito do Direito brasileiro, na presente seção, é elaborada uma digressão histórica sobre a origem da Internet no Brasil e no Mundo, ao mesmo tempo em que é exposto o seu conceito e suas repercussões na legislação brasileira, sobretudo a Lei n.º

12.965/14 (Marco Civil da Internet) e Lei n.º 13.709/2018 (e a Lei Geral de Proteção de Dados Pessoais).

Nada obstante, adverte-se que o objetivo não é realizar uma historiografia minuciosa, visa-se, como dito, expor os aspectos introdutórios do tema.

1.1 A EVOLUÇÃO HISTÓRICA DA INTERNET

A palavra “Internet”, no inglês, é o resultado da união entre o prefixo *inter* (que representa internacional) e a palavra *net* (rede, em português). Significa, portanto, rede internacional. Apesar das diversas definições sobre a Internet na literatura, Gustavo Corrêa a conceitua como

> [...] um sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina à outra qualquer, conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando com a criação de novos mecanismos de relacionamento (Corrêa, 2002, p. 8).

Em outras palavras, é um conglomerado de conexões entre máquinas que, de modo bastante descentralizado, podem compartilhar dados e mensagens por meio de um conjunto de protocolos chamado de “*Internet Protocol Suite*” ou simplesmente de *Transmission Control Protocol/Internet Protocol* (TCP/IP). De acordo com Castells (2003), nesse protocolo comum, criado por Vint Cerf e seu grupo de pesquisas em Stanford, o TCP cuida da transmissão de dados e da correção de erros, e o IP, do endereçamento.

Em decorrência da criação da Internet, surgiu sua subdivisão entre intranet e extranet. A Internet atua de modo bastante descentralizado e irrestrito, possibilitando a acessibilidade a qualquer pessoa, em qualquer lugar e tempo. A intranet, por sua vez, surgiu da necessidade de as empresas centralizarem as informações como forma de conter gastos, sendo restrita à instituição e seus colaboradores, os quais acessam a intranet por meio de um nome de usuário e senha específicos (ARAYA, VIDOTTI, 2010).

Ademais, a intranet viabiliza um maior número de protocolos de comunicação, não somente o *Hypertext Transfer Protocol* (HTTP – em português, Protocolo de Transferência de Hipertexto) utilizado pela Internet. De modo bastante comum, o acesso à intranet é realizado em um servidor local em uma rede local denominada

LAN, sigla da língua inglesa que significa “*Local Area Network*” (rede de acesso local), instalada na própria empresa. Por último, a extranet enquadra-se como uma ampliação do conceito de intranet.

A Internet surge dentro do contexto da Guerra Fria (1945-1991), quando as superpotências União Soviética e Estados Unidos travaram uma longa disputa de poder e hegemonia, polarizando o mundo após a Segunda Guerra Mundial. Com o receio de ataques russos às suas bases militares, os Estados Unidos idealizaram um sistema de compartilhamento de informações como forma de fortalecer as estratégias de combate.

Nessa conjuntura, a agência norte-americana *Advanced Research and Projects Agency* (ARPA), mirando conectar os computadores dos seus departamentos de pesquisa, criou a Arpanet, protótipo da primeira rede de Internet, que a partir de 1969 estabelecia conexão entre quatro instituições: Universidade da Califórnia, Universidade de Santa Bárbara, Instituto de Pesquisa de Stanford e Universidade de Utah.

A Arpanet operava por meio de um sistema chamado chaveamento de pacotes, um sistema de transmissão de dados em rede de computadores, no qual as informações são repartidas em pequenos pacotes que são devidamente preenchidos de trecho dos dados do endereço do destinatário, bem como de informações que possibilitavam a remontagem da mensagem original (Castells, 2013).

Durante a década de 1970, com a diminuição da tensão entre as duas superpotências, estudiosos e pesquisadores americanos, livres da iminência de um suposto ataque, intensificaram os estudos acerca da rede, e, a partir disso, foi criado o TCP/IP, conglomerado de protocolos que permitem a troca de mensagens de uma rede para a outra, sendo esses a principal base operacional da Internet até hoje.

A partir de então, os protocolos TCP/IP foram implantados ao Sistema Operacional UNIX, portátil e multitarefa, desenvolvido pelos Laboratórios Bell. Esse sistema operacional passou a ser usado pela Universidade da Califórnia e, depois, por diversas universidades que passaram a integrar a Arpanet. Esse marco é importante porque o sistema operacional Unix “permitia que computadores copiassem arquivos uns dos outros” (Araya; Vidotti, 2010, p. 25).

No ano de 1985, por meio da *National Science Foundation* (NSF), o governo estadunidense interconectou os supercomputadores do seu centro de pesquisa, a NSFNET, que no ano seguinte aderiu à Arpanet. A Arpanet e a NSFNET tornaram-se,

assim, as espinhas dorsais (*backbones*) de uma nova rede que, conjuntamente com outros computadores a elas conectadas, formou a Internet (Vale; Costa; Alves Júnior, 2014).

Em 1992, o cientista britânico Tim Berners-Lee, da Organização Europeia para a Pesquisa Nuclear, criou um navegador conhecido como *World Wide Web* (www). Averiguado o incrível potencial de rentabilidade que esse inovador meio de comunicação poderia proporcionar, a Internet deixou de ser uma instituição meramente acadêmica e de estratégias bélicas e passou a ter finalidade comercial. Assim, a década de 1990 foi a do “boom da Internet”, quando ela se popularizou pelo mundo através do surgimento de novos navegadores como o Internet Explorer, Mozilla Firefox, Google Chrome, entre outros (Vale; Costa; Alves Júnior, 2014).

Como reflexo da criação de diversos navegadores, ocorreu uma vasta proliferação de sites e redes sociais tais como o *Orkut*, o *Facebook*, o MSN, o *Twitter*, *Instagram*, entre outros, que fizeram crescer de forma exponencial o número de usuários, e hoje é quase impossível encontrar alguém na face da Terra que não seja usuário da Internet.

1.1.1 A Internet no Brasil

De acordo com Rezende e Lima (2016), o debate sobre a criação de uma rede de transmissão de dados no Brasil começou na década de 1970, quando houve um aumento nas compras de equipamentos de informática no país. Até então, os principais computadores existentes em território nacional pertenciam a universidades e agências governamentais.

Segundo as mesmas autoras, em 1979, foi criada a Secretaria Especial de Informática (SEI), que posteriormente criou a Comissão Especial de Teleinformática, responsável por direcionar os rumos para o desenvolvimento do setor, de maneira que houvesse melhor integração com a Política Nacional de Informática. A SEI foi também responsável pelas decisões exclusivas sobre a transferência de dados para o exterior e era quem decidia autorizar seu uso ou não (Rezende; Lima, 2016).

Contudo, a SEI era subordinada ao Serviço Nacional de Inteligência e ao Conselho de Segurança Nacional do governo do Presidente (General) João Figueiredo, portanto, alvo da interferência militar. Isso intimidou professores universitários e membros de empresas estatais, que foram chamados para depor

pelos militares para a construção de um relatório sobre a situação informática. Essa intervenção marcou um retrocesso no avanço tecnológico que vinha sendo desenvolvido e fez com que o setor entrasse em crise (Rezende; Lima, 2016),

Logo após surgir, a SEI criou uma Comissão Especial de Teleinformática, responsável por analisar o panorama da teleinformática nacional e orientar a SEI e o Ministério da Comunicação no direcionamento de uma política para o desenvolvimento do setor, integrada no quadro mais geral da Política Nacional de Informática (Benakouche, 1997, p. 127).

Como consequência do trabalho dessas organizações, em 1984, foi publicada a Lei n.º 7.232/1984, conhecida como “Lei da Informática”, que propunha a criação de uma reserva de mercado para incentivar a criação de produtos nacionais de informática.

A Internet propriamente dita só veio chegar ao Brasil em 1988, quando o Laboratório Nacional de Computação Científica (LNCC), no Rio de Janeiro, teve permissão do Governo e conseguiu entrar em conexão com a Universidade norte-americana de Maryland e, a partir disso, abriu caminho para que as universidades brasileiras conectassem com as instituições nos Estados Unidos (Carvalho, 2006).

Em 1989, o Ministério da Ciência e Tecnologia criou a Rede Nacional de Ensino e Pesquisa (RNP), com a intenção de construir a infraestrutura para a criação de uma rede nacional de Internet para a comunidade acadêmica. A RNP é uma organização de interesse público cujo principal propósito, desde o nascedouro, é fazer uma rede de cunho acadêmico cuja extensão abrange todo o Brasil (Rezende; Lima, 2016).

Somente em 1995 foi implantada a Internet comercial, que estendeu o acesso à rede para todo o país de forma descentralizada e indistinta. Carvalho (2006, p. 138) ressalta que “a Embratel iniciou seu serviço de acesso à Internet via linha discada (14.400 bps) em caráter experimental em dezembro de 1994, por meio de um teste com um pequeno grupo de usuários”.

Só em 1995 ela passou a oferecer o serviço de acesso à Internet através do acesso ao *Global Internet Exchange* (GIX) que provia acesso *ao Commercial Internet eXchange* (CIX) nos Estados Unidos. A partir de então, não só as entidades acadêmicas poderiam acessar o mundo virtual, mas o serviço foi, de forma bastante democrática, disponibilizado às pessoas físicas e jurídicas.

Depois disso, criou-se o Comitê Gestor de Internet, através de nota conjunta do Ministério das Comunicações e do Ministério da Ciência e Tecnologia. O objetivo do Comitê é tornar factual a participação de toda a sociedade nas decisões relativas à implantação, administração e uso da Internet no Brasil. O órgão possui múltiplas competências, entre elas as de acompanhar a disponibilização de serviços de Internet no Brasil, registrar os nomes de domínios, coordenar a atribuição de endereços de IP e recomendar procedimentos operacionais e técnicos para os serviços de Internet (Carvalho, 2006, p. 148).

Em 15 de agosto de 1995, foi publicada a Emenda Constitucional n.º 8, que permitiu a flexibilização do monopólio estatal na exploração dos serviços públicos de telecomunicações, abrindo a área à competição do mercado, uma vez que o Estado não era capaz de atender à demanda do capital privado.

Assim, referida alteração na Constituição da República Federativa do Brasil de 1988 (CRFB/1988) permitiria a elaboração de leis que estimulassem a competição na área, como a Lei n.º 9.295/96 – Lei Geral das Telecomunicações. O diploma normativo regulamentou a participação da iniciativa privada na exploração do serviço móvel celular, de satélites e dos serviços via satélite, comunicação de dados e serviços de valor adicionado, viabilizando a fase inicial da Emenda Constitucional da quebra do monopólio e criando condições para a ampliação do serviço comercial da Internet.

Com isso, a Internet decolou, principalmente devido à melhoria nos serviços oferecidos pela Embratel e ao crescimento do mercado brasileiro. Portanto, a Internet no Brasil cresceu de modo exponencial em número de usuários, provedores e de serviços oferecidos por ela (Carvalho, 2006).

A despeito do percurso de 30 anos de Internet no Brasil e dos cerca de 100 milhões de usuários, faltava ainda uma lei que regulamentasse os direitos e deveres do usuário e guiasse as questões relativas à governança da Internet. Esse longo período de insegurança jurídica foi rompido pela Lei n.º 12.965/14, o Marco Civil da Internet e Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

De acordo com Rezende e Lima (2016), o Marco Civil da Internet foi pensado como um conjunto de normas para regulamentar o uso da Internet com base em princípios tais quais a neutralidade da rede, a privacidade do usuário e a liberdade de expressão. Planejado inicialmente em 2009, nos primeiros anos do Governo Dilma

Rousseff, a proposta era a criação democrática de uma lei com ampla participação da comunidade.

Oriunda do Projeto de Lei n.º 2.126/2011, de iniciativa do Poder Executivo Federal, a Lei n.º 12.965/14 foi sancionada em 23 de julho de 2014, cinco anos depois do início do seu planejamento, cujo objetivo é regulamentar o universo jurídico da Internet, que antes só se encontrava respaldo na doutrina e jurisprudência.

O Marco Civil da Internet regulamenta nacionalmente o uso da rede mundial de computadores, dispondo de princípios e garantias que asseguraram a circulação de uma rede livre e democrática, além de garantir os direitos e estabelecer os deveres dos usuários, provedores e dos serviços online. Para Jesus e Milagre (2014, p. 88), ele garante o "mínimo em segurança jurídica que o País necessitava, de modo a evitar decisões contraditórias em casos similares e fomentar o desenvolvimento econômico e a inovação".

O art. 1º da Lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação dos entes federativos sobre a matérias. A lei está dividida em cinco capítulos e 32 artigos. Os quatros primeiros capítulos são expostos resumidamente a seguir, excetuando-se o último, por se tratar apenas das disposições finais.

O primeiro capítulo pontua os fundamentos, princípios e objetivos que regem a Lei, como o respeito à liberdade de expressão; os direitos humanos e o exercício da cidadania em meio digital; a manifestação livre do pensamento com base na Constituição Federal; a proteção da privacidade do usuário e de seus dados pessoais; a preservação e garantia da neutralidade da rede; a preservação da natureza participativa da rede; o direito de acesso à Internet, à informação e ao conhecimento.

O segundo capítulo trata dos direitos e garantias do usuário. Parte-se do princípio de que o acesso à Internet é essencial para o exercício da cidadania. Portanto, o usuário tem o direito a ter sua vida privada e intimidade preservadas e, em caso de violação, o direito à indenização; inviolabilidade e sigilo do fluxo de comunicações pela Internet e comunicações privadas armazenadas, exceto por ordem judicial.

Sobre os dados pessoais, registros de conexão e aplicações de Internet, o Marco Civil da Internet, antes mesmo da LGPD, já proibia aos provedores de aplicações que armazenassem dados dos usuários, exceto pela sua autorização, que

poderá ser cancelada a qualquer momento e, consequentemente, os dados totalmente excluídos.

O terceiro capítulo trata da provisão de conexões e serviços de aplicações, impondo que a conexão deve ser neutra, ou seja, os pacotes de dados não devem conter distinção entre conteúdo, origem e destino, serviço, terminal ou aplicação, salvo exceções em casos especiais, como em serviços de emergência. O mesmo capítulo também regulamente a atividade dos provedores quanto à coleta, guarda, armazenamento e tratamento de registros de dados, impondo o respeito ao sigilo destes. Ademais, normatiza que os provedores de conexão não são responsáveis por conteúdo danoso gerado por terceiros, salvo quando descumpre ordem judicial que impõe a retirada do ar do conteúdo.

O quarto capítulo aborda a atuação do Poder Público, definindo diretrizes para a atuação dos entes federativos em relação ao desenvolvimento da Internet e utilização da mesma pelo Poder Público. Vale destacar a ênfase que a legislação dá, quanto ao papel do Estado na educação e o uso da Internet como ferramenta para o exercício da cidadania, promoção cultural e desenvolvimento tecnológico.

Já a Lei Geral de Proteção de dados (Lei n.º 13.709/2018) cria um quadro normativo inspirado pelo Regulamento Europeu de proteção de dados pessoais na Internet. Desse modo, a legislação estabelece uma série de obrigações para as empresas em relação à coleta, do uso e das garantias de integridade dos dados pessoais, sob pena de pesadas sanções.

Da mesma forma, atribuiu direitos aos titulares dos dados pessoais que podem ser exercidos contra quaisquer empresas ou entidades públicas que detenham tais informações. Nesse sentido, se os dados pessoais se tornaram indubitavelmente um precioso ativo, eles podem dar origem, se mal administrados, a um importante passivo para aqueles que os detêm.

Uma vez exposto brevemente o desenvolvimento da Internet e sendo a Lei Geral de Proteção de Dados o objeto central da presente dissertação, a ela será dedicada capítulo próprio, iniciado a seguir.

2 O DESENVOLVIMENTO DA PROTEÇÃO DE DADOS

A presente seção pontua os aspectos importantes sobre a Lei Geral De Proteção de Dados, destacando o desenvolvimento da proteção de dados no contexto global e nacional.

A LGPD entrou em vigor depois de oito anos de debates. Seu conteúdo é baseado no Regulamento de Proteção de dados da União Europeia (*General Data Protection Regulation* – GDPR). Considerando não só a inspiração do diploma internacional para elaboração da lei brasileira, mas também os reflexos da globalização e o caráter internacional da Internet, o presente tópico apresenta como, no cenário global, foi se desenvolvendo a concepção de proteção de dados até chegar ao GDPR.

De acordo com Viktor Mayer-Schönberger (1997), a noção de proteção de dados é resultado de uma série de gerações de leis sobre o tema. Segundo ele, a primeira fase de leis desse tipo visava regulamentar um cenário no qual centros de processamento de dados de grande porte concentravam a coleta e gestão de dados pessoais, sendo esses centros criados mediante autorizações e sob o controle do Poder Público.

Portanto, regia o uso de informações pessoais pelo Estado e pelas suas estruturas administrativas, ele era o destinatário principal (quando não o único) destas normas. A estrutura e a gramática destas leis eram tecnocráticas e condicionadas pela informática. Elas se tornaram obsoletas em razão da multiplicação dos centros de processamento de dados, o que inviabilizou o controle baseado em um regime de autorizações (Mayer-Schönberger, 1997).

A segunda geração de leis surgiu no final da década de 1970. Seu primeiro grande exemplo foi a lei francesa de proteção de dados pessoais de 1978, a Lei *Informatique et Libertées*. Nesta segunda fase, as leis não se dirigiam apenas ao fenômeno computacional em si, mas na privacidade e proteção dos dados pessoais como uma liberdade negativa, a ser exercida pelo próprio cidadão.

Antes, o objetivo era evitar o uso de informações pessoais nas redes, agora, o uso dessas informações passou a ser um requisito para a vida social, de modo que se o cidadão negasse a utilização dos seus dados com base em direitos da personalidade ou privacidade, seria excluído da sociedade (Mayer-Schönberger, 1997).

Já a terceira geração de leis, surgida na década de 1980, além de sofisticar a tutela dos dados pessoais, visou garantir a efetividade desta liberdade. De acordo com a Escola Nacional de Defesa do Consumidor (Brasil, 2010, p. 42), nesse momento:

> o tratamento dos dados pessoais era visto como um processo, que não se encerrava na simples permissão ou não da pessoa à utilização de seus dados pessoais, porém procurava inclui-la em fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros, além de compreender algumas garantias, como o dever de informação.

Tais leis fortaleceram a posição da pessoa em relação às entidades que coletam e processam seus dados, reconhecendo um desequilíbrio nesta relação, o qual não era resolvido por medidas que simplesmente reconheciam o direito à autodeterminação informativa. Elas também reduziram o papel da decisão individual de autodeterminação informativa em certos contextos, como quanto a certos dados sensíveis. Exemplo são as Diretivas europeias em matéria de proteção de dados, em especial a Diretiva 95/46/CE e a Diretiva 2000/58/CE (conhecida como “Diretiva sobre privacidade e as comunicações eletrônicas”).

De acordo com a União Europeia (2020a), a Diretiva 95/46/CE é o marco para a trajetória que culminou, recentemente, no Regulamento Geral sobre Proteção de Dados da União Europeia. Tal Diretiva trata da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

Já a Diretiva 2000/58/CE tratou da confidencialidade das comunicações conforme os instrumentos internacionais relacionados aos direitos humanos, especialmente os Convenção Europeia para a Proteção dos Direitos Liberdades humanas e fundamentais e as constituições dos Estados-Membros (European Union, 2020a).

Seguindo a linha cronológica, em 2011, a Autoridade Europeia para a Proteção de Dados, entidade independente dotada de poderes de supervisão, publica um parecer sobre a Comunicação da Comissão Europeia alegando a necessidade de uma regulação uniforme e abrangente, bem como acerca da necessidade de atualização das normas até então vigentes. Um ano depois, a Comissão Europeia elabora proposta para fortalecer os direitos de privacidade on-line e impulsionar a economia digital da Europa (European Union, 2020a).

Os anos de 2012 e 2013 foram de debates, até que tal proposta teve voto de apoio pelo Parlamento Europeu em 12/03/2014, tendo sido aprovado por 621 votos a favor, 10 contra e 22 abstenções (European Union, 2020a). Em 2015, a Comissão

Europeia e o Parlamento Europeu fecham acordo sobre a GDPR e levam a legislação adiante. Em 27 de abril de 2016, foi emitido o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho Europeu.

O *General Data Protection Regulation* passou a ser um marco mundial. Tal regulamento foi criado para uniformizar as normas de proteção de dados entre os países da União Europeia. O seu âmbito de aplicação objetiva abrange toda e qualquer operação de "tratamento" de "dados pessoais", ambos os termos dotados de definição ampla na norma. Isso inclui a coleta, o registro, a organização, a conservação, a utilização, a divulgação e destruição de qualquer informação relativa a uma pessoa física identificada ou identificável (European Union, 2020b).

Do ponto de vista subjetivo, o regulamento é aplicável não apenas a empresas física dos países que integram a União Europeia, mas também a pessoas físicas e jurídicas estabelecidas inteiramente fora daquele território.

O GDPR estabelece uma série de direitos para os titulares de dados pessoais e impõe diversas obrigações aos agentes de tratamento, sejam eles controladores – que determinam as finalidades e os meios do tratamento, ou processadores – que façam as operações de tratamento por conta dos controladores.

O tratamento de dados pessoais pode ser feito por esses agentes não apenas mediante o consentimento do titular, mas também quando necessário para a execução de um contrato do qual o titular dos dados seja parte, para o cumprimento de obrigação jurídica a que o agente do tratamento esteja sujeito, para a defesa de interesses vitais do titular ou de outra pessoa física, além de outras hipóteses.

Quando fundado no consentimento, este deve corresponder a uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular aceita, mediante declaração ou ato positivo inequívoco, que os seus dados pessoais sejam objeto de tratamento. O titular tem o direito de retirar o seu consentimento a qualquer momento, com a mesma facilidade com que o tenha dado.

Há outros direitos relevantes previstos no GDPR, assegurados ao titular dos dados pessoais independentemente de o tratamento ser realizado com base no seu consentimento ou sob outra circunstância prevista na norma (European Union, 2020b). São eles:

- Direito de acesso, segundo o qual o titular pode pleitear e obter do agente a confirmação de que os seus dados pessoais são ou não objeto de tratamento e, em caso positivo, acessar tais dados e obter informações

como as categorias de dados pessoais tratados, as finalidades do tratamento, os terceiros para os quais foram ou serão divulgados e a existência de decisões automatizadas, incluindo para a criação de perfis (seção 2, art. 15, do GDPR);

- Direito de retificação, pelo qual o titular pode pleitear e obter do agente de tratamento, sem demora injustificada, a correção dos dados pessoais inexatos que lhe digam respeito (seção 3, art. 16, do GDPR);
- Direito de apagamento, pelo qual o titular pode pleitear e obter do agente o apagamento dos seus dados pessoais quando deixarem de ser necessários para a finalidade que motivou sua coleta ou tratamento, bem como (sendo o caso) se o titular retirar o seu consentimento, entre outras circunstâncias (seção 3, art. 17 do GDPR);
- O inovador direito de restrição do tratamento, que pode ocorrer, por exemplo, quando o tratamento for ilícito e o titular se opuser ao apagamento dos seus dados pessoais, solicitando ao agente, em vez disso, a limitação da sua utilização (seção 3, art. 18 do GDPR);
- O também inovador direito de portabilidade dos dados, pelo qual o titular pode pleitear e receber do agente de tratamento os dados pessoais que lhe tenha fornecido, em formato estruturado, de uso corrente e de leitura automática, bem como transmiti-los livremente a outro agente (seção 3, art. 20, do GDPR).

As autoridades de controle têm amplos poderes de investigação sobre os agentes de tratamento de dados pessoais, incluindo as prerrogativas de requisitar informações, obter acesso às suas instalações, ordenar a adoção de medidas para o cumprimento dos deveres e obrigações previstos no GDPR, impor limitação temporária ou definitiva e até a proibição do tratamento de dados, bem como aplicar multas em valores que podem chegar a 20 milhões de euros ou, no caso de empresas, a 4% do seu faturamento anual em nível mundial — o que for maior.

O rol de direitos garantido pelo GDPR aos titulares de dados pessoais e de obrigações compulsórias aos agentes de tratamento não se limita aos exemplos destacados acima. Há, ainda, muitas outras regras a serem observadas por pessoas físicas e jurídicas que realizem operações de tratamento de dados pessoais abrangidas pelo campo de incidência do GDPR, incluindo condições específicas para a transferência internacional dessas informações.

A mudança promovida pelo GDPR é profunda, mas o próprio texto fornece subsídios para a identificação e implementação dos ajustes necessários aos agentes de tratamento de dados pessoais ao detalhar a forma pela qual devem cumprir os deveres e obrigações previstos, assim como ao descrever medidas de organização e procedimentos internos a serem observados para o atendimento da norma. As empresas que se anteciparem nesse processo de mudança certamente terão maior facilidade na adequação de suas práticas ao GDPR.

2.1 A PROTEÇÃO DE DADOS NO BRASIL

A Lei Geral de Proteção de Dados foi promulgada em 14 de agosto de 2018, trazendo diversas inovações no Direito Digital Brasileiro. Como já mencionado, a legislação brasileira teve como base normas gerais acerca da proteção de dados da União Europeia. Nada obstante, já havia fundamentos legais para proteção de dados na legislação pátria antes mesmo da edição da Lei n.º 13.709/2018, os quais são tratados a seguir.

Antes da edição do Marco Civil da Internet e da LGPD, o reconhecimento da proteção de dados não era previsto expressamente como um direito autônomo, mas fruto da consideração dos riscos que o tratamento automatizado traz à proteção da personalidade à luz das garantias constitucionais, como o direito à igualdade substancial, à liberdade e à dignidade da pessoa humana, juntamente com a proteção da intimidade e da vida privada. Além desses direitos, o ordenamento pátrio protegia os dados a partir da ação de *Habeas Data* e da proteção às informações do consumidor nos termos do Código de Defesa do Consumidor (CDC).

Assim, as leis que versam sobre a proteção de dados pessoais eram idealizadas e essenciais, em decorrência da dispersão das diretrizes relacionadas ao tema em vários instrumentos normativos, como o Marco Civil da Internet, o CDC, o Código Penal, a Lei Anticorrupção, a Lei Geral de Telecomunicações, a Lei de Acesso à Informação, entre outro. Neste trabalho, restringe-se a análise à questão na esfera cível.

De acordo com Lais Bergstein, Flávia Aragão e Maria Câmara (2022, p. 3), “quando uma informação constitui dado pessoal ela passa a ser caracterizada como uma extensão do seu titular”. Sendo a personalidade um conjunto de características e atributos da pessoa humana, ela é considerada um valor, tendo em vista que os

atributos inerentes ao ser humano se irradiam da personalidade, constituindo bens jurídicos em si mesmos e, portanto, dignos de tutela privilegiada.

Sendo um valor e não um direito, a personalidade tem diversos atributos que, por vezes, não são passíveis de enumeração. Cada novo aspecto da personalidade humana construída ao longo das situações existenciais reforça ser a personalidade algo inerente ao ser humano (Bergstein; Aragão; Câmara, 2022).

De acordo com Bruno Bioni (2019, p. 58), “os dados que influem na projeção de uma pessoa e na sua esfera relacional adequam-se conceitualmente como um novo direito da personalidade. Alocar a proteção dos dados pessoais nessa categoria jurídica é uma construção dogmática necessária”.

A Constituição alberga o problema da informação através das garantias à liberdade de expressão e do direito à informação, junto aos direitos da personalidade e, em especial, o direito à privacidade. Nesses termos, a Carta Magna considera invioláveis a vida privada e a intimidade (art. 5º, X) e regulamenta a interceptação de comunicações telefônicas, telegráficas ou de dados (art. 5º, XII), bem como instituiu a ação de *Habeas Data* (art. 5º, LXXII), que estabelece uma modalidade de direito de acesso e retificação dos dados pessoais.

Na legislação infraconstitucional, o art. 43 do CDC já previa uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em “bancos de dados e cadastros”, implementando uma sistemática baseada nos *Fair Information Principles* à matéria de concessão de crédito e possibilitando (Brasil, 1990).

Inclusive, parte da doutrina aponta esta norma como marco dos princípios de proteção de dados pessoais no direito brasileiro (Lima, 2014). Esse art. 43 foi inspirado na normativa estadunidense de proteção ao crédito estabelecida pelo *National Consumer Act* e pelo *Fair Credit Reporting Act* – FCRA, de 1970, conforme consta do anteprojeto do CDC (Benjamin, 2007).

A previsão do *Habeas Data* na Constituição introduziu em nosso ordenamento o direito de acesso, carregando algo da carga semântica do *Habeas Corpus*. Trata-se de um instrumento para a requisição de informações pessoais em posse do poder público, visando, sobretudo, a garantia de informações dos cidadãos presentes nos órgãos responsáveis pela repressão durante o regime militar.

Tal remédio constitucional foi regulamentado pela Lei n.º 9.507/1997, que garantiu ao cidadão acessar e retificar seus dados pessoais em bancos de dados “de

entidades governamentais ou de caráter público", inclusive dados referentes a consumidores, mesmo que administrados por privados.

A ação não é acompanhada, porém, de instrumentos que possam torná-la ágil e eficaz o suficiente para a garantia fundamental de proteção dos dados pessoais, além do seu perfil de proteção a liberdades negativas. Conforme a Escola Nacional de Defesa do Consumidor (Brasil, 2010, p. 51), isto é perceptível através de vários dos seus pontos estruturais, como a necessidade de sua interposição através de advogado ou então a necessidade de demonstração de recusa de fornecimento dos dados por parte do administrador de banco de dados.

O *Habeas Data*, hoje, é anacrônico e ineficaz à realidade das comunicações e tratamentos de dados pessoais na Sociedade da Informação.

O CDC, especificamente em seu art. 43, já tentava resolver o problema da utilização abusiva da informação sobre consumidores em bancos de dados. Inclusive, antes da edição da LGPD, ele foi responsável por suprir muitas das lacunas deixadas pela ausência de um marco normativo específico relacionado aos dados pessoais.

As disposições do diploma consumerista revelam que o legislador já se preocupava com o estabelecimento de equilíbrio na relação de consumo através da interposição de limites ao uso da informação. Assim, e.g., o registro de dados negativos sobre um consumidor não poderá ser mantido por um período maior de 5 anos; é prevista a necessidade de comunicação escrita sobre o tratamento da informação ao consumidor em certos casos, assim como o direito de acesso, correção e, implicitamente, o cancelamento justificado.

A partir do CDC, a doutrina explorava princípios de proteção de dados pessoais aplicáveis a situação não especificamente da relação de consumo, como o princípio da finalidade, através da aplicação da cláusula da boa-fé objetiva e da própria garantia constitucional da privacidade, pelo que os dados fornecidos pelo consumidor deverão ser utilizados somente para os fins que motivaram a sua coleta, o que servia como fundamentação para o reconhecimento de um princípio de vedação da coleta de dados sensíveis e da comercialização de bancos de dados de consumidores.

A fim de consolidar e trazer inovações referentes a proteção de dados na sociedade da informação, foi editada a LGPD.

Como já exposto, a proteção de dados pessoais na Internet foi consagrada na Lei n.º 12.965/2014, legislação pioneira no mundo que estabeleceu, em seu art. 3º,

inciso III, a elaboração de lei específica para a proteção de dados, o que só aconteceu em 10 de julho de 2018, data em que a LGPD foi aprovada.

O Marco Civil da Internet foi regulamentado pelo Decreto Lei n.º 8771/2015, que complementou as diretrizes de privacidade e liberdade de expressão, sendo possível depreender de seu conteúdo a preocupação com “uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes” (Brasil, 2014).

Uma vez exposto o desenvolvimento histórico da ideia de proteção de dados no Brasil e no mundo, o próximo capítulo dedica-se a analisar mais especificadamente os aspectos da proteção de dados no contexto nacional.

3 A LEI GERAL DE PROTEÇÃO DE DADOS E O DIREITO À PRIVACIDADE

Mesmo após a vigência do Marco Civil da Internet, seguiu-se sem nenhuma previsão legal acerca dos dados pessoais no Direito brasileiro, persistindo a insegurança jurídica nesse quesito. Tal previsão de caráter legislativo só veio com a LGPD, que regula as atividades de tratamento dos dados pessoais e que também altera os arts. 7º e 16 do Marco Civil da Internet.

A LGPD é oriunda do Projeto de Lei da Câmara n.º 53/2018, de iniciativa do Deputado Federal Milton Monti (PR/SP), fruto da aglutinação de outras propostas que tramitavam há anos no Congresso. Durante o período de trâmite, foram realizadas duas consultas públicas em que houve mais de 2.500 contribuições de atores nacionais e internacionais. A lei foi sancionada em 14 de agosto de 2018, publicada no Diário Oficial em 15 de agosto de 2018 e republicada parcialmente no mesmo dia em edição extra. A republicação se deu para ampliar o *vacatio legis* de 18 para 24 meses, com a edição da Medida Provisória n.º 869/2018.

Vale destacar que a matéria foi votada em regime de urgência no Plenário, depois de ter sido aprovada em maio de 2018 na Câmara e em julho de 2018 na Comissão de Assuntos Econômicos (CAE) do Senado, em razão dos escândalos de privacidade envolvendo o Facebook, a *Cambridge Analytics*, o Brexit e o Serviço Federal de Processamento de Dados (Serpro), relacionado à coleta indevida de milhões de dados pessoais de usuários da supracitada rede social, bem como dados pessoais de terceiros.

Sobre a *Cambridge Analytics*, trata-se de uma empresa privada britânica de consultoria comercial e política criada em 2013, cuja finalidade era atuar em campanhas eleitorais, coletando, tratando e analisando dados de usuários de redes sociais, sobretudo o Facebook, a fim de identificar o público-alvo de suas ações e direcionar propagandas, com o intuito de arrebanhar eleitores para determinados candidatos. O escândalo teve notoriedade na campanha eleitoral de Donald Trump e por suas ações no Brexit, sob acusações de coleta, uso e venda indevida dados de milhões de estadunidenses a fim de fazer circular *fake News* e moldar o pensamento dos usuários da Internet (Roncolato, 2018).

Em solos brasileiros, foi divulgado falha de segurança evidenciada no aplicativo e-Saúde, do Ministério da Saúde, com a presença de dados pessoais de inúmeras pessoas usuárias do Sistema Único de Saúde, com a exposição de dados

de ordem médica, histórico de utilização de medicamentos e consultas médicas nas redes públicas. Além disso, conforme reportagem do site de notícias G1 (2020), descobriu-se um esquema de venda de dados pessoais de brasileiros pelo Serviço Federal de Processamento de Dados (Serpro), com dados como endereço, nome da mãe, sexo e data de nascimento de inscritos no Cadastro de Pessoa Física (CPF) e Jurídica (CNPJ) por até R$ 273 mil.

Percebe-se que, no panorama brasileiro, há um eminente e contínuo risco de ataques cibernéticos através de hackers, contendo ameaças à segurança e privacidade dos dados pessoais. Dessa forma, o objetivo da regulamentação foi reprimir abusos relativos à proteção dos dados pessoais. Pois, a LGPD está adaptada ao contexto da evolução das tecnologias baseadas em plataformas digitais, *Big Data,* inteligência artificial, *machine learning*.

A LGPD no Brasil opera da mesma forma que o *General Data Protection Regulation* na União Europeia, e o *California Consumer Privacy Act* of 2018 (CCPA), nos Estados Unidos. Ela é fundamentada por múltiplos valores, tais como o respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e a inovação; à livre iniciativa, livre concorrência e defesa do consumidor e aos direitos humanos liberdade e dignidade das pessoas, os quais passam a ser abordados a seguir.

3.1 VIGÊNCIA, PRINCIPAIS CONCEITOS E ÂMBITO DE APLICAÇÃO DA LGPD

De acordo com o art. 3º da LGPD, suas normas se aplicam a qualquer operação de tratamento realizada por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, país de sua sede ou país onde estejam localizados os dados, desde que: (i) a operação de tratamento seja realizada no território nacional; (ii) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; e (iii) os dados pessoais objeto do tratamento tenham sido coletados no território nacional. Dessa forma, a Lei brasileira tem a mesma amplitude do GPDR Europeu.

Nada obstante, existem exceções acerca da aplicação da LGPD, conforme dispõe o art. 4º, inc. I, II, III, IV, que destaca a inaplicabilidade da lei ao tratamento de

dados pessoais: I – realizado por pessoa natural para fins exclusivamente particulares e não econômicos; II – realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, III – de a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais; ou IV – provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei (Brasil, 2018).

Dentre os conceitos trazidos pela LGPD no seu art. 5º, destacam-se o de:

(i). “Titular”, que se refere à pessoa natural cujos dados pessoais que são objeto de tratamento;

(ii). “Controlador”, isto é, a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

(iii). “Operador”: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador;

(iv). “Agentes de Tratamento”, que são o Controlador e o Operador;

(v). “Encarregado”, que é a pessoa natural indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares e a autoridade nacional de proteção de dados; e

(vi). a “autoridade nacional de proteção de dados”, o órgão da Administração Pública indireta responsável pelo cumprimento da lei geral de proteção de dados, criado posteriormente por ato do Poder Executivo.

3.1.1 Do Conceito de Dados

Para Semidão (2014), dado é o conhecimento bruto ou matéria-prima da informação que ainda não foi tratada e não gerou nenhuma informação relevante ao negócio. Castro (2011) afirma que dado é a sequência de quantificados ou quantificáveis que ainda não possui uma inteligibilidade à informação. Nada obstante, o conceito de dado varia conforme a ciência que o cerca.

O dado é diferente da informação, que, segundo Semidão (2014), o dado devidamente tratado que produziu um conhecimento relevante à organização. Castro

(2011) explica que a informação é vista como um estímulo a um determinado dispositivo, agrupado em padrões que influenciam a transformação de outros padrões, sem que a mente o reconheça tal como padrão. Em linhas gerais, a informação é a transformação de um dado em padrões que geram um valor.

Por fim, é necessário diferenciar o dado do termo “informação” e “conhecimento”. O conhecimento é a ação de entender por meio da inteligência. Nessa linha de raciocínio, a partir de uma coleta básica de um dado, é possível transformá-lo em informações processadas, agrupando em padrões pré-estabelecidos. O conhecimento é, então, o conjunto de informações agregados à inteligência. Para qualquer sistema, é necessário um processo contínuo de geração de dados, informações e produção de conhecimento.

O conceito de dados pessoais foi definido no Regulamento 2016/679 da União Europeia (GDPR) em seu art. 4º, n. 1, que estipula:

> Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular (European Union, 2016, tradução nossa).

Nesse diapasão, os dados pessoais são uma universalidade de “informações”, desde dados cadastrais como nome, endereço, e-mail, ao endereço de IP, dados biométricos, de raça, saúde (Lima, 2014, p. 155). As redes sociais – em especial *Facebook*, *Twitter* e *Instagram* – se destacam como plataformas de coleta desses dados, o que se dá geralmente por meio de testes, elaborados de forma atraente aos usuários, e que por meio do “aceite”, têm acesso a diversos dados como nome, idade, e-mail, e todas as fotos contidas no perfil do usuário.

A LGPD traz esse conceito no art. 5º, inc. I, segundo o qual dado pessoal é a “informação relacionada a pessoa natural identificada ou identificável”. Como se vê, a definição é bastante ampla. Constituem os dados pessoais o conjunto de informações distintas que podem levar á identificação de determinada pessoa. Ademais, nos termos do mesmo art. 5º, os dados pessoais podem ser classificados, além dos dados pessoais *latu sensu*, em dado pessoal sensível ou anonimizado. Referido dispositivo também define o que é banco de dados e anonimização de dados. Leia-se:

> Art. 5º: [...] 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; III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV – banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; [...] XI – anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; (Brasil, 2018).

Dessa forma, para a LGPD, dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, mas que ainda podem ser utilizados para reidentificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação do LGPD.

Alguns exemplos do que vem a ser dados pessoais são: nome, sobrenome, RG, CPF, apelido, data de nascimento, endereço de IP, os dados colhidos por um hospital que permitam identificar uma pessoa de forma inequívoca, fotos, imagens relativas às pessoas recolhidas através dos sistemas de videovigilância, gravação de chamadas telefônicas quando informadas à pessoa, pois com esses dados se vai imediatamente a um indivíduo.

Nada obstante, conforme art. 12, § 2º da LGPD, poderão ser igualmente considerados como dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada. Por outro lado, não são dados pessoais, por exemplo, o Número de Identificação do Registro de Empresas (NIRE) e um endereço de correio eletrônico de uma pessoa jurídica.

Dados como raça, etnia, religião, sexualidade e posição política podem eventualmente ser utilizados para fins espúrios por pessoas mancomunadas, por essa razão, são considerados ‘’sensíveis’’ e recebem proteção. São os dados relacionados a questões mais subjetivas e comportamentais, e, por terem maior potencial lesivo, caso violados, o seu tratamento deve observar regras mais rígidas.

Noutro giro, quando o dado não pode identificar, de forma direta ou indireta, um indivíduo, ele é chamado de dado anonimizado. Nos termos do art. 12 da LGPD, os dados anonimizados estão excluídos do escopo de aplicação da lei, uma vez que tais dados não identificam, per si, o titular, e não têm potencial de lhe causar danos.

A anonimização é uma das formas previstas na LGPD para assegurar proteção dos dados pessoais, devendo ser utilizada sempre que possível, como no caso de estudos em saúde pública, a fim de que deixem de ser considerados dados pessoais. Vale ressaltar que, para que os dados sejam verdadeiramente anonimizados, o processo deve ser irreversível.

3.2 DIREITOS DOS TITULARES DE DADOS PESSOAIS

O art. 18 da LGPD é expressão pormenorizada de tais direitos, aplicando-os ao armazenamento, recuperação e transferência de dados pessoais, como dispõe segundo o qual o titular tem direito a obter do controlador, a qualquer momento, e mediante requisição:

> Art. 18 da LGPD: I – confirmação da existência de tratamento; II – acesso aos dados; III – correção de dados incompletos, inexatos ou desatualizados; IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei ; VII – informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII – informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX – revogação do consentimento (Brasil, 2018).

Quanto ao procedimento para realização desse direito, diz o §1º do mesmo artigo que o titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional, mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento (§3º), sem custos para o titular.

3.3 ASPECTOS PRÁTICOS DA LGPD

A LGPD afeta inúmeras empresas nas mais diversas categorias de telecomunicação digital, como as redes sociais (*Facebook*, *Orkut*, *Twitter* etc.), servidores de Internet (*Google Chrome*, *Internet Explorer*, *Mozilla Firefox* etc.), bancos que utilizam o serviço de *Internet banking*, hospitais, universidades ou qualquer outra entidade que guardar banco de dados de terceiros por via digitais.

Alguns aspectos relacionados a Lei Geral de Proteção de Dados devem ser analisados, como: a) maior controle sobre como as farmácias usam o CPF e dados de saúde; b) um maior controle do usuário acerca dos seus próprios dados; c) discussão em condomínios residenciais acerca do reconhecimento da digital biométrica para controlar a entrada no prédio; d) sanções claras em caso de vazamento de dados pessoais.

Sobre as farmácias, a lei veda, e.g., os dados fornecidos pelo consumidor sejam compartilhados com os planos de saúde, para estabelecer uma diferença de preços de acordo com o seu perfil e sua doença; tal conduta é vedada pela impossibilidade de compartilhamento de dados de saúde com a finalidade de proveito econômico. O indivíduo deve ser informado do desígnio da coleta da existência ou não do tratamento desses dados, a fim de tomar a decisão sobre a aderência ao tratamento de seus dados.

Em alguns condomínios residenciais passou a ser adotada a biometria de forma compulsória para ingresso no local. Tal prática apresentou aspectos positivos: praticidade, segurança e uso de tecnologias. Entretanto, apresentou características negativas, como limitação da privacidade.

Com o advento da LGPD, a exigência obrigatória da biometria para entrada nos condomínios residenciais deve ser rediscutida em assembleia, e a nova Lei deverá ser observada, pois apenas deve ser exigida a biometria para fins de segurança, com a concordância dos condôminos, e, havendo condições seguras para o armazenamento de dados biométricos. Ademais, caso a coleta dos dados biométricos seja feita impositivamente, ela pode questionada com base no art. 5º, inc. II, da LGPD.

Após o inicial consentimento acerca da coleta de informações pessoais, ele passa a ter controle dos próprios dados, com direitos de modificação de informações incorretas, o que se opõe claramente a coleta de informações sensíveis, a exemplo de religião ou cor de pele, e revisões de decisões tomadas de maneira automatizada.

Sobre as multas e situações pecuniárias, o art. 52 da LGPD elencou, nos incisos I, II, III,I V, as responsabilidades e sanções administrativas que poderão ser aplicadas pela Autoridade Nacional de Proteção de Dados em caso de descumprimento das normas pelos agentes de tratamento, citando-se como exemplo: a responsabilização dos agentes de tratamento pelos danos decorrentes da violação da segurança dos dados pessoais em virtude da negligência na adoção de medidas

de segurança previstas na norma; a aplicação de multa de até 2% do faturamento do exercício social anterior do agente de tratamento ou do grupo econômico ou conglomerado de que faça parte no Brasil, limitada ao máximo de R$ 50.000.000,00 (cinquenta milhões de reais) por infração; e a possibilidade de publicização da infração apurada, que pode resultar em danos à credibilidade do agente de tratamento no mercado.

Dentre os critérios para a apuração da gravidade da infração e aplicação das sanções está a avaliação do empenho do infrator no combate a práticas abusivas e à proteção e segurança dos dados pessoais, como, e.g., a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano e demonstrar o tratamento seguro e adequado de dados pessoais, a adoção de política de boas práticas de governança e a pronta implementação de medidas corretivas, o que reforça a importância da revisão minuciosa das práticas dos *players* de mercado sob a ótica da LGPD.

Vale ressaltar que a LGPD outorga o tratamento de dados com a finalidade de cumprir imposição legal ou regulatória pelo responsável (art. 7ª, inc. II). É o caso de dados pessoais de empregados, como nome, endereço, férias, salários, benefícios, licenças, para fins de cadastramento obrigatório perante as autoridades públicas (e-social). Ademais, é liberado, também, na hipótese do compartilhamento de dados pessoais dos usuários dos serviços de telecomunicações e Internet, entre as empresas privadas e a Anatel, para fins de política pública de comunicações.

Igualmente, é lícito o tratamento de dados por parte da Administração Pública na hipótese de uso compartilhado de dados essenciais à realização de políticas públicas (art. 7º, III). Engajam-se nessa prognose as políticas públicas de tributação, com o compartilhamento de dados pessoais dos cidadãos, como a finalidade de arrecadar tributos.

Ainda, de acordo com a legislação brasileira, é permitido o tratamento de dado pessoal destinado à proteção do crédito (art. 7º, X), como ocorre no sistema nacional de proteção ao crédito (Serasa e SPC), utilizado no comércio, indústria e setor de serviços.

Há capítulo próprio sobre o tratamento de dados sensíveis, em seu art. 11. A título de exemplo, neste aspecto, há a previsão da seguinte regra legal, no art. 11, §3º:

> A comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto

> de vedação ou regulamentação por parte de autoridade nacional, ouvidos os órgãos setoriais do Poder Público, no âmbito de suas competências (Brasil, 2018).

Este dispositivo legal pode ser aplicado, por exemplo, pela Agência Nacional de Saúde Suplementar (ANS), para restringir o compartilhamento de dados pessoais sensíveis, tais como a utilização de dados pessoais, em prontuários médicos e históricos clínicos que poderiam ser utilizados por planos de saúde, para verificar doenças pré-existentes.

Com relação ao tratamento de dados pessoais de crianças e adolescentes, somente poderá ocorrer com o consentimento específico por um dos pais ou responsável legal, conforme dispõe o art. 14, §1º: “O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal” (Brasil, 2018). A título de exemplo, o acesso de crianças e adolescentes à plataforma do *YouTube* dependerá da concordância de genitores ou do responsável legal.

Acerca do tratamento de dados pessoais pelo poder público, devem ser respeitados os princípios de proteção de dados, elencados no art. 6º dessa supracitada lei, pois o uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, bem como o princípio da boa-fé.

Ainda sobre o tratamento dos dados pessoais pelo Poder Público, cumpre ressaltar que eles devem ser usados de forma lícita, e, que nem mesmo o CNJ escapou dos *hackers* (Bonfim, 2024).

Conforme dispõe o art. 23 em seus parágrafos 4 e 5:

> § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei. § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo (Brasil, 2018).

Então, o tratamento de dados pessoais pelo serviço notarial de registro deve seguir as normas aplicáveis ao setor público. Há, inclusive, a previsão de que estes serviços notariais e de registros devem fornecer o acesso aos dados para a Administração Pública, por meio eletrônico.

Empresas públicas e sociedade de economia mista que atuem em regime de concorrência devem seguir as regras aplicáveis às pessoas jurídicas de direito privado.

Há, ainda, disposições legais sobre a responsabilidade e do ressarcimento de danos causados por controladores e/ou operadores de tratamento de dados pessoais. Neste artigo, existem regras acerca da responsabilidade solidária entre o controlador e operador pelos danos causados ao titular do dado pessoal e as hipóteses de isenção da responsabilidade legal dos agentes de tratamento de dados pessoais, conforme art. 42, em seu parágrafo primeiro, incisos I e II:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo. § 1º A fim de assegurar a efetiva indenização ao titular dos dados: I – o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei; II – os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei (Brasil, 2018).

Vale destacar o fato de a lei prever o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (art. 58 e 69), ademais, a Lei n.º 13.709/18 altera o Marco Civil da Internet, em dois tópicos. Por uma órbita, é previsto legalmente à exclusão em definitivo dos dados pessoais, proporcionado pelos que utilizam a determinada aplicação de Internet, no fim da relação entre as partes, com exceção para as hipóteses de guarda obrigatória de registros previstos na lei.

Por outro ângulo, existe o direito à exclusão definitiva de dados pessoais que sejam demasiados no tocante à finalidade do consentimento dado pelo seu respectivo titular, resguardando as hipóteses legais.

3.4 A PRIVACIDADE

A proteção ao direito à privacidade, por um longo período, foi associada à ideia de isolamento, refúgio ou segredo. Hoje em dia, abarca diversos direitos, como a igualdade, liberdade de escolha, não discriminação, entre outras.

A honra, a intimidade e a própria imagem foram consideradas pela teoria jurídica tradicional como manifestações dos direitos da personalidade. Atualmente, ao se estabelecer um sistema de direitos fundamentais, são classificados como expressão do valor da dignidade humana.

A revolução burguesa, historicamente, inicia o processo de positivação dos direitos naturais, na forma de direitos subjetivos, através dos quais o objetivo é a elaboração de um instrumento técnico para a proteção dos interesses patrimoniais de particulares e, em especial, da propriedade.

De acordo com Rodotà (2008, p. 26), com a desagregação da sociedade feudal e a emergência da classe burguesa, seu fascínio pela individualidade é potencializado. O burguês apropria-se dos espaços, levantando novas barreiras, buscando a proteção de um local apenas seu, revelando uma nova necessidade de intimidade.

No período medieval, a separação das esferas da vida era privilégio das mais altas esferas da nobreza ou de quem por livre escolha ou necessidade renunciava à vida em comunidade. A necessidade do isolamento vai aparecendo e crescendo ao ponto em que as condições sociais e econômicas conduzem ao desenvolvimento dos núcleos urbanos, aparecendo, assim, novas formas de divisão do trabalho que marcam a diferença entre o lugar em que se vive e o lugar no qual se trabalha.

A intimidade configura-se, desse modo, como uma aspiração da burguesia de lograr o que antes era privilégio de poucos. “*My home is my castle*”, a máxima inglesa, expressa claramente o ideal burguês, potencializado pelas novas condições de vida. O antigo castelo da nobreza é, ao tempo, a casa do homem burguês, revestido pelas prerrogativas dos direitos da personalidade. Da ideia de propriedade como instrumento de proteção nasce a intimidade, e essa distinção ultrapassa o limite dos conceitos jurídicos formais, pois a partir de então, a propriedade aparece como condição para se alcançar a intimidade.

Nas palavras de Cancelier (2017), além das dimensões política e econômica, a mudança de percepção de público e privado é interna, manifestando-se como forma de expressão da personalidade. Há uma emancipação do sujeito face a sociedade. Contrapõe-se privado x público, ganha força a oposição entre o social e o íntimo. Portanto, a privacidade surge na relação entre indivíduo e sociedade (Doneda, 2020, p. 127).

O direito subjetivo surge, em suas primeiras manifestações, como um poder de domínio sobre as coisas. A construção de um direito unitário da personalidade encontrou reservas na doutrina, com teses abertamente críticas.

Elas insistem na necessidade de não estender a proteção da personalidade a uma pluralidade de objetos ou bens precisos, o que ampliaria muito o leque de situações tuteladas, dando-lhes rotulações abstratas e genéricas. Mas, ao final, admite-se a proposta de direito plural da personalidade, específico para cada uma de suas manifestações objeto de individualizada proteção jurídica.

Importante, é entender que esses direitos, ao surgirem, foram revestidos pelo pensamento burguês. Ou seja, a forma encontrada para protegê-los era os considerar objeto da propriedade privada, estendendo a eles a tutela externa do direito de propriedade.

No cerne do pensamento anglo-saxão, o conceito de privacidade teve seu pressuposto teórico na ideia de liberdade como autonomia individual, defendida por John Stuart Mill em seu trabalho "*On liberty*", de 1859, no qual defende que sobre si mesmo, sobre seu corpo e sua mente, o indivíduo é soberano.

De acordo com Zanon (2013, p. 40), o direito à privacidade como figura jurídica é recente que tem reconhecido seu marco inicial, geralmente, no trabalho realizado por Warren e Brandeis, tratado mais adiante. Porém, o autor ressalta que antes de Warren e Bradeis, havia traços daquilo que seria definido, futuramente, como o direito à privacidade. Zanon ressalta que foi Thomas McIntyre Cooley (1824-1898), jurista norte-americano e Presidente da Suprema Corte de Michigan, quem cunhou, em 18887, a expressão o direito de estar só (*the right to be let alone*).

Mas o marco para o estabelecimento desse direito foi, sem dúvidas, o artigo publicado na Harvard Law Review por D. Warren e Louis D. Brandies, em 1890, *"The Right to Privacy*". Nele, os autores enfatizam que a configuração desse instituto consiste no direito à solidão, ou na faculdade *"to be alone*", ou seja, como a garantia do indivíduo à proteção do sagrado recinto da sua vida privada e doméstica perante qualquer invasão.

A primeira manifestação do interesse individual de "ser deixado só" ocorreu no caso Wheaton v. Peters, decidido pela Suprema Corte no ano de 1834, mas com caráter marcadamente individualista, passando pela propriedade privada, mas sem se voltar à inviolabilidade da personalidade (Zanini, 2017).

Os autores apresentam no artigo limitações ao privacy, e.g., a permissão de publicação de material de interesse geral e público, a possibilidade de publicação de fatos danosos quando o indivíduo consente, bem como a inexistência de defesa quando se alega que o fato é verdadeiro ou então que não houve “malícia” na publicação (Soma, 2008, p. 14).

Para fundamentar o *privacy*, os autores recorreram ao direito à vida, expressamente enunciado na declaração de independência dos Estados Unidos e formalmente reconhecido pela Quinta Emenda à Constituição. Acrescentaram ainda que, apesar da Constituição estadunidense não mencionar a palavra *privacy*, seus princípios já faziam parte da *Common Law*, ante a proteção do domicílio, tendo o desenvolvimento tecnológico apenas tornado necessário reconhecer expressa e separadamente essa proteção sob o nome de *privacy* (Soma, 2008, p. 13-14).

Nessa linha, o direito em questão garantiria ao indivíduo uma ampla liberdade contra intromissões não desejadas em sua vida, tutelando seus pensamentos, sentimentos, emoções, dados pessoais e até mesmo o nome.

Desde 1890, já se preocupava como a tecnologia afetaria direitos da personalidade ligadas à privacidade. A imagem também foi incluída no âmbito de proteção do *privacy*, destacando-se que os avanços da fotografia tornaram possível a captação de forma oculta dos traços pessoais, pelo que se fazia necessária a utilização da *Tort Law* diante dos riscos inerentes ao progresso técnico (Warren; Brandeis, 1890, p. 211).

Contudo, o período que vai do início do século XX até a sua metade não apresentou evolução aparente da doutrina do *privacy*, registrando apenas decisões que confirmaram a concepção desenvolvida por Warren e Brandeis. Perdeu-se então a oportunidade de incluir os avanços tecnológicos do período na proteção.

Nas palavras de Cancelier (2017), nascido em berço burguês, o direito à privacidade, de maneira geral, permaneceu restrito às suas origens até o final da primeira metade do século XX. Conforme Doneda (2020, p. 12), esse contexto muda “no decorrer da década de 1960 motivado, sobretudo, pelo crescimento da circulação de informações, consequência do desenvolvimento exponencial da tecnologia de coleta e sensoriamento, resultando em uma “capacidade técnica cada vez maior de recolher, processar e utilizar a informação”.

Em 1977, a Suprema Corte estadunidense extraiu do *right of privacy* a existência de um *right of publicity*. O referido direito foi considerado independente do

privacy e garantiria um privilégio exclusivo à pessoa quanto ao aproveitamento econômico de sua notoriedade, o que poderia ser considerado um *property right*, na medida em que teria valor pecuniário (Rigaux, 1990, p. 393-396).

Assim, o *right of publicity* pode ser concebido, em linhas gerais, como o direito que cada pessoa tem de controlar o uso comercial de sua identidade, nela incluída a imagem, o nome ou a voz, bem como objetos materiais dirigindo sua tutela para aspectos meramente patrimoniais. O instituto é visto como uma espécie do gênero da concorrência desleal, já que garante o privilégio exclusivo quanto à exploração da identidade. Nota-se que desde muito já se reconhecia um valor econômico aos dados pessoais/personalidade.

O conceito de *right of privacy* se difundiu para os países que adotam o sistema da Common Law. Esses países, entretanto, apresentam um grau bastante variado de proteção da personalidade humana, e.g., no Direito Inglês não haveria uma espécie de proteção geral, mas apenas uma tutela indireta, relacionada com elementos constitutivos de determinados delitos (Lévy, 2002).

No plano da legislação internacional, a proteção à privacidade surgiu em 1948, através em primeiro lugar da Declaração Americana dos Direitos e Deveres do Homem aprovada pela XI Conferência Internacional em Bogotá. A referida Declaração mencionava em seu art. 5º que “toda pessoa tem direito à proteção da lei contra os ataques abusivos a sua honra, a sua reputação e a sua vida privada e familiar”.

No mesmo ano foi aprovada pela Assembleia Geral das Nações Unidas a Declaração Universal de Direitos do Homem, que enunciava em seu art. 12 que “ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação.

Em 1966, surge o Pacto Internacional de Direitos Civis e Políticos, em que declarava:

> Art. 14 – Todas as pessoas são iguais perante os tribunais e as cortes de justiça. Toda pessoa terá o direito de ser ouvida publicamente e com as devidas garantias por um tribunal competente, independente e imparcial, estabelecido por lei, na apuração de qualquer acusação de caráter penal formulada contra ela ou na determinação de seus direitos e obrigações de caráter civil. A imprensa e o público poderão ser excluídos de parte ou de totalidade de um julgamento, quer por motivo de moral pública, de ordem pública ou de segurança nacional em uma sociedade democrática, quer quando o interesse da vida privada das Partes o exija, em circunstâncias específicas, nas quais a publicidade venha a prejudicar os interesses da justiça; entretanto, qualquer sentença proferida em matéria penal ou civil deverá tornar-se pública, a menos que o interesse de menores exija o

> procedimento oposto ou o processo diga respeito a controvérsias matrimoniais ou à tutela de menores (ONU, 1966).

Ainda, no que diz respeito à proteção da vida privada, estabelece o art. 17 que:

> Art. 17 – Ninguém poderá ser objeto de ingerências arbitrárias ou legais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra e reputação. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas (ONU, 1966).

A proteção de dados no Brasil antes da vigência do Marco Civil da Internet e da LGPD já era realizada com base na CFRB/88, a qual previu, expressamente, a liberdade, a intimidade e a privacidade como direitos fundamentais.

A intimidade e a privacidade são expressões dos direitos da personalidade. Nas palavras de Doneda (2020, p. 41-42):

> A proteção da privacidade identifica-se e acompanha a consolidação da própria teoria dos direitos da personalidade [...] serve a proporcionar ao indivíduo os meios necessários à construção e consolidação de uma esfera privada própria, dentro de um paradigma de vida em relação e sob o signo da solidariedade – isto é, de forma que a tutela da privacidade cumpra um papel positivo para o potencial de comunicação e relacionamentos do indivíduo.

A inserção da dignidade como princípio constitucional fundamental, contida em preceito introdutório do capítulo dos direitos fundamentais, significa, afinal, adoção mesmo de um direito geral de personalidade, cujo conteúdo é justamente a prerrogativa do ser humano de desenvolver a integralidade de sua personalidade, todos os seus desdobramentos e projeções, nada mais senão a garantia dessa sua própria dignidade

Consoante o escólio doutrinário de Silvio Romero Beltrão (2014, p. 23), “os direitos da personalidade designam direitos privados fundamentais, os quais devem ser respeitados como o conteúdo mínimo para a existência da pessoa humana, impondo limites à atuação do Estado e dos demais particulares”. Para Orlando Gomes (2016), são direitos essenciais ao desenvolvimento da pessoa humana, que a doutrina moderna preconiza e disciplina, no corpo do Código Civil, como direitos absolutos. Destinam-se a resguardar a eminente dignidade da pessoa humana, preservando-a dos atentados que pode sofrer por parte de outros indivíduos.

Segundo Ramos (2008), no ordenamento jurídico do Brasil, embora houvesse previsões sobre a proteção aos direitos fundamentais em Constituições anteriores,

que incidiam indiretamente na privacidade, tais como a inviolabilidade de domicílio, sigilo das correspondências e das comunicações, somente a partir da Constituição Federal de 1988 passou a existir expressa referência à vida privada e à intimidade. A proteção constitucional é deferida não apenas em face do Estado, mas igualmente dos demais particulares.

A privacidade concebida em seu sentido lato ainda pode ser entendida como:

> O conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito. Embarca todas as manifestações das esferas íntimas, privadas e da personalidade, que o texto constitucional consagrou. A esfera de inviolabilidade, assim, é ampla, abrange o modo de vida doméstico, nas relações familiares e afetivas em geral, fatos, 23 hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo (Ramos, 2008, p. 13).

Diante de tais considerações, verifica-se que a privacidade à luz da CRFB é o conjunto de modo de ser e viver, como direito de o indivíduo viver sua própria vida. Consiste ainda na faculdade que cada indivíduo tem de obstar à intromissão de estranhos na sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um e que sejam divulgadas informações sobre esta área de manifestação existencial do ser humano.

De acordo com Cancelier (2017), no Brasil, tanto o constituinte quanto o legislador ordinário, ao elaborarem a Constituição 1988 e o Código Civil de 2002 (Lei n.º 10.406) optaram por não fazer uso do termo privacidade, mas das expressões vida privada e intimidade, sem oferecer conceitos a nenhuma delas. A CRFB/88 fala, ainda, em sigilo (de correspondência, das comunicações telegráficas, de dados e das comunicações telefônicas) e na inviolabilidade da casa.

Segundo o mesmo autor:

> Qualquer um dos termos para referenciar a mesma situação. Por exemplo, fala-se em vida privada ou vida íntima para tratar do mesmo espaço da vida sobre a qual se fala. Algo secreto, sigiloso ou íntimo pode ser relacionado ao mesmo aspecto que se deseja manter em segredo. O privado pode ser íntimo, o íntimo pode ser secreto, o secreto pode ser privado. Ao mesmo tempo, cada um deles poderá assumir – de forma bastante subjetiva – a depender do sujeito da fala, um significado específico. Assim, nem sempre o íntimo será secreto ou o assunto sigiloso será privado. O que se quer dizer é que o significado do discurso irá variar conforme quem o profere, possibilitando cada um dos termos aqui apresentados usos variados. Juridicamente, a mesma possibilidade é aventada. Privacidade, então, deve ser vista antes de tudo como exercício de uma liberdade da pessoa, uma necessidade humana. Parte-se para uma visão da privacidade que é interna ao sujeito, faz parte dele, formando-o como ser humano. Seja trabalhando a

> privacidade como o estar só14 ou numa perspectiva mais contemporânea de controle informacional, não se pode perder o vínculo com a pessoa, como forma de manifestação da personalidade (Cancelier, 2017).

Frise-se que direito à intimidade e à vida privada não se trata de direitos semelhantes, mas direitos que apresentam peculiaridades. Isto pode ser constatado no art. 5º, X, que distintamente refere-se à intimidade, vida privada, honra e imagem. A privacidade é o conjunto de 'informações' que cada indivíduo tem como suas, e a intimidade é a esfera secreta da vida do indivíduo, o direito a estar só, sem interferência dos outros.

Assim, a LGPD, ao proteger a intimidade, visa assegurar uma parcela da personalidade reservada da indiscrição alheia para satisfazer exigências de isolamento moral do sujeito.

Como ressalta Cancelier (2017), não se pode resumir a tutela da privacidade a uma liberdade puramente negativa, sob pena de ignorar os avanços tecnológicos que modificaram as formas de expressão da privacidade. Entende-se que embora o instituto da responsabilidade civil deva ser utilizado como instrumento remedial típico à tutela dos direitos da personalidade, faltam a ele "[...] os instrumentos adequados à realização da função promocional da tutela da privacidade como meio de proteção da pessoa humana e da atuação da cláusula geral da proteção da personalidade" (Schreiber, 2013, p. 134).

Contudo, a LGPD surge para demonstrar que o dano à privacidade não se resolve com indenização. A intimidade e a privacidade estão relacionadas à liberdade na LGPD não por acaso. A efetivação da privacidade pela proteção dos dados pessoais é expressão do direito à liberdade.

A CRFB demonstra que a liberdade é parte essencial da ordem jurídica brasileira ao dar-lhe caracterização de direito fundamental e cláusula pétrea, além de procurar positivá-la nas mais variadas formas: liberdade de locomoção (art. 5º, XV, CF), liberdade de reunião (art. 5º, XVI, CF), liberdade de expressão (art. 5º, IX), liberdade de pensamento (art. 5º, IV, CF). O próprio preâmbulo da constituição afirma que o Brasil é um Estado Democrático destinado a assegurar a liberdade.

Nos termos doa art. 17 da LGPD, "Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei".

No caso da LGPD, trata-se de uma liberdade negativa, a ser exercida pelo próprio cidadão, qual seja, a liberdade de fornecer ou não os próprios dados pessoais, além de garantir a efetividade desta liberdade. Desse modo, a proteção de dados é um processo mais complexo, que envolve a própria participação do indivíduo na sociedade e considera o contexto no qual lhe é solicitado que revele seus dados, estabelecendo meios de proteção para as ocasiões em que sua liberdade de decidir livremente é cerceada por eventuais condicionantes – proporcionando o efetivo exercício da autodeterminação informativa.

Neste sentido, a proteção dos dados pessoais tem caráter complexo. Isso significa que a tutela da privacidade se presta a proteger um plexo de interesses comum (sentido negativo), busca-se atribuir à pessoa maior poder para controlar os dados que lhe dizem respeito – principalmente aqueles sobre as convicções políticas e filosóficas, credo religioso, vida sexual, estado de saúde, entre outros – a fim de que suas liberdades não sejam tolhidas pelo fomento ao conformismo e pela discriminação social (sentido positivo).

3.4.1 Do Conceito (ou da Ausência de um Conceito) de Privacidade

Definir o conceito de privacidade não é uma tarefa das mais fáceis. A carga emotiva que leva consigo, as noções de intimidade e vida privada as fazem confusas e ambíguas e dificulta a precisão de seu significado. Privacidade, se olhada por um lado, pode ser enquadrada em quase tudo, como também pode ser quase nada (Solove, 1996).

Representa uma poderosa batalha retórica sediada numa gama de conceitos relacionados. Como a palavra liberdade, a privacidade pode significar diferentes conjuntos de fatores para pessoas distintas. Quando as pessoas clamam que sua privacidade deve ser protegida, não fica claro o que exatamente elas estão demandando. Essa falta de clareza na definição de seu conceito cria uma dificuldade quando se tenta desenvolver políticas ou procurar soluções para problemas concretos, tornando a vida de legisladores e juízes um pouco mais complicada na articulação desses conceitos e na definição do que é ou não uma invasão de privacidade.

Dificuldade essa que se amplia ao se defrontar com os desafios e os impactos trazidos pelas novas tecnologias para o âmbito da privacidade. Primeiramente, é

necessário que se faça uma breve distinção entre privacidade e intimidade. Aquela é mais ampla que esta, pois a intimidade protege a esfera em que se desenvolvem as facetas mais reservadas da vida de uma pessoa. Já a primeira constitui um conjunto mais amplo, mais global, de facetas da personalidade humana, que, isoladamente, podem carecer de um significado intrínseco, mas, quando coerentemente interrelacionadas, retratam um rasgo da personalidade do indivíduo, que tem o direito de a manter reservada (Sánchez-Bravo, 1996).

Antes de avançar, convém lembrar a necessidade de se estabelecer fronteiras e terminologias. Uma teoria completa sobre a privacidade tem que levar em conta, mesmo com restrições teóricas, dimensões vastas, incorporando experiências sobre a informação circundante, as atividades cotidianas do homem, as decisões, os pensamentos e a comunicação. Dimensões que ganham extensão ao se considerarem as transformações tecnológicas que incluem uma rede de informações ampliada, a "*world wide web*", os dispositivos móveis, os avanços nas áreas de vídeo, áudio, a biotecnologia, os GPS's, a robótica, as bases de dados de informações compiladas e a evolução dos sensores e das redes sociais.

Para alguns autores, o fato de haver uma confusão sobre o conceito de privacidade cresce a partir da falha em reconhecer a diferença entre uma concepção neutra e uma concepção normativa. A primeira busca um estado para a privacidade sem fazer nenhum tipo de juízo de valor (se ela é uma coisa boa), ou seja, que necessita de uma proteção moral ou legal. A concepção normativa toma parte nesse debate, assumindo que a privacidade é essencial e merece a proteção devida.

Uma teoria plausível sobre a privacidade, dotada de legitimidade moral, deverá basear-se em princípios para estabelecer seu ponto de partida e seus limites. Esses princípios devem emergir de valores que integrem sua concepção, compondo uma importante associação entre privacidade e os valores sociais nela envolvidos. O bem-estar, o desenvolvimento, a criatividade, a autonomia, a saúde mental e a liberdade são aspectos que compõem diretamente ou bordeiam o conceito de privacidade.

Dentre eles, a liberdade configura-se como um valor fundamental e intrinsecamente ligado. Vale lembrar que a privacidade tem relação direta com um grupo de direitos humanos como a liberdade de expressão e direito à informação, deles indissociáveis.

Neste sentido, deve-se resguardar a personalidade da pessoa que é afetada por um constrangimento pessoal decorrente do próprio comportamento em público. Numa sociedade em que qualquer movimento público pode virar motivo de chacota, ações chulas e constrangedoras, a garantia de preservação da imagem é fundamental para a saúde mental e para o desenvolvimento da personalidade do cidadão.

Essa relação entre privacidade e liberdade pode até certo ponto ser questionada, pois se pode argumentar que a privacidade não facilitaria a liberdade, mas, sim, seria uma forma de esconder comportamentos reprováveis socialmente, já que somente com algo a esconder é que se pode temer represálias. Entretanto, a questão não é vista por esta ótica, mas como uma proteção moral à timidez, fato de grande importância para fortalecimento da personalidade.

A privacidade não somente resguarda o cidadão, mas, ao fazê-lo, também abre a possibilidade, junto a outros direitos, de as pessoas assumirem suas escolhas, promovendo a tolerância e o respeito às diferenças. Vale ressaltar o posicionamento de Jeroen van den Hoven (2004), o qual lança mão de quatro razões pelas quais a privacidade merece proteção: 1 – dano informacional; 2 – desigualdade informacional; 3 – injustiça informacional; 4 – usurpação da autonomia moral.

Por dano informacional, entende-se uma proteção à coleta irrestrita de informação, tal como nome, vínculos parentais, números de identificação e passaporte, que habilitará construções de identidades fraudulentas, através de crimes conhecidos como roubo de identidade.

A desigualdade informacional refere-se a constrangimento no fluxo das informações, em que uma das partes esteja sendo prejudicada, por exemplo, os mercados paralelos de venda de informações por parte dos governos e empresas privadas, prejudicando consumidores e clientes.

A terceira razão aloca-se nas esferas envolvidas no fluxo da informação, ou seja, uma informação que pertence a uma esfera (saúde, por exemplo) não deve invadir outra indevidamente. Por fim, a usurpação da autonomia moral retoma o que fora debatido acima, pois resguardando a privacidade aumenta-se a disparidade da relação entre o que o indivíduo deseja ser para o que é, diminuindo o risco de perda de parte de sua personalidade devido a pressões externas (Hoven, 2004).

4 CIDADES INTELIGENTES E A LGPD

4.1 CONCEITO DE CIDADE INTELIGENTE

A ideia de cidades inteligentes promovidas pela TIC é endossada por autoridades nacionais e municipais, grandes corporações globais de tecnologia e instituições e organizações internacionais como a Comissão Europeia (2020), OCDE (2020) e ISO (2015).

De acordo com Kitchin (2015), o conceito de cidades inteligentes se apresenta como a solução para o enigma fundamental das cidades: reduzir custos e criar crescimento econômico, ao mesmo tempo que produz sustentabilidade, participação, um padrão aceitável de serviços cívicos e qualidade de vida. Nada obstante, o autor ressalta que esta não é a única finalidade de uma "cidade inteligente", pois, na concepção neoliberal, liderada pelo mercado e tecnocrática, se visa puramente o ganho econômico.

Não se pode falar sobre um consenso na definição do que é uma cidade inteligente, pois cada lugar tem suas próprias características industriais, políticas, sociais e cívicas. Assim, é mais correto traçar suas características comuns:

a) redes de sensores conectados a objetos do mundo real, como estradas, carros, geladeiras, medidores de eletricidade, eletrodomésticos e implantes médicos humanos que conectam esses objetos a redes digitais (IoT, "computação ubíqua"), que, por sua vez, geram dados em grandes quantidades ("*Big Data*");
b) redes de comunicações digitais que permitem fluxos de dados em tempo real que podem ser combinados entre si e, em seguida, selecionados e reaproveitados para obter resultados úteis;
c) infraestrutura de alta capacidade, geralmente baseada em nuvem, que pode oferecer suporte e fornecer armazenamento para essa interconexão de dados, aplicativos, coisas e pessoas.

Segundo Dal Magro e Fortes (2021), o conceito de *smart city* gera divergências e convergências na literatura. Certo é que, no âmbito da convergência, a literatura é uníssona em estabelecer um núcleo ao conceito como o uso de tecnologia no contexto do crescimento da economia de conhecimento.

As tecnologias disruptivas, i.e., as inovações que vêm para substituir um processo, um produto ou uma tecnologia já estabelecida, criando uma nova maneira de operar, seja para consumidores, organizações, ou ambos, também são partes integrantes da ideia de cidade inteligente.

Do ponto de vista conceitual, definimos as cidades inteligentes enquanto comunidades urbanas que utilizam tecnologias avançadas e a conectividade para melhorar a qualidade de vida dos cidadãos, impulsionar a eficiência operacional e promover a sustentabilidade. Elas têm como características a incorporação de soluções inovadoras, como a Internet das Coisas (em inglês, *Internet of Things* – IoT), análise de dados, inteligência artificial e outras tecnologias emergentes para coletar informações, otimizar processos e fornecer serviços eficientes.

O objetivo de uma cidade inteligente é criar um ambiente urbano mais seguro, sustentável, eficiente e inclusivo, onde os recursos sejam utilizados de forma inteligente e os cidadãos tenham acesso a serviços de alta qualidade, abrangendo setores como transporte, energia, segurança, governança e infraestrutura. É o que Alexandre Freire Pimentel (2023) designa como cidadania digital um fenômeno social, típico da era tecnológico-reticular, representado por uma situação jurídica atrelada a uma política pública inclusivista de promoção de acesso pleno à Internet sem qualquer tipo de dificuldade, barreira impeditiva ou discriminatória.

A cidadania digital seria a base do “estado algorítmico de direito”, expressão cunhada por Moisés Barrio Andrés, professor de Direito Digital na Universidade Carlos III de Madri, para quem o termo expressa uma visão positiva sobre os impactos da tecnologia no direito e na vida social, pelo que o estado algorítmico, para ser “de direito” deve adotar “[…] ferramentas automatizadas apenas quando melhoram, em vez de minar, os fundamentos da legitimidade dos estados democráticos” (Barrio Andrés, 2020, p. 1).

Os pilares das cidades inteligentes são a conectividade; infraestrutura de redes e comunicações; governança: envolvimento dos cidadãos e uso de dados para tomada de decisões; mobilidade: transporte público inteligente, compartilhado e sustentável; e sustentabilidade: eficiência energética, gestão de resíduos e uso de energias renováveis. Como exemplos, podem ser citados o Gerenciamento de Tráfego: semáforos inteligentes, estacionamento inteligente, rotas otimizadas; Gestão de Resíduos: coleta seletiva inteligente, sensores para otimizar a coleta; Segurança Pública: monitoramento por câmeras, detecção de incidentes em tempo real;

Eficiência Energética: medidores inteligentes, iluminação pública controlada por sensores.

Dentre os recursos tecnológicos aplicáveis está a Internet das Coisas: conexão de dispositivos e sensores a sistemas, permitindo a coleta e troca de informações em tempo real. Cria uma rede inteligente, onde diferentes elementos da cidade podem interagir e se adaptar às necessidades dos cidadãos. Ex.: sensores de umidade do solo e de luz solar em jardins verticais e hortas urbanas para monitorar e otimizar a irrigação e a iluminação necessárias para o cultivo; Inteligência artificial: capacidade de dispositivos eletrônicos de funcionar de maneira que lembra o pensamento humano, percebendo variáveis, tomando decisões e resolvendo problemas de maneira autônoma e aprendendo por si mesmas, graças ao processamento de um grande volume de dados.

De acordo com Ehrhardt Júnior, França Netto e Malheiros (2022, p. 1276), a inteligência artificial é “o estudo do design de agentes e sistemas inteligentes, capazes de reproduzir, digitalmente, uma estrutura de decisão semelhante à humana”. Ex.: monitorar a quantidade de lixo em diferentes áreas da cidade e ajudar os caminhões de coleta de lixo a otimizar suas rotas; identificação de vazamento de água através de sistemas de áudio nas tubulações.

- Análise de dados: aplicação de técnicas estatísticas e algoritmos avançados para identificar correlações, padrões ocultos e insights relevantes. Ex.: Previsão de demanda de transporte: Utilizando dados históricos de tráfego e informações demográficas;
- Computação em nuvem: modelo de entrega de serviços de computação, como armazenamento, processamento de dados e aplicativos, através da Internet, em vez de utilizar recursos locais, como servidores físicos ou infraestrutura local. Ex.: Plataformas de Gerenciamento de Dados Urbanos: a computação em nuvem fornece uma plataforma escalável e flexível para armazenar, processar e analisar a infinidade de dados produzidos pelas cidades inteligentes, permitindo que as autoridades urbanas tomem decisões informadas e baseadas em dados;
- Acesso Remoto e Colaboração: acesso remoto aos dados e aplicativos o que facilita a colaboração entre diferentes partes interessadas, como autoridades, empresas, pesquisadores e cidadãos, permitindo uma

participação mais ampla e eficaz na gestão e no desenvolvimento da cidade;

- Conectividade de alta velocidade: fibra óptica, redes 5G, Wi-Fi de alta capacidade e LoRaWAN (rede de longo alcance e baixo consumo de energia), fornecem velocidades de transmissão rápidas, baixa latência e alta capacidade de rede para atender às demandas crescentes de dados das cidades inteligentes. Ex.: LoRaWAN permite a comunicação em áreas amplas, cobrindo distâncias de vários km em áreas urbanas e até dezenas de quilômetros em áreas rurais, sistema de vagas de estacionamento na cidade, onde sensores instalados nas vagas de estacionamento detectam a presença de veículos.

De acordo com o Smith (2015), Barcelona está no topo da lista de “cidades inteligentes”, devido ao uso abrangente de novas tecnologias, incluindo um sistema de semáforo inteligente que coloca as luzes em verde até que os carros de bombeiros passem, aparelhos instalados na residência do indivíduo e conectados por meio de linha telefônica (fixa ou móvel) a um *Call Center*, que pode ser contatado com o simples toque de um botão, entre outras inovações. lista das cinco cidades mais inteligentes é completada por Nova York, Londres, Nice e Cingapura.

Atualmente, “inteligência” tornou-se um índice competitivo entre as cidades por atenção, financiamento e investimento interno. Trata-se de um fenômeno global social, econômico, político e tecnológico.

As cidades inteligentes não são, portanto, apenas uma questão de produzir cidades menos poluídas ou mais eficientes, mas geram capital político considerável e grandes oportunidades de negócios, juntamente com um grande mercado de exportação potencial.

Nos países em desenvolvimento, as cidades inteligentes são marcadas pela desigualdade social, pois a iniciativa é cercada de privilégios, haja vista que as pessoas pobres são privadas de acesso à grande parte de recursos tecnológicos. Além disso, a implementação desses recursos tende a ser por Parceria Público-Privada (PPP), que assim é definida, conforme art. 2º da Lei n.º 11.079/2004:

> Art. 2º Parceria público-privada é o contrato administrativo de concessão, na modalidade patrocinada ou administrativa. § 1º Concessão patrocinada é a concessão de serviços públicos ou de obras públicas de que trata a Lei nº 8.987, de 13 de fevereiro de 1995, quando envolver, adicionalmente à tarifa cobrada dos usuários contraprestação pecuniária do parceiro público ao parceiro privado. § 2º Concessão administrativa é o contrato de prestação de

> serviços de que a Administração Pública seja a usuária direta ou indireta, ainda que envolva execução de obra ou fornecimento e instalação de bens. § 3º Não constitui parceria público-privada a concessão comum, assim entendida a concessão de serviços públicos ou de obras públicas de que trata a Lei nº 8.987, de 13 de fevereiro de 1995, quando não envolver contraprestação pecuniária do parceiro público ao parceiro privado (Brasil, 2004).

Um exemplo alardeado de financiamento de PPP é o Centro de Operações de Inteligência no Rio de Janeiro, que foi construído pela IBM em preparação para a Copa do Mundo de 2014 e os Jogos Olímpicos de 2016.

O Rio foi considerado um dos as cidades mais perigosas do mundo e sentiu-se a necessidade de, de alguma forma, tranquilizar o afluxo de visitantes globais esperado para as Olimpíadas e a Copa do Mundo. Centenas de câmeras e incontáveis outros sensores e dispositivos colocados por toda a cidade transmitem dados ao vivo em uma parede de vídeo gigante do Centro de Monitoramento 24 horas, permitindo que os operadores da cidade sejam mais rapidamente responsivos a tempestades, crimes, acidentes, quedas de energia, e outras ocorrências (Hojda; Martins; Fariniuk, 2020).

O sistema municipal do Centro, integrando dados de cerca de 30 agências, é um olho que tudo vê que pode reunir, analisar e agir com precisão nas informações sobre os sistemas e serviços da cidade e reconhece o comportamento da cidade como um todo (Ribeiro, 2017).

O caso do Rio levanta claramente a questão de quem (se é que alguém) possui os dados que as cidades inteligentes produzem e processam em tão grandes quantidades. Policiamento, vigilância, controle de multidões, resposta a emergências são funções historicamente estatais, e os cidadãos podem esperar que os dados muito confidenciais envolvidos sejam mantidos pelo estado. No entanto, a probabilidade em uma cidade construída com PPP é que os dados se encontrem (pelo menos parcialmente ou não exclusivamente) sob controle privado.

A falta de padrões universais abertos para a troca de dados é outra questão importante que direciona os dados para silos privados. Os dados abertos são frequentemente mencionados como uma questão fundamental para o envolvimento dos cidadãos em cidades inteligentes, e.g., o repositório de dados do Rio é aberto ao público com conjuntos de dados importantes.

Mas, na pior das hipóteses, uma cidade inteligente pode se tornar o feudo de dados privado de um monopólio de tecnologia ou telecomunicações (Ribeiro, 2017).

Essas questões fazem parte das preocupações e incertezas contínuas sobre quem é o proprietário e como controlar “*Big Data*”.

Diante disso, surgem os seguintes questionamentos: por que discutir privacidade e cidades inteligentes? Por que não privacidade e IoT, ou privacidade e *Big Data*, ou mesmo privacidade e o colapso da demarcação de espaços públicos/privados?

Primeiro, porque as cidades inteligentes representam a síntese de todos esses problemas. Segundo, pois, no futuro, a maioria das pessoas estará vivendo em cidades, e muitos, em cidades “inteligentes” ou, pelo menos, não burras. Terceiro, em razão do aumento de investimento em cidades inteligentes. Quarto, por ser necessária uma literatura que examine as cidades inteligentes e a privacidade em termos do contexto social do Brasil e das regras obrigatórias da legislação brasileira.

De acordo com o Baeck e Saunders (2015), após analisar várias cidades inteligentes, muitas

> falharam em cumprir sua promessa, proporcionando altos custos e baixos retornos [...] oferecem sensores, 'Big Data' e computação avançada como respostas para esses desafios, mas eles muitas vezes enfrentaram críticas por estarem muito preocupados com o hardware e não com as pessoas.

Dentre essas falhas, está a de segurança, i.e., a suscetibilidade dos dados a violações acidentais ou deliberadas como resultado de falhas técnicas ou organizacionais, além do problema da privacidade.

As cidades e suas infraestruturas são os feitos mais complexos já criados pelo ser humano e, entrelaçando-as com soluções de cidades inteligentes igualmente complexas, baseadas em redes de sensores sem fio e sistemas de comunicação integrados, as torna extremamente vulneráveis a falhas de energia, erros de *software* e ataques cibernéticos (Townsend, 2013). Mesmo um simples bug pode ter um grande impacto na infraestrutura urbana (Cerrudo, 2015).

A insegurança e vulnerabilidade dos sistemas de cidades inteligentes é um fenômeno comum e até reconhecido, que ecoa, e, em grande parte, deriva, da falta de segurança e confiabilidade dos IoT em geral. A FTC, em seu relatório de 2015 sobre a IoT, observa os riscos de segurança como sua maior preocupação, tanto em termos de vulnerabilidade dos próprios dispositivos IoT, levando ao seu comprometimento ou falha, e seu uso potencial para espalhar vulnerabilidades através

de redes e outros sistemas. Por exemplo, potencialmente, uma geladeira inteligente conectada à Internet pode ser sequestrada para enviar *spam*.

A FTC já tomou sua primeira ação de fiscalização contra uma implementação de IoT vulnerável: uma empresa que fabrica monitores para bebês conectados à Internet, permitindo que os pais vejam imagens ao vivo de seus bebês à distância, teve seus *feeds* "hackeados" em cerca de 700 casos. Carros conectados (ou "veículos autônomos") são outro caso de uso de IoT em que a vulnerabilidade a hackers externos já foi demonstrada: e.g., a *Wired* relatou em 2016 como o *Jeep Cherokees* poderia ser confiavelmente "sequestrado" por *hackers* externos enquanto na estrada (Greenberg, 2016).

Brown (2015), em um relatório de 2015 para a ITU, observa que "ataques eletrônicos podem levar a ameaças à segurança física", citando possíveis alvos como como marcapassos médicos, bombas de insulina e freios de carro, e observando as possibilidades dos ladrões de identificarem instalações com "medidores inteligentes" como atualmente desocupadas.

Dispositivos IoT sendo, geralmente, pequenos, muito baratos, sem fonte de alimentação independente e produzidos aos milhões são rotineiramente projetados com força de criptografia pobre e falta de outros recursos de segurança (Akamai, 2014). A IoT depende fortemente de protocolos de comunicação sem fio ou APIs que, devido à falta de padrões técnicos e de segurança obrigatórios, são geralmente "protegidos apenas em uma reflexão tardia, ou pior, não são protegidos de forma alguma, transmitindo dados sem proteção" (Cerrudo, 2015).

O FTC, em relatório sobre IoT, observa que as empresas que fabricam dispositivos IoT podem não ter experiência em lidar com questões de segurança, que muitas vezes foram concebidos como descartáveis; que a correção de vulnerabilidades pode não ter sido considerada; e que os consumidores em geral têm pouca ou nenhuma ideia sobre a segurança da IoT (Cerrudo, 2015).

Para cidades inteligentes, esses problemas são transmitidos e serão multiplicados pelas complexidades envolvidas em vários fornecedores e sistemas interoperáveis; e os efeitos podem ser muito mais devastadores. Cerrudo (2015) afirma que a maioria das cidades está implementando novas tecnologias com pouco ou nenhum teste de segurança cibernética, o que significa que, e.g., sensores de controle de tráfego podem ser facilmente atacados.

Brown (2015) acrescenta que as vulnerabilidades das Cidades Inteligentes serão particularmente difíceis de abordar devido aos links para sistemas mais antigos dos setores público e privado. Vulnerabilidades em arquiteturas não podem ser corrigidas digitalmente de forma tão simples quanto o *software* convencional. Resumindo, as cidades inteligentes são um desastre de segurança prestes a acontecer.

4.2 QUESTÕES ENTRE AS CIDADES INTELIGENTES E A PROTEÇÃO DE DADOS

A Lei de Amara, formulada pelo futurista Roy Amara, sugere que “tendemos a superestimar o efeito de uma tecnologia no curto prazo e subestimar seu efeito no longo prazo”. Esta observação é particularmente relevante quando aplicada ao conceito de cidades inteligentes, ou *smart cities*. As promessas iniciais de eficiência, sustentabilidade e melhor qualidade de vida, amplamente divulgadas pelos defensores dessas tecnologias, frequentemente obscurecem os riscos subjacentes, especialmente aqueles relacionados à privacidade dos cidadãos.

Nas primeiras fases de implementação, as tecnologias emergentes como a Internet das Coisas, *Big Data* e inteligência artificial são promovidas com um otimismo quase utópico. As cidades inteligentes são retratadas como soluções mágicas para os desafios urbanos modernos, prometendo tudo, desde a redução de congestionamentos de tráfego até a gestão eficiente de resíduos e a melhoria da segurança pública (Mattern, 2017). No entanto, conforme postulado pela Lei de Amara, essa superestimação inicial frequentemente ignora as complexidades e os desafios inerentes à integração dessas tecnologias no tecido urbano (Kitchin, 2016).

À medida que essas tecnologias são implementadas, começam a surgir questões significativas relacionadas à privacidade. Sensores onipresentes, câmeras de vigilância e dispositivos conectados coletam dados em uma escala sem precedentes, permitindo o monitoramento constante das atividades dos cidadãos (Zuboff, 2019). Embora essa coleta de dados seja muitas vezes justificada pela promessa de serviços urbanos mais eficientes, ela também cria um cenário perigoso para a privacidade individual. Os riscos não são imediatamente aparentes, mas com o tempo, o potencial de vigilância em massa e abuso de dados se torna uma preocupação crítica.

Os defensores das *smart cities* frequentemente subestimam os impactos de longo prazo dessas tecnologias sobre a privacidade (Greenfield, 2017). A retórica predominante concentra-se nos benefícios imediatos e tangíveis, como a redução de custos operacionais e a melhoria na prestação de serviços (Taylor; Richter, 2017). No entanto, a análise crítica da Lei de Amara revela uma negligência alarmante quanto aos riscos profundos e persistentes. As tecnologias que são inicialmente celebradas por sua inovação podem, a longo prazo, comprometer a privacidade e a autonomia dos indivíduos.

Por exemplo, a implementação de câmeras de reconhecimento facial em espaços públicos é frequentemente aplaudida por sua capacidade de aumentar a segurança. Contudo, essa tecnologia pode facilmente ser utilizada para vigilância em massa, rastreamento de movimentos e monitoramento de comportamentos, sem o consentimento ou conhecimento adequado dos cidadãos (Zuboff, 2019). Estudos destacam que a vigilância generalizada pode levar a discriminação, uso indevido de dados e um ambiente de constante monitoramento que erosiona a confiança pública (Cardullo; Kitchin, 2018).

Além disso, a coleta massiva de dados por dispositivos IoT representa outro risco significativo para a privacidade (Greenfield, 2017). A promessa de eficiência e personalização na gestão urbana muitas vezes ignora a necessidade de medidas robustas de segurança e privacidade. Dados coletados sem uma análise de impacto adequada podem ser vulneráveis a acessos não autorizados, levando a possíveis abusos por parte de entidades públicas e privadas (Verma; Raghubanshi, 2018). A ausência de regulamentação clara e a falta de transparência na utilização desses dados exacerbam esses riscos, criando um cenário onde os cidadãos se tornam alvos fáceis de vigilância e controle.

A análise de impacto de privacidade (*Privacy Impact Assessment* – PIA) deveria ser uma prática padrão antes da implementação de qualquer tecnologia em cidades inteligentes. No entanto, muitas vezes, essa etapa crítica é negligenciada em favor de uma rápida implementação, impulsionada pelo entusiasmo inicial (Kitchin, 2016). Sem PIAs, as *smart cities* correm o risco de se transformar em distopias digitais, onde os direitos de privacidade são constantemente violados em nome da eficiência tecnológica. Estudos recentes mostram a importância das PIAs para identificar e mitigar riscos de privacidade em projetos de *smart cities* (Taylor; Richter, 2017).

Cidades como Toronto, com o projeto *Sidewalk Labs*, demonstram a importância de integrar PIAs no planejamento de *smart cities*. Esses projetos mostram que é possível equilibrar inovação tecnológica com proteção de privacidade, mas exigem um compromisso sério com a transparência e a regulamentação robusta (Cavoukian, 2012). Estudos evidenciam que a consideração proativa dos riscos de privacidade pode mitigar os impactos negativos a longo prazo e fomentar um ambiente urbano mais seguro e confiável (Verma; Raghubanshi, 2018).

A Lei de Amara nos lembra que os efeitos a longo prazo das tecnologias nas *smart cities* são frequentemente subestimados, especialmente em relação à privacidade. Para que as cidades inteligentes realizem seu potencial de maneira ética e sustentável, é essencial que os planejadores urbanos e os formuladores de políticas reconheçam esses riscos desde o início. Eles devem gerir as expectativas dos cidadãos, investir continuamente em medidas de segurança e envolver ativamente a comunidade no processo de decisão.

Portanto, a implementação de tecnologias em *smart cities* deve ser acompanhada de uma análise crítica e contínua dos riscos à privacidade, garantido que as inovações tecnológicas não comprometam os direitos fundamentais dos cidadãos. Só assim será possível construir cidades verdadeiramente inteligentes e justas, que respeitem a privacidade e promovam o bem-estar de todos os seus habitantes.

Um dos problemas fundamentais desse modelo de governança é a influência de empresas privadas nos espaços urbanos e na governança democrática, ao passo que serve de receita financeira estável para as empresas envolvidas, tanto pela prestação de serviços em si quanto pelo valor mercantil dos dados coletados, é possível que se estabeleça uma parceria de dominância entre empresa e grupos políticos, tornando extremamente difícil uma alteração no sistema por vias democráticas.

Ademais, mesmo que os dados permaneçam não identificáveis, a questão da propriedade dos dados permanece; apenas a entidade gestora foi alterada. Se uma empresa obtivesse acesso a esses dados públicos, somente ela obteria os benefícios advindos desse armazenamento, considerando que os produtores dos dados (os cidadãos) são externos a essas considerações.

Dentre as ameaças à privacidade nas cidades inteligentes, é possível destacar os seguintes riscos:

- Vigilância em massa: com a coleta generalizada, as informações podem incluir dados de localização, comportamento e hábitos dos cidadãos, o que pode comprometer a privacidade individual;
- Vazamento de dados: roubo de identidade e outros abusos;
- Perfilagem e análise de dados: os dados coletados nas cidades inteligentes podem ser usados para criar perfis detalhados dos cidadãos. Esses perfis podem ser usados para segmentar anúncios, influenciar comportamentos e até discriminar certos grupos de pessoas;
- Falta de consentimento informado: em algumas situações, os cidadãos podem não estar cientes de como seus dados estão sendo coletados, usados e compartilhados nas cidades inteligentes. A falta de transparência e consentimento informado adequado pode minar a privacidade e a autonomia dos indivíduos;
- Falhas de segurança em infraestrutura conectada: as cidades inteligentes dependem de uma infraestrutura conectada, o que pode torná-las vulneráveis a ataques cibernéticos. Um ataque bem-sucedido pode comprometer sistemas críticos, como redes de energia, transporte e saúde, levando a violações de privacidade em larga escala.

Diante desse contexto, ou a solução específica para o problema de segurança, que já foi parcialmente implementada, é obrigar a divulgação da violação de segurança. Atualmente, isso está previsto no art. 38 da LGPD, leia-se:

> 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 (Brasil, 2018).

Contudo, um problema óbvio é a falta de harmonização global dos padrões legais de segurança em um mundo de compras globais. A Convenção de Crime Cibernético de Budapeste fornece um mínimo de harmonização internacional sobre regulamentação de segurança, mas tem como objetivo principal permitir a aplicação da lei global em questões criminais, mas não promover padrões de segurança mais elevados para a indústria, sobretudo porque não impõe nenhuma responsabilidade civil (embora o art. 13 permita que exista).

É importante investigar se as várias disposições em discussão para proteger infraestruturas críticas de ataques de guerra cibernética e insegurança cibernética

pode se estender a cidades inteligentes. Uma alternativa para esses problemas é um mercado de seguro de segurança cibernética global adequado. Isso é algo que está estagnado até o momento e ainda é emergente, mas que pode ser iniciado por uma mudança global para a notificação de violação de segurança obrigatória.

Esse problema é maior porque a LGPD tende a proteger uma zona ou “bolha” de privacidade que começa com os corpos, abrange as casas e se estende às comunicações privadas. Em contraste, as cidades parecem essencialmente um espaço público, onde as expectativas de privacidade (exceto pelo anonimato) têm sido historicamente reduzidas a zero. Mas, como MacSithigh (2012) observou na sociedade da informação muitos espaços virtuais controlados por interesses privados adquiriram um caráter quase público semelhante a praças ou bibliotecas públicas, lugares onde historicamente direitos de expressão, acesso ao conhecimento ou reunião eram tradicionalmente exercidos: notavelmente comunidades *online* e motores de busca (MacSithigh, 2012).

Em “cidades inteligentes”, opera o paradigma reverso: o que era historicamente público, como as praças, as estradas, o transporte público, os sistemas de saúde e policiamento, provavelmente será operado de forma privada ou, pelo menos, cheio de sensores operados de forma privada, cujos dados coletados serão tratados em bancos de dados privados.

Essas partes das cidades agora se tornaram o que pode ser chamado de “lugares públicos privados” (ou, como prefere MacSithigh (2012), lugares “pseudoprivados”). Koops (2014) desconstruiu essa noção de “limites dos espaços privados” natural, argumentando que o lugar não é mais um fator útil para delinear os limites da esfera privada. Ele ressalta que, hoje em dia, os dados pessoais, que antes teriam ficado com segurança em casa, agora são transportados ou armazenados em *smartphones* e dispositivos portáteis, servidores de *webmail* ou na nuvem em geral.

Além disso, dados que eram opacamente seguros em casa, agora, são frequentemente transparentes para o mundo: e.g., casas equipadas com medidores inteligentes revelam detalhes de consumo de energia e aplicações elétricas para banco de dados das empresas. Sensores de calor, microfones direcionais e minúsculos drones de vigilância também podem romper a parede doméstica. Finalmente, mesmo em espaços públicos, onde antes as pessoas confiavam na “obscuridade prática” do anonimato causado pelo fato de ser mais um na multidão é anulada ou diminuída pela prevalência da vigilância por meio de sistemas inteligentes

de videomonitoramento, reconhecimento de placa de veículos, GPS, rastreamento de rede Wi-Fi e *software* de reconhecimento facial.

Vivemos uma era de dados onipresentes na qual não mais se pode entender o conceito de privado a partir de um espaço. Diante desse quadro, surgem os seguintes questionamentos.

Se os dados pessoais são facilmente acessíveis nas áreas “públicas” de uma cidade inteligente, então as mesmas proteções de privacidade devem ser aplicadas em uma residência privada? Koops (2014) aponta a problemática em áreas como processo criminal. Por exemplo, o *smartphone* deve ser protegido quando há mandados de busca e apreensão na residência? E quando há prisão em flagrante? A mesma regra vale para os dados de localização do GPS?

Vive-se, verdadeiramente, no panóptico urbano. Em defesa das cidades inteligentes, argumenta-se que a divulgação de dados por residentes em uma cidade “inteligente” simplesmente não pode ser evitada. Finch e Tene (2014, p. 41) apontam que, ao contrário de quando se escolhe uma rede social de provedor de entretenimento online, um site de compras ou um mecanismo de pesquisa (digamos), “os residentes de cidades inteligentes têm poucas alternativas aos sensores operados pelo governo e tecnologias de vigilância. implantados em todo os arredores”.

Isso é particularmente verdadeiro quando se trata de serviços essenciais, como saúde, resposta a emergências e policiamento. Contudo, tais dados podem dar poder extremo a um governo paternalista, e.g., que pode exigir que um cidadão obeso caminhe em vez de pegar o ônibus (inteligente e conectado) para o trabalho, salvando assim vidas, ou, dinheiro do orçamento da saúde.

Ainda, os dados podem cair nas mãos de provedores privados e daí para o mercado aberto, com impactos negativos nos contratos com seguradoras, empregadores ou agentes da lei. A *Xsolla*, e.g., em sua filial russa, demitiu 150 dos 450 funcionários de seus escritórios em Perm e Moscou, seguindo apenas a recomendação de um algoritmo de eficiência no trabalho que os considerou “improdutivos” e “pouco comprometidos” com os objetivos da empresa a partir da dados coletados do *Big Data* (Echarri, 2021).

A história das corporações comerciais privadas da Internet tem sido de uma nítida falta de competição, onde quase todas as empresas contam com políticas de privacidade padrão para obter o máximo de dados pessoais possível, contando com a ignorância e inércia do consumidor, falta de transparência e o efeito de “bloqueio”

dos efeitos de rede em setores como as redes sociais, para restringir a resistência dos consumidores.

Pode ser útil perguntar neste ponto identificar quais expectativas (se houver) o público tem de proteção à privacidade em cidades inteligentes, ou dados falhos sobre isso, em sua interação com a IoT.

A confiança e a confiança do público nas tecnologias são geralmente consideradas vitais para sua adoção, e já foram registradas dúvidas sobre a confiança do público na IoT, em parte por causa das ameaças à segurança já debatidas e em parte devido aos sentimentos gerais entre os usuários comuns de perda de controle sobre os dados pessoais para terceiros, mais frequentemente em contextos como redes sociais, motores de busca e publicidade direcionada.

Uma pesquisa da Comissão Europeia sobre Governança da Internet das Coisas descobriu que 67% dos entrevistados concordaram que “os aplicativos da Internet das Coisas representam ameaças à proteção da identidade de um indivíduo” e 81% estavam preocupados sobre como os dados adquiridos da IoT seriam “usados, armazenados e acessado por quem (União Europeia, 2013).

Estabelecido o panorama geral dos riscos que as cidades inteligentes apresentam à privacidade, na próxima seção analisaremos como a LGPD pode responder a esses riscos e se o pode.

As cidades inteligentes são um ambiente propício para as ameaças à privacidade, como demonstrado. Um dos fatores centrais é a IoT. Há uma literatura crescente sobre a ameaça potencial que a IoT representa para a privacidade e o aumento da conscientização pública sobre a IoT, especialmente no contexto de cidade inteligente, como uma ferramenta de vigilância abrangente.

Nesse sentido, o relógio inteligente revela falta de exercício para o plano de saúde, o carro diz à seguradora sobre o excesso de velocidade frequente e a lata de lixo informa à prefeitura que o cidadão não está seguindo os regulamentos locais de reciclagem. O principal problema da IoT, para fins de privacidade, é que os dispositivos foram explicitamente projetados para serem discretos e ininterruptos como uma experiência de usuário, i.e., para se entrelaçar sorrateiramente na trama da vida cotidiana até que sejam indistinguíveis dela.

Os sistemas IoT, como iluminação ambiente inteligente ou aquecedores inteligentes, como o NESTA (Baeck; Saunders, 2015) são frequentemente projetados para estar contextualmente cientes das necessidades e desejos do usuário, coletando

informações sobre suas práticas e rotinas diárias, enquanto permanecem invisíveis para os usuários.

Isso é mais nítido quando se contrasta a coleta de dados por esses aparelhos com a coleta de dados por empresas como o *Facebook*, *Google*, *Amazon* ou *eBay*. O cidadão tem ciência de que está fornecendo informações a essas empresas e geralmente tem a oportunidade de dar ou negar consentimento para a coleta de tais dados antes de começar a usar o serviço.

Na IoT, o aviso de consentimento é ausente no design do objeto. Mesmo onde a discrição não é uma especificação de função, os dispositivos IoT simplesmente não têm meios para exibir avisos de privacidade e/ou fornecer consentimento ajustado de acordo com as preferências expressas pelos indivíduos, visto que os dispositivos são geralmente pequenos, sem tela ou sem um mecanismo de entrada (um teclado ou uma tela sensível ao toque).

Se o quadro já é ruim em residências domésticas, torna-se mais grave em locais públicos de cidades inteligentes. Embora os consumidores possam, pelo menos teoricamente, ter tido a chance de ler a política de privacidade de suas luzes inteligentes antes de assinar o contrato, eles não terão essa oportunidade quando seus dados forem coletados pela estrada, transporte coletivo inteligente em que vão trabalhar. É fácil ver que, em tais sistemas, o esquema de consentimento na LGPD não serve de salvaguardas para a privacidade do cidadão.

O art. 7º da LGPD exige que os controladores de dados pessoais os tratem apenas amparados nas hipóteses exaustivas de seus incisos, sendo o consentimento apenas um desses motivos. Leia-se:

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

> atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X – para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (Brasil, 2018, negrito nosso).

Indubitavelmente, muitos ou a maioria dos sistemas de IoT em cidades inteligentes irão processar dados pessoais, a menos que medidas tenham sido tomadas para torná-los anônimos de maneira eficaz.

O consentimento é definido no art. 5, inc. XII da LGPD como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (Brasil, 2018). Essa definição é consideravelmente problemática pelos recursos do ambiente de IoT.

O consentimento é a única maneira desse armazenamento de dados pela IoT ser legitimado; não há motivos alternativos. O consentimento, conforme observado acima, deve ser “informado” por elementos abrangentes anteriores, mas não precisa ser explícito. A ideia de consentimento foi originalmente destinada para controlar a colocação de cookies “legítimos” no computador de um usuário, como uma questão de privacidade. Mas não é claro se esse esquema serve para dados sobre usuários coletados de sensores de vários tipos no “mundo real”.

Tal dificuldade ocorre por alguns motivos: os dados podem ser compartilhados automaticamente de máquina para máquina, sem transparência para o usuário ou oportunidade de revisão e a qualidade de qualquer consentimento do usuário pode ser ruim na IoT.

Nada obstante, a LGPD dispensa o consentimento nos seguintes casos.

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei (Brasil, 2018).

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: [...] II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de

> saúde, serviços de saúde ou autoridade sanitária; g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (Brasil, 2018).

Como se vê, quando os sistemas IoT são usados para prevenir ou detectar crimes (como com a maioria dos sistemas de circuito fechado de TV [CFTV] inteligentes), a LGPD pode afastar a sua incidência, com base no seu art. 11, inc. II, alínea e). Isto ocorre, e.g., quando as agências governamentais locais ou nacionais coletam dados para sistemas de governo eletrônico, saúde eletrônica, bem-estar eletrônico (art. 11, inc. II, alíneas b e c). Até aí tudo bem.

Mas, para a maioria dos sistemas comerciais, o que se pode esperar é uma forte confiança no fundamento dos "interesses legítimos" do art. 7º, inc. IX da LGPD, que seria uma maneira preocupantemente fácil de evitar qualquer aparência de controle do usuário. As empresas podem alegar que os dados coletados do usuário servem à otimização do sistema e melhoramento do serviço para todos, configurando, então, o interesse legítimo previsto no dispositivo acima citado.

O art. 10 da LGPD define o que seriam interesses legítimos:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I – apoio e promoção de atividades do controlador; e II – proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei. § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. § 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse. § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial (Brasil, 2018).

A preocupação se dá porque não é possível saber se as informações coletadas pelo IoT estão armazenadas somente no "equipamento terminal do usuário" e se as redes as quais os sensores IoT estão conectados se qualificam como "públicas" o suficiente para se enquadrarem no escopo dos permissivos da LGPD para tratamento de dados sem consentimento.

Veja-se o exemplo: imagine-se um celular que conta os passos de um usuário e identifica sua localização, armazenando essas informações no dispositivo, o qual,

por sua vez, periodicamente sincroniza esses dados pela Internet. Nesse caso, sem dúvida, a informação que no ponto de coleta é armazenada no equipamento terminal do usuário, exige o consentimento do usuário.

Agora, imagine que o mesmo usuário tenha sua localização e quilômetros percorridos coletados por um carro inteligente sem motorista ou “conectado”, agindo como um serviço de transporte por aplicativo. Nesse caso, é o “usuário”, o proprietário do veículo ou a operadora (que pode não ser a mesma pessoa) do carro conectado o titular desses dados? Assim, o consentimento é uma noção clara no contexto de um telefone móvel, mas muito menos em um ambiente de espaço público IoT inteligente.

No exemplo, poder-se-ia alegar a incidência dos § § 4º e 5º do art. 7º da LGPD, segundo os quais:

> Art. 7º [...] § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei. § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei (Brasil, 2018).

Ora, pode-se afirmar que quem anda na rua não pode esperar anonimato do seu trajeto porque seu caminho é visível a quem nela estiver ou que os dados são compartilhados em prol de interesses legítimos do controlador, o qual pode afirmar que precisa do compartilhamento dos dados para tornar os custos do processamento de tais dados e seus benefícios acessíveis aos consumidores.

No exemplo do transporte por aplicativo, o que é menos claro é: a) se o consumidor, o proprietário do veículo ou o seu operador em algum momento do processo puderam decidir sobre o uso desses dados e quem seria o titular; b) se é permitida a reutilização desses dados de localização, e.g., para a construção de um perfil para fornecer anúncios direcionados, permitindo a isenção do consentimento, já que seria útil para o usuário saber das ofertas considerando os lugares pelos quais ele trafega.

Toda essa questão poderia ser evitada se fosse obrigado aos responsáveis pelo tratamento de dados a anonimização dessas informações, sendo passíveis de utilização apenas naquilo que não identificassem os usuários. Mas, como se sabe, isso teria pouco valor comercial agregado.

Superada a problemática da IoT, avançasse a discussão para o *Big Data*. O principal problema são as indústrias de dados *online* – e agora as indústrias de IoT – que possuem um campo de dados incrivelmente vasto para minerar.

As cidades inteligentes são consumidoras e produtoras de *Big Data*. Na urbanidade moderna, os dados gerados dentro da infraestrutura e serviços públicos tradicionais da cidade, e.g., transporte, gás, eletricidade e água, não são apenas fluxos digitais, mas também são complementados e combinados com *Big Data* gerados por empresas privadas comerciais (como operadoras de telefonia móvel, mídia social, proprietários de sites, muitas vezes por meio de corretores de dados comerciais) e dados abertos de *crowdsourcing* (e.g., iniciativas de ciência cidadã).

Hoje, muitos desses dados vivem em silos, mas cada vez mais será combinado por gestores públicos municipais e também por provedores de serviços privados, como já é o caso em algumas aplicações de cidade inteligente, a exemplo das salas de controle centralizado para monitoramento da cidade encontradas no Rio de Janeiro.

Esses enormes volumes de dados granulares gerados a partir de sistemas IoT permitir a inferência de dados em uma escala sem precedentes. Os *smartphones* já permitem inferências sobre o humor do usuário, níveis de estresse, tipo de personalidade, distúrbios psicológicos, hábitos de fumar, características demográficas, padrões de sono, felicidade e níveis de exercício e movimento; as informações completas da IoT de uma cidade inteligente sobre seus cidadãos individuais permitirão muito mais. Como comenta Wisman (2013), O Panóptico de Bentham é uma brincadeira de criança em comparação com a vigilância em um IoT totalmente funcional.

Portanto, as cidades inteligentes geram grandes conjuntos de dados e os processa também. Em ambos os casos, o *Big Data* não precisa envolver dados pessoais, mas quase sempre o fará. Mesmo nos casos em que os dados são gerados com aparente anonimato – e.g., quantidade de pessoas pisando em uma praça públicas (*fottfall*) – a relativa facilidade de associar dois grandes bancos de dados – digamos, um banco de dados *fottfall* e um banco de dados circuito fechado de televisão (CFTV) – para identificar pessoas, é uma prática bastante conhecida (Ohm, 2009). Esse processamento de dados, isto é, a busca de dados em mais de um conjunto para encontrar a identidade de uma pessoa a partir de fontes distintas,

mesmo quando houve tentativas de desidentificação, é chamada também de “efeito mosaico”.

Fotos de usuários, nomes reais ou apelidos on-line também podem ser usados como identificadores exclusivos ou quase exclusivos em vários bancos de dados. Sobre a privacidade, as principais preocupações em torno de “*Big Data*” residem, portanto: a) no potencial de reidentificação de dados supostamente anônimos ou pseudonimizados; b) na redefinição de “*Big Data*” coletados para fins diferentes do original; c) a falta de transparência sobre como os resultados são derivados de *Big Data*, em particular onde a mera correlação (e.g., “jovens negros estão mais frequentemente envolvidos em crimes violentos” com a causalidade (“jovens negros devem ser os primeiros a serem presos por suspeita quando ocorrem crimes violentos “); d) a tendência de coleta exaustiva de todos os dados” e de afastamento do princípio de minimização da coleta de dados geralmente promovido pela LGPD.

A análise do marco regulatório atual, particularmente em relação à Lei Geral de Proteção de Dados, revela a tentativa de equilibrar inovação tecnológica e privacidade individual. No entanto, como enfatizado por Patrícia Peck Pinheiro, a digitalização nas cidades inteligentes demanda uma revisão constante das leis para assegurar que a proteção de dados pessoais se mantenha como um pilar fundamental à confiança e à sustentabilidade desses ambientes urbanos inovadores. Assim, a adequação das leis deve ser vista como um processo contínuo, que acompanha a evolução tecnológica e os seus impactos sobre a sociedade.

4.2.1 Discriminação Algorítmica

Para compreender o tema, Inicialmente, pode-se estabelecer as seguintes diferenciações:

- Preconceito: é uma ideia estereotipada de alguém sobre alguém. Quando uma pessoa pensa algo sobre outrem a partir de demarcadores existenciais humanos tais como etnia, nacionalidade, religião, orientação sexual, origem etc., sendo essa pré-compreensão pejorativa e redutora da dignidade daquela outra pessoa humana, haverá preconceito. De todo modo, é algo que está no plano interno do sujeito, podendo até mesmo nem mesmo ser manifestado publicamente;

- Discriminação: discriminação ocorre quando existem atos materiais concretos para tratar de modo diverso um indivíduo ou um grupo de indivíduos em razão de características pessoais suas. Quando alguém age para segregar alguém ou grupos de pessoas a partir de demarcadores existenciais, haverá discriminação. É algo que transcende o plano interno do sujeito, ganhando manifestação no mundo dos fatos;
- Racismo: ocorre quando há discriminação de modo sistemático e geral, especificamente, em razão do aspecto étnico.

A partir da delimitação de tais conceitos, pode-se trabalhar algumas espécies de discriminação. Inicialmente, pode-se, seguindo a literatura norte-americana e nacional sobre o tema, diferenciar em discriminação direta (*disparate treatment*) e indireta (*disparate impact*).

A discriminação direta existe quando são tomados atos materiais intencionais com o intuito de discriminar. Segundo Roger Raupp Rios, Desembargador Federal do Tribunal Regional Federal da 4ª Região (TRF4), a discriminação direta no direito norte-americano, pode ser de 3 (três) espécies:

i) Discriminação Explícita (*facial discrimination*): é a mais clara e manifesta demonstração de discriminação. É a manifestação intencional, direta e objetiva contra uma pessoa ou grupo fundada em um critério constitucionalmente vedado;
ii) Discriminação na Aplicação do Direito (*discriminatory application*): ocorre quando a medida a ser aplicada, em tese, não é discriminatória, mas é aplicada de modo discriminatório. Por exemplo: a lógica das revistas policiais, os conhecidos “baculejos”. Em tese, tais atos não são per si discriminatórios, pois cabe à atividade policial, de fato, investigar suspeitos, mas quando tais atos de investigação só recaem apenas contra públicos étnicos e sociais específicos, revela- se aí uma aplicação discriminatória explícita da medida;
iii) Discriminação na Concepção (*discrimination by design*): ocorre quando na formulação de leis, políticas públicas ou ações privadas modela-se um padrão discriminatório de conduta. Um exemplo seria a exigência de determinados atributos físicos (os famosos anúncios de “boa aparência”) para alguém ocupar um cargo na iniciativa privada.

Tal como não poderia deixar de ser, Raupp Rios afirma que o "ordenamento jurídico brasileiro sanciona, de modo claro e direto, a discriminação na sua forma direta e intencional". Já a discriminação indireta (*disparate impact*) ocorre de modo mais sorrateiro. Na discriminação indireta não é necessário demonstrar a intencionalidade. No Brasil, esta forma de discriminação ficou especialmente conhecida como Teoria do Impacto Desproporcional.

A Teoria do Impacto Desproporcional está atrelada aos conceitos de discriminação de fato e discriminação por ações neutras:

i) Discriminação de Fato: ocorre quando a realidade é desigual e os atores envolvidos poderiam agir para encerrar a desigualdade, mas, por omissão, mantém a desigualdade de fato.
ii) Discriminação por Ações Neutras: acontece quando há uma norma aparentemente neutra, que, na sua aplicação, efetivamente irá discriminar uma pessoa ou grupo, ou seja, a mera aplicação da norma leva à discriminação.

No bojo da Ação Direta de Inconstitucionalidade (ADI) n.º 4.424, sobre a desnecessidade de representação da vítima na Lei Maria da Penha, o Ministério Público Federal (MPF), em peça subscrita pela Ex-Procuradora Nacional dos Direitos do Cidadão, Deborah Duprat, entendeu que a situação de discriminação indireta é correlata com a Teoria do Impacto Desproporcional. A Teoria do Impacto Desproporcional foi citada no voto do min. Joaquim Barbosa, na mesma ADI n.º 4.424:

> que tal teoria (do impacto desproporcional) consiste na ideia de que toda e qualquer prática empresarial, política governamental ou semigovernamental, de cunho legislativo ou administrativo, ainda que não provida de intenção discriminatória no momento de sua concepção, deve ser condenada por violação do princípio constitucional da igualdade material se, em consequência de sua aplicação, resultarem efeitos nocivos de incidência especialmente desproporcional sobre certas categorias de pessoas" (Brasil, 2012).

Uma preocupação particular gira em torno do potencial para discriminação com base na análise de dados e a possível criação de uma "subclasse de dados", incapaz de acessar os mesmos serviços e instalações que seus pares devido ao seu perfil de "*Big Data*" – um novo tipo de "linha vermelha" (Citron; Pasquale, 2014), semelhante ao que acontece no episódio *Nosedive*, da terceira temporada da série *Black Mirror*.

Sobre a questão, destaca Ehrhardt Júnior, França Netto e Malheiros (2022) que não se pode confundir discriminação com diferenciação. Segundo os autores: “A dialética de recursos e demandas subsidia as discriminações de ordem estatística, que de forma racional promovem separações entre indivíduos, vinculando-os a determinados grupos, de acordo com similitudes detectadas” (Ehrhardt Júnior; França Netto; Malheiros, 2022, p. 1288).

Desse modo, embora algumas discriminações sejam material e juridicamente aceitáveis, pois respeitam os mandamentos constitucionais relativos à isonomia e à vedação à discriminação. Desse modo, ocorre a discriminação, e não diferenciação, quando o processo de tomada de decisões por algoritmos de inteligência artificial resulta “em nocivos enviesamentos direcionados a indivíduos e grupos desprestigiados no curso da história” (Ehrhardt Júnior; França Netto; Malheiros, 2022, p. 1293)

De acordo com Hildebrandt (2008), o perfilamento (*profiling*) é a criação de perfis a fim de descobrir correlações entre dados que podem ser usados para identificar e representar um indivíduo ou grupo. Tais dados são transformados em conhecimento ou inferências, as quais são uteis para individuar, representar ou identificar um sujeito como membro de uma categoria, com a construção de prováveis atributos ou comportamentos.

Para Patz e Piaia (2021, p. 697):

> Contudo, quando sistemas de IA são utilizados para fins de avaliações educacionais, campanhas políticas, seleção de candidatos a empregos, e até mesmo para a implementação de mecanismos relacionados a policiamento preditivo e a admissão de migrantes em um Estado, diversas considerações devem ser feitas. Uma delas diz respeito à falta de transparência em relação aos titulares dos dados ou destinatários desses sistemas, que, muitas vezes, não conseguem acessar ou avaliar a qualidade das inferências que são realizadas sobre eles. Tal situação coloca em risco questões fundamentais inerentes à dignidade humana, como liberdade, igualdade, não discriminação, devido processo legal, proteção dos dados pessoais e dados pessoais sensíveis e da autodeterminação informacional.

Assim, as análises baseadas em informações capturadas em um ambiente de IoT podem permitir a detecção de padrões de vida e comportamento ainda mais detalhados e completos de um indivíduo. Isso pode levar à negação de um seguro, como aponta Thiago Junqueira (2020), à exclusão de venda digital de certos produtos de luxo ou de ponta, compartilhamento de inferências comprometedoras com

agências estaduais, ou mesmo a exclusão total dos mercados de serviços e utilidades essenciais para aqueles que não desejam compartilhar dados pessoais.

Pimentel e Nunes (2021), apontam alguns episódios de discriminação racial por algoritmos. Por exemplo. O aplicativo Google Fotos etiquetava pessoas negras como gorilas, pois a Inteligência Artificial não foi capaz de distinguir a pele humana com a do animal, embora conseguisse identificar imagens quando era buscado por “orangotangos”, “babuínos” ou “saguis”, mas não respondia quando se buscava por “macacos” ou “gorilas”. Assim, o Google decidiu resolver o problema de uma forma mais simples: apagando a etiqueta “gorila”. Tais problemas á se repetiram em plataformas como *Flickr* e o *Facebook*, que permitiam distinguir usuários por raça (Pascual, 2019).

Em 2016, a *Red Cross Blood Service*, prestadora de serviços de coleta e de doação de sangue na Austrália, foi vítima de um atentado em seu sistema de segurança de dados e informações, o qual continha cerca de 550 mil doadores. No vazamento, foram expostos usuários que tinham “comportamentos sexuais de risco”, expondo a intimidade (Pimentel; Nunes, 2021).

Em um sistema de recrutamento para novos funcionários, a empresa *Amazon* precisou remover seu sistema de algoritmos, utilizado para seleção de candidatos, porquanto a inteligência artificial adotada priorizava somente candidatos do sexo masculino. Pois ele deletava automaticamente as fichas que continham a palavra “mulher” (Ribeiro, 2018).

Em uma cidade inteligente, as consequências da exclusão de dados seriam tanto físicas quanto digitais. Certas pessoas (ou seus carros) podem ser fisicamente impedidos de entrar em algumas ruas – um novo tipo de “condomínio fechado” – ou em certas lojas ou complexos de entretenimento. A natureza complexa da parceria público-privada em cidades inteligentes também parece importante aqui – o que acontece com qualquer direito de reunião em praças públicas (ou discurso público em geral) quando todos os espaços são pelo menos parcialmente privatizados?

Outra preocupação prática é que os dados de IoT provavelmente estão cheios de erros e, portanto, os perfis de “*Big Data*” derivados também estariam. Kitchin (2015) enfatiza que, como os fluxos de dados em uma cidade inteligente são gerados de maneiras diferentes, usando uma infinidade de instrumentos e padrões, juntá-los resultará em dados enganosos de baixa qualidade.

4.3 *BIG DATA* E A LGPD

O termo *Big Data*, traduzido como grandes dados, resulta da necessidade de desenvolver uma tecnologia capaz de trabalhar com o crescente volume de dados e a demanda para extrair informações sobre esses dados, que na maioria das vezes são armazenados sem destino e ou objetivo certo.

Já comum em publicações científicas e em editais de fomento à pesquisa, o termo significa um dos aspectos do campo da ciência de dados que trata de estratégias para extração, transformação e carga dos dados, modelagem, construção e avaliação de algoritmos descritivos e preditivos, visualização de grandes quantidades de dados e *deploy* dos modelos em ambientes de produção para a tomada de decisão, entre outros.

De acordo com Saldanha, Barcellos e Pedroso (2021, p. 52) “o que importa na definição de *Big Data* não é o volume ou mesmo a velocidade da produção de dados, mas a complexidade estrutural desses dados (variedade) e o poder computacional necessário para analisá-los integralmente”.

Para manejo desses dados, há tecnologias-base como o *Data Mining*, *Business Intelligence* e Computação em Nuvens, além de uma das maiores fontes de dados para o *Big Data*, as Redes Sociais.

Data Mining significa mineração de dados, consiste em um processo analítico projetado para explorar grandes quantidades de dados (tipicamente relacionados a negócios, mercado ou pesquisas científicas), na busca de padrões consistentes e/ou relacionamentos sistemático entre variáveis para, então, validá-los aplicando os padrões detectados a novos subconjuntos de dados. Visando transformar esses dados em conhecimento, criou-se o processo conhecido por Descoberta de Conhecimento em Bancos de Dados (*Knowledge Discovery in Databases* – KDD).

De acordo com Caldas e Silva (2016, p. 70):

> A premissa de um Data Mining é uma argumentação ativa, em que, uma vez definido o problema, os dados e a ferramenta de análise, o Data Mining pesquisa, automaticamente, nesse montante de dados, anomalias e prováveis relacionamentos, encontrando possíveis problemas que não foram identificados anteriormente pelos usuários. Usando técnicas de estatística e inteligência artificial, além de reconhecimento de padrões e recuperação de informações, como também o Data Mining é possível fazer uso de algoritmos de aprendizagem ou classificação baseada em redes neuronais, para explorar um conjunto de dados, retirando e auxiliando na identificando de padrões, favorecendo, assim, a descoberta por meio do conhecimento.

Business Intelligence é uma tecnologia que tem como conceito básico a entrega da informação coletada a partir de dados do *Data Warehouse*, de forma exata e útil, para a tomada de decisões.

Conforme os mesmos autores:

> Uma solução de BI permite monitorar o desempenho dos processos operacionais, táticos ou estratégicos por meio de indicadores de desempenho e apresentá-los em painéis de controle ou *dashboard*, com recursos analíticos e interativos que permitem cruzar e analisar informações, no tempo em que se precisa, transformando o processo de decisão em algo simples, rápido e eficiente. As soluções de BI também englobam diversas técnicas e ferramentas para coletar dados de diversas fontes de dados. Entretanto, o BI coleta dados relacionais; já o Big Data usa dados não relacionais e fontes inusitadas (Caldas; Silva, 2016, p. 71).

A LGPD interage de forma problemática com "*Big Data*" em pelo menos três maneiras importantes: limitação da finalidade, transparência algorítmica e minimização de dados.

Em primeiro lugar, e mais importante, a LGPD baseia-se fundamentalmente na ideia de que os dados devem ser recolhidos para fins "especificados, explícitos e legítimos" e não posteriormente processados de forma incompatível com esses fins, conforme art. 5º, inc. I, da LGPD, o qual conceitua finalidade como "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". São diversos os dispositivos nesse sentido[1].

Esta regra de "limitação de propósito" se aplica mesmo quando o processamento foi legitimado por um motivo diferente do consentimento. O *Big Data* está em total desacordo com esse princípio. Como Mayer-Schönberger e Cukier (2013) dissertam, "na era do *Big Data*, os usos secundários mais inovadores não foram imaginados quando os dados são coletados pela primeira vez".

---

[1] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.;
Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I – finalidade específica do tratamento;

Pode-se (e é) argumentado que o ataque de *Big Data* à limitação de propósito pode ser tratado por uma série de estratégias legais, incluindo pedir consentimento para reutilizações plausíveis no início, obter um novo consentimento para reutilizar os dados à medida que surgem ou usar um fundamento não baseado no consentimento, como “interesses legítimos”, para tornar o reaproveitamento legal, conforme já é previsto no art. 7º, § 7º da LGPD, segundo o qual:

> O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei (Brasil, 2018).

No entanto, em cada caso, parece evidente que a solução é de fato ilusória. Um consentimento geral para todas as reutilizações possíveis seria por si só tão vago a ponto descumprir a regra de “fins específicos e limitados”; buscar um novo consentimento também envolveria certamente despesas proibitivas para controladores de dados comerciais e de serviço público. Finalmente, e o mais problemático, uma característica muito citada do tratamento de dados é que ela pode dar respostas a perguntas nem mesmo pensadas anteriormente, que não estavam nos termos de consentimento inicial.

Assim, o *Big Data* desafia a ideia fundamental de Proteção de Dados que é a transparência de processamento. O *Big Data* atua como uma “caixa preta”: os dados entram e saem, mas o algoritmo que cria o resultado geralmente é invisível para o usuário e os resultados muitas vezes inescrutáveis. Os algoritmos também aprendem e mudam de maneira semiautônoma – tornando-os extremamente difíceis de documentar. Por fim, os algoritmos são o segredo comercial definitivo – a fortuna do Google é baseada inteiramente em seus avanços em algoritmos de busca – e, portanto, as empresas estarão incrivelmente relutantes em torná-los públicos.

Algoritmos opacos de *Big Data* são perigosos porque a discriminação que poderia ser ilegal, e.g., sobre raça ou orientação sexual, pode ser facilmente escondida, deliberadamente ou não, por trás do véu algorítmico. Embora os direitos de acesso do sujeito para descobrir quais dados são mantidos sobre eles por um controlador de dados sejam razoavelmente bem conhecidos (pelo menos para advogados e ativistas), muito pouca atenção é dada a um direito também concedido pela LGPD: conhecer a “lógica do processamento aplicado aos seus dado”, como previsto no art. 9º segundo o qual:

> O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso (Brasil, 2018).

Por sua vez, o art. 6º, inc. IV da LGPD assim dispõe:

> 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; [...] (Brasil, 2018)

Esse direito à transparência algorítmica sempre foi limitado para proteger a propriedade intelectual e segredos comerciais. Como ele pode ser aplicado e usado como proteção ao consumidor no mundo do *Big Data* é difícil de vislumbrar: mesmo se o controlador realmente sabe o que seu algoritmo está fazendo (o que muitos agora duvidam em cenários de processamento vasto, como o algoritmo de pesquisa do Google), como isso seria explicado ao titular dos dados de forma compreensível?

Além disso, o *Big Data* também se opõem totalmente ao princípio de que os dados pessoais coletados devem ser “adequados, relevantes e não excessivos” em relação aos fins para os quais são coletados e/ou processados posteriormente, isso vai contra o art. 6º, inc. III da LGPD, que positiva o princípio da necessidade, segundo o qual deve haver “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”.

A minimização de dados é uma falácia para esse sistema, pois é mais barato, mais fácil e mais útil coletar todos os dados do que alguns deles, de modo que os impulsos comerciais apontam para a aquisição do máximo de dados possível, apenas no caso de serem úteis para aquela “caça ao tesouro” no futuro.

A Autoridade Europeia para a Proteção de Dados (AEPD) declarou recentemente:

> há uma tendência preocupante no sentido de se pensar que, no que diz respeito às informações pessoais, tudo o que for possível também é desejável 'se houver dados pessoais disponíveis, devem ser recolhidos e armazenados indefinidamente e explorados para qualquer finalidade expediente (Fuster; Scherrer, 2015, p. 8).

Esses problemas não são realmente solúveis sem uma grande alteração dos modelos de negócios de *Big Data* ou da LGPD. Na verdade, a maior parte do tratamento de dados, coleta excessiva e subsequente reaproveitamento de dados são

justificados, não pela prova de conformidade com a LGPD, mas pela alegação de que o que é processado não são dados pessoais de forma alguma.

Como já dito, para a AEPD, o que normalmente ocorre é a substituição do verdadeiro anonimato pela pseudonimização de valor duvidoso de proteção da privacidade, em razão do baixo valor comercial de dados minimizados e anonimizados. Ademais, perfis de dados pseudonimizados, como usados, e.g., pelas mídias sociais e mecanismos de pesquisa para fornecer publicidade direcionada, ainda permitem que os indivíduos sejam “selecionados” e sujeitos a tratamento discriminatório.

Uma guerra de territórios está acontecendo entre o que a LGPD pensa ser anonimização suficiente e o que as empresas comerciais e alguns reguladores nacionais gostariam que fosse, enquanto, entretanto, a maioria dos usuários (e a maioria dos advogados) nada sabem a respeito das reivindicações concorrentes de anonimização, pseudonimização ou criptografia bem-sucedida.

O progresso vacilante da LGPD em pontos-chave como a definição de consentimento, a extensão da base de “interesses legítimos” para processamento e a invenção repentina de uma categoria mal pensada de dados pseudônimos se dá pela pressão da indústria (Mundie, 2014), de certos setores da ciência (Goerge, 2014) e governos, sob argumentos de pragmatismo, benefício social e redução de custos.

Nesse cenário, é impossível policiá-los quando forem processados, traçados, “anonimizados”, extraídos de dados, reidentificados, copiados, espelhados e enviados ao redor do mundo para várias jurisdições com leis diferentes. Em resumo, portanto, a LGPD, conforme constituída atualmente, não tem boas respostas para lidar com os problemas de privacidade apresentados pelo *Big Data*. Tais respostas podem vir de outros instrumentos jurídicos, como o CDC e legislação trabalhista, ou da afirmação do direito ao devido processo, previsto no art. 5º, LIV da CRFB/88.

4.4 A NUVEM E A LGPD

O *cloudcomputing* chegou ao público em 2008, e corresponde a tudo o que hoje é computação (processamento, armazenamento e *softwares*), só que armazenado na rede, podendo ser acessadas, remotamente, de qualquer lugar do mundo, e independente de plataforma, nas mais variadas aplicações por meio da Internet com a mesma facilidade de tê-las instaladas no próprio computador.

O armazenamento dos dados é realizado por serviços que podem ser acessados de qualquer lugar do mundo e a qualquer hora, não importando se o usuário possui ou não o *software* ou até mesmo espaço em disco para isso. O acesso é feito, principalmente, por meio de navegadores que acessam remotamente servidores físicos localizados em qualquer lugar do mundo.

Obviamente, a maior parte dos dados gerados pelas cidades inteligentes é armazenada na nuvem. A computação em nuvem é normalmente baseada no fornecimento de recursos aos usuários de uma rede de servidores e de provedores e subprovedores, com armazenamento de dados, *software* e infraestrutura disponibilizados dinamicamente “como serviço”: geralmente com grandes vantagens em velocidade, custo e escalabilidade para o consumidor ou empresa.

Os dados na nuvem normalmente têm um local desconhecido e variável de armazenamento e/ou processamento, muitas vezes composto por vários backups ou processamento distribuído de dados em várias jurisdições. Às vezes, é possível especificar contratualmente que os dados não serão armazenados ou processados fora da do Brasil, mas isso é atualmente muito incomum no mercado de consumo, por razões de logística por parte das empresas americanas dominantes no mercado, e a falta de um forte setor da indústria em nuvem no Brasil.

O uso generalizado da computação em nuvem para receber e processar dados de dispositivos e aplicativos IoT inteligentes, portanto, levanta questões legais espinhosas que giram em torno da jurisdição e da lei aplicável, agravadas pela diferença nas culturas de privacidade. A LGPD prevê o fluxo livre de dados pessoais para países localizados fora do Brasil apenas se o país ou o destinatário fornecer um nível “adequado” de proteção de dados, potencialmente limitando assim as transferências de dados transfronteiriças, conforme art. 4º, inc. IV da LGPD:

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: IV – provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, **desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei** (Brasil, 2018, negrito nosso).

Dado o número muito pequeno de países que possuem legislação de proteção de dados compatíveis com a LGPD, a inaplicabilidade da lei a permitir a transferência de dados para fora do Brasil é uma questão crucial. A Lei estabelece uma série de motivos, como o consentimento do titular dos dados, cláusulas

contratuais modelo e regras corporativas vinculativas (BCRs). Uma solução aspirante para as cidades inteligentes pode ser ajudar a construir e usar uma nuvem exclusiva para o Brasil.

4.5 O RECONHECIMENTO FACIAL

A relação entre inteligência artificial (IA) e cidades inteligentes, ou "*smart cities*", é cada vez mais importante à medida que as cidades buscam usar tecnologia avançada para melhorar a qualidade de vida de seus habitantes e otimizar a gestão de recursos. A IA desempenha um papel fundamental nas *smart cities* de várias maneiras, como na gestão de tráfego, segurança pública, eficiência energética, estão de resíduos, qualidade do ar, atendimento ao cidadão, planejamento urbano, saúde pública e sustentabilidade.

Em resumo, a IA desempenha um papel crucial na transformação das cidades em lugares mais eficientes, seguros e sustentáveis. Ela capacita as *smart cities* a coletar, analisar e utilizar dados de maneira mais eficaz, o que, por sua vez, melhora a qualidade de vida dos cidadãos e a gestão urbana como um todo.

Há muito a literatura de ficção científica avisa a humanidade sobre os perigos da tecnologia aplicada ao controle das pessoas. Os cenários distópicos de George Orwell e Aldous Huxley, no entanto, trata-se de uma realidade concreta, sobretudo com o advento de tecnologias de reconhecimento facial.

Compreende-se que o reconhecimento facial se trata de um mecanismo de correspondência um contra todos que compara uma face de referência contra várias faces no banco de dados para associar a identidade da face de consulta com uma daquelas no banco de dados. Serve tanto para a identificação quanto para a confirmação da identidade de pessoas.

De acordo com Bennamoun, Guo e Sohel (2015), o sistema opera conforme as seguintes etapas: aquisição de dados, pré-processamento de dados, extração de características e classificação. A aquisição de dados ocorre por meio câmeras apanham imagens estáticas ou dinâmicas (vídeo) (modelo 2D) ou através de scanner 3D ou sensor de profundidade.

O reconhecimento facial (TRF) se trata de uma forma de inteligência artificial, depende de algoritmos para treinar conjuntos de dados faciais para reconhecer pessoas com precisão. Recentemente, a implantação do TRF provou ser útil na

identificação de pessoas que participaram da insurreição de 8 de janeiro (Serapião, 2023). No entanto, também houve casos em que seu uso foi deletério, como denuncia o New York Times acerca da utilização da tecnologia para inibir protestos legítimos na China (Mozur; Fu; Chien, 2022).

Embora haja argumentos relevantes para o emprego da tecnologia na área de segurança pública, por exemplo, os resultados de políticas públicas baseadas em reconhecimento facial podem ser bastante drásticos, como ocorre na China.

Em 2014, o Conselho de Estado da China divulgou o *Planning Outline for the Construction of a Social Credit System*, planejando o aprimoramento de um dos principais métodos já em utilização em várias *smart cities* chinesas: o Sistema de Créditos Sociais (Liang *et al.*, 2018).

Esse sistema foi inicialmente introduzido na Província de Jiangsu, em 2010, para medir e pontuar a conduta dos cidadãos, os quais começavam com 1.000 pontos, sendo que a cada quebra de normas, há uma subtração de pontos. Essa dedução ocorre não apenas pelo infringimento de normas legais (estritas), mas também por infringir normas administrativas e até morais (Creemers, 2018).

Entre as condutas que podem levar a uma perda de pontos, tem-se: conduzir automóvel embriagado, 50 pontos; ter um filho fora das permissões do planejamento familiar, 35 pontos; não realizar o pagamento de empréstimos, 30 a 50 pontos. Gradativamente, os cidadãos podem recuperar os pontos em 2 a 5 anos, a depender da norma violada e da gravidade da infração (Creemers, 2018).

A partir do score individual, cidadãos são categorizados em classes de A a D. Os da classe A possuem acesso preferencial a oportunidades de emprego, tornar-se membro de partido político; realizar alistamento militar; qualificar-se em processo para concorrer a moradias de baixo custo; obter licenças de funcionamento na categoria de comerciante individual.

Embora algumas consequências desse modelo tenham sido extintas, o sistema em si não foi se tornando parte da governança de algumas províncias da China a ideia de vigilância permanente (panoptismo), publicização do nome de “agressores”, expondo-os ao constrangimento público; e a expansão da utilização do mecanismo de crédito para além do contexto econômico, atingindo, também, a violação de normas administrativas e de gestão urbana.

Mas o que isso tem a ver com o reconhecimento facial? A união de um sistema de créditos sociais associada a essa tecnologia ao já citado episódio Nosedive, da

terceira temporada da série *Black Mirror*. Na trama, a personagem principal, busca melhorar a sua avaliação numa rede social para pagar um apartamento de luxo. Contudo, as avaliações pessoais da personagem são expostas publicamente e utilizadas como critério determinante para sua participação na vida social, a semelhança do que o projeto chinês pode conduzir.

A possibilidade de reconhecimento facial e um sistema de pontos expressa uma associação perigosa entre o desejo de controle total do Estado, tornando-se um mecanismo capaz de determinar os comportamentos mais corriqueiros e irrelevantes das pessoas.

Aqui, vale falar da teoria do ponto patético de Gotthold Ephraim Lessing, a partir de Marcelo Labanca Corrêa de Araújo e Walles Henrique de Oliveira Couto (2021). Originalmente aplicada à literatura e à pintura, mas que tem sido reinterpretada e adaptada ao contexto da tecnologia da informação. Neste novo cenário, o "ponto patético" pode ser entendido como o momento ou elemento específico em um sistema, interface ou aplicação que maximiza a resposta emocional do usuário. Vamos explorar como essa teoria pode ser aplicada ao design e desenvolvimento de tecnologia da informação.

Inicialmente, Gotthold Ephraim Lessing, proeminente teórico do Iluminismo, desenvolveu a teoria do ponto patético para discutir a eficácia emocional na arte. Na tecnologia da informação, o ponto patético de Lessing é reimaginado como o instante ou característica de um produto digital que gera a maior conexão emocional com o usuário. Esse ponto é crucial para garantir uma experiência de usuário eficaz, promovendo engajamento, satisfação e lealdade. Este ponto é essencial para que o produto digital atinja seu clímax emocional, causando um impacto significativo e duradouro no usuário.

Isso pode ser uma animação bem elaborada, uma mensagem de erro empática, um design visual atraente ou uma funcionalidade que resolve um problema específico de maneira inovadora, como a interação suave e intuitiva que faz o usuário sentir que está no controle total da aplicação. Em um site de *e-commerce*, pode ser a experiência de *checkout* simplificada que alivia o estresse do usuário ao finalizar uma compra. Em um jogo, pode ser o momento de vitória ou um elemento de narrativa que ressoa profundamente com o jogador.

Dessa forma, os designers e desenvolvedores identificam e enfatizam os momentos ou elementos chave que criam uma forte conexão emocional com o

usuário. Isso exige uma compreensão profunda das necessidades, desejos e emoções dos usuários, bem como habilidades técnicas para criar interfaces e funcionalidades que possam evocar essas emoções de maneira eficaz.

O Ministério de Segurança da China desenvolve, desde 2015, um projeto para identificação por vídeo de qualquer indivíduo entre seus 1,3 bilhão de habitantes em apenas três segundos. As informações relativas à imagem dos cidadãos perfazem um total de 13 *terabytes*, enquanto o banco de dados completo totaliza 90 *terabytes* (Chen, 2017).

Com essa tecnologia, em 20 de janeiro de 2020, as autoridades da cidade chinesa de Suzhou divulgaram fotos de sete pessoas, acompanhadas de número de identificação governamental e localização, após suas condutas serem classificadas como “comportamento não civilizado” porque estavam usando pijamas em público. Essas pessoas foram identificadas através de reconhecimento facial. Em Pequim, alguns banheiros públicos usam o reconhecimento facial para negar papel higiênico caso alguém o solicite mais de uma vez em certo período (Chen, 2017).

Também em 2019, a China protagonizou um caso de racismo (automatizado) utilizando reconhecimento facial a partir das características étnicas da comunidade uigures, grupo minoritário, formado em sua maioria por muçulmanos, que vivem na cidade de Yarkand, região de Xinjiang (Buckley; Mozur; Ramzy, 2019).

Durante a pandemia da Covid-19, a empresa chinesa de inteligência artificial, *SenseTime*, anunciou um sistema de reconhecimento facial aliado com câmeras de imagem térmica, a fim de identificar pessoas com temperatura elevada (sistema de detecção de febre). A partir disso, usuários do *software* passariam a receber alertas (*pop-up*) com os dados de identificação dessas pessoas como forma de aviso de possíveis pacientes do vírus ou proibir a entrada de pessoas que não usavam máscaras em prédios (Li, 2020).

No Brasil, o conflito entre uso de imagens e políticas públicas surge no debate recente e atual acerca do uso de câmeras acopladas nos uniformes de policiais militares. A tecnologia trouxe ótimos resultados para o Estado de São Paulo que, pela primeira vez, em 8 anos, não registrou mortes por abordagens policiais nos batalhões da Polícia Militar (PM) que integram o Programa “OlhoVivo”. São 18 no total, com aproximadamente 3 mil câmeras.

Embora parte dos policiais tenha se incomodado com o uso das câmeras, não há que se falar em violação a privacidade dos agentes, posto que as imagens são

coletadas durante o exercício do serviço público e não em momentos de sua vida privada. Contudo, a mesma lógica não vale para os cidadãos que terão suas imagens coletadas e passarão a constar de um enorme banco de dados.

Como se sabe, dados referentes a rostos humanos são dados pessoais e devem, portanto, ser protegidos do uso não consentido ou distinto daquele para o qual foram coletados. O problema surge com a falta de a falta de informações sobre o registro das imagens após o cumprimento do turno e a inviolabilidade das informações coletadas.

Nos aeroportos, o uso do reconhecimento facial serve para o *check-in* para embarque de companhias aéreas, como também para o sistema de vigilância. A Gol e a Latam firmaram parceria com o Serviço Federal de Processamento de Dados (Serpro), pois a validação da foto é feita pela comparação com as imagens no banco de dados de motoristas habilitados e/ou do Superior Tribunal Eleitoral.

Patz e Piaia (2021) apontam lacunas nesse projeto, como legitimidade do compartilhamento de dados entre o Denatran e o Serpro, até a ausência de esclarecimentos sobre a tecnologia utilizada no Programa e, por fim, informações relativas e elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) (Gomes, 2020).

De acordo com o Gomes (2020), a elaboração do RIPD deve ocorrer antes do tratamento de dados pessoais dos titulares. O Instituto questiona se foi feito um relatório de impacto pelo Ministério da Infraestrutura e Serpro antes de ser feito qualquer teste com pessoas naturais e, se sim, por que o relatório de impacto não foi publicizado ou por que ele não foi sequer mencionado? Se não, por que o relatório de impacto não foi elaborado? No caso do Embarque Mais Seguro, já houve o compartilhamento da base de dados do Denatran com a Serpro e não é possível, inclusive, saber se foi realizado um relatório de impacto para avaliar os riscos associados a esse compartilhamento (Gomes, 2020).

Para Patz e Piaia (2021, p. 706):

> Outro ponto de questionamento é porque a base de dados do Denatran foi compartilhada com a Serpro e está sendo usada para verificação de identidade dos passageiros nos aeroportos por meio de tecnologias de reconhecimento facial. Consoante o Instituto, a base de dados do Denatran possui atualmente dados pessoais de cerca de 78 milhões de pessoas. Essa mesma base de dados foi alvo de controvérsias anteriores, como, por exemplo, o vazamento de dados em 2019 no Detran RN e no Detran RJ, além da solicitação pela Agência Brasileira de Inteligência (ABIN) à Serpro de todas as CNHs no Brasil.

Os autores apontam outros exemplos de risco à privacidade e à proteção de dados pelo uso de reconhecimento facial. Informam eles que, desde 2016, a Receita Federal do Brasil usa o sistema de reconhecimento facial da empresa NEC em 14 aeroportos internacionais, com investimento de R$ 7.576.090,72. Isso com objetivo de encontrar viajantes com risco aduaneiro identificado, previamente selecionados pelo sistema de gerenciamento de risco, a fim de os encaminhar para fiscalização minuciosa" (Vigilância [...], 2021, p. 61). Nada obstante, a Receita afirmou que não existem mecanismos no sistema para extrair os dados coletados mediante solicitação do titular (Vigilância [...], 2021, p. 61), violando, portanto, a LGPD.

Patz e Piaia (2021, p. 707) mencionam, ainda, o projeto Fronteira Tech, de 2019, um piloto de Cidades Inteligentes, que inclui sistema inteligente de controle, monitoramento e segurança, realizado em parceria pela Receita Federal e Instituto de Desenvolvimento Tecnológico. O projeto funciona de forma integrada com o banco de dados da Receita Federal e atua no controle aduaneiro na Ponte da Amizade, em Foz do Iguaçu (PR), na fronteira entre Brasil e Paraguai. Em setembro de 2021, o projeto foi implementado nas áreas de fronteira de Pacaraima, em Roraima (RR), na divisa do Brasil com a Venezuela.

Para o Instituto Brasileiro de Defesa do Consumidor (Idec), o uso de reconhecimento facial traz riscos práticas abusivas, discriminação e invasão de privacidade. No campo da discriminação, há o chamado "viés algorítmico", i.e., a reprodução de padrões discriminatórios nos resultados apresentados ou no uso feito pelos algoritmos. A discriminação por algoritmos pode levar a práticas discriminatórias (negação de serviços, distinção de preços), tecnologias essenciais que não funcionam bem com toda a população (autenticação facial de pessoas negras, por exemplo), e outros problemas potenciais.

O conjunto de tecnologias empregadas nas *smart cities*, como *Big Data*, IoT, inteligência artificial, reconhecimento facial, utilizadas pelos sistemas de crédito social e monitoramento de pessoas caracteriza Estado de vigilância. O uso dessas tecnologias sem efetiva proteção enseja a construção de sistemas políticos totais, com máximo controle e opressão.

4.6 PANOPTISMO E CIDADES INTELIGENTES

A relação entre privacidade, liberdade e autonomia se reflete em dois exemplos clássicos: o Panóptico de Bentham e o *Big Brother* de Orwell.

O Panóptico surgiu como um modelo radial de prisão celular nos Estados Unidos da América do Norte por volta de 1800. Esse sistema consistia em um núcleo central de observação com visibilidade para todas as celas. A entrada de luz pelo lado externo das celas possibilitava que todos os movimentos de qualquer detento fossem monitorados por um único guarda. A genialidade do panóptico reside na capacidade de ver sem ser visto. Através de mecanismos que impedem os detentos de perceberem a presença do inspetor no posto de inspeção, as pessoas passam a sentir que estão constantemente sob observação ou, pelo menos, existe uma grande possibilidade de tal vigilância estar em curso.

Conforme Foucault (2002) destaca, o Panóptico se preocupa com a observação individualizada, a caracterização, a classificação e a organização analítica do objeto sob vigilância. O Panóptico é utilizado por Michel Foucault como um conceito filosófico para destacar e descrever os mecanismos de opressão e controle social característicos do mundo moderno. Nesse sentido, ele é mais do que um simples modelo de poder elevado à sua forma ideal; é uma representação de tecnologia política que pode e deve ser distinguida de qualquer uso específico.

Esse modelo clássico de vigilância recebeu aprimoramentos com base nas inovações tecnológicas, principalmente por meio das infraestruturas de tecnologias da informação. Esses avanços resultam na transformação da vigilância, que, além de evoluir quantitativamente, é enriquecida com o componente qualitativo dos dados, ultrapassando a mera ideia de vigilância digital para dar origem ao fenômeno da *surveillance*.

Algumas características do panoptismo estão presentes em cidades inteligentes, como a:

- Capacidade de influenciar o comportamento dos indivíduos;
- Aplicação ativa do poder com recursos humanos limitados e ao menor custo possível;
- Inversão na visibilidade da organização do espaço, aquele que vigia não é percebido pelos vigiados;

- São dispositivos arquitetônicos de vigilância que operam de forma automática.

Portanto, as cidades inteligentes podem ser um equivalente digital do Panóptico, onde a presença de um observador invisível mantém a ordem de forma mais eficiente do que a violência física. Com os avanços no processamento de dados, aprendizado automático e visão computacional, as câmeras de vigilância não apenas monitoram, mas também analisam emoções e comportamentos, ao mesmo tempo em que interpretam movimentos e intenções, assemelhando-se às distopias como “1984” de Orwell ou “Admirável Mundo Novo” de Aldous Huxley.

Na obra renomada de Orwell, “1984”, o Estado é retratado como um observador constante de todas as ações dos indivíduos, que acabam conformando-se aos desejos do Grande Irmão, influenciados pelo temor de buscar suas próprias identidades pessoais. A realidade da sociedade atual não está distante dessa perspectiva, uma vez que a capacidade de coleta e processamento de dados, juntamente com as tecnologias de vigilância, questionam a autonomia das pessoas, sendo a privacidade um elemento crucial nesse contexto.

Em “Admirável Mundo Novo,” escrito por Aldous Huxley e publicado em 1932, a reprodução humana é estritamente regulamentada em laboratórios, visando criar cidadãos conformes às normas da sociedade. O Estado exerce controle total sobre as vidas dos indivíduos, desde o nascimento até a morte, utilizando uma droga chamada “soma” para manter a população pacífica e satisfeita.

A sociedade retratada em “Admirável Mundo Novo” é fortemente hierarquizada, com diferentes castas condicionadas para desempenhar funções específicas. A busca pela estabilidade social e a eliminação de conflitos são prioridades, mesmo que isso signifique sacrificar a liberdade individual e a busca pelo conhecimento.

A obra aborda a questão do condicionamento social para manter a ordem e a conformidade. Nos sistemas de pontuações sociais contemporâneos, como os observados em alguns lugares, a conduta dos cidadãos é avaliada, e as pontuações podem influenciar o acesso a certos benefícios ou privilégios. Ambos exploram a ideia de recompensas e penalidades com base no comportamento social.

Como no exemplo Chinês, os sistemas de pontuações sociais refletem uma busca incessante por felicidade e bem-estar através do controle social e tecnológico.

Há uma tensão entre a garantia de estabilidade e conforto e a preservação da liberdade individual.

Esses exemplos são significativos para evidenciar que a privacidade vai além de seu valor pessoal ou da individualidade; ela é uma ferramenta essencial para a sociedade como um todo. A privacidade representa um interesse comum, público e coletivo. Uma sociedade se estrutura de maneira mais sólida quando a privacidade está presente. Sua transição do âmbito do direito privado para o público, especialmente em termos constitucionais, reforça a ideia de sua natureza como um bem comum a todos, desde sua origem histórica na concepção burguesa, onde se destaca como um dos pilares para o desenvolvimento das sociedades liberais.

Por isso, a tecnologia não é apenas um fator terceiro (externo) na surveillance, mas um componente próprio e, portanto, interno, das relações sociais cotidianas. Fato é que o fenômeno da *surveillance* é permanentemente renovado. Nesse passo, na medida em que a tecnologia é um fator determinante de uma cidade como *smart city*, a surveillance desenvolve-se em consonância e em linear velocidade, sendo aquela uma condição para a existência dessa.

De acordo com Morais, Saldanha e Pimentel (2021), no artigo “Estado de Direito e Tecnopoder”, discorre sobre as complexas relações entre tecnologia, vigilância digital e o conceito de tecnopoder, fornece um instrumental teórico fundamental para compreender as implicações jurídicas, sociais e éticas das tecnologias empregadas nas cidades inteligentes.

Segundo ele, a transição da sociedade disciplinar para a sociedade do êxtase comunicacional espelha o contexto das cidades inteligentes, onde a vigilância e o controle social se intensificam por meio do uso avançado de tecnologias digitais. A governança algorítmica e o advento do capitalismo digital-vigilante ressoam com as preocupações levantadas neste capítulo sobre o potencial das cidades inteligentes para promover um panoptismo digital, onde a vigilância se torna onipresente e onisciente, porém muitas vezes invisível aos olhos do cidadão.

Há uma ilusão quanto à autonomia e neutralidade da tecnologia, pois as decisões tecnológicas são profundamente humanas e refletem as intenções de quem as desenha e implementa. Assim, as cidades inteligentes, em seu ímpeto de otimização e eficiência, podem inadvertidamente perpetuar uma forma de controle social que vai além do físico, infiltrando-se nas dimensões mais privadas da existência humana.

Por isso, explora o conceito de tecnopoder, que seria, uma fusão entre tecnologia e as estruturas de poder, reflete uma nova dimensão de controle e vigilância que transcende as formas tradicionais de governança, situando-se na interseção entre a inovação tecnológica e o exercício do poder.

Nas palavras dos autores:

> O tecnopoder representa a estratégia de emprego dos distintos métodos cibernéticos de vigilância e monitoramento comportamental com o objetivo de controlar as ações humanas, de modo que O capitalismo de vigilância age por meio de assimetrias nunca antes vistas referentes ao conhecimento e ao poder que dele resulta (Morais; Saldanha; Pimentel 2021, p. 20).

Neste sentido, o tecnopoder não se manifesta apenas como uma extensão do poder estatal ou corporativo, mas como uma reconfiguração da própria base sobre a qual o poder é exercido e percebido na sociedade. Através do uso de tecnologias digitais avançadas, como a coleta massiva de dados, a análise preditiva e a inteligência artificial, o tecnopoder molda comportamentos, influencia decisões e redefine a noção de privacidade e autonomia individual.

A era da digitalização não apenas transformou as dinâmicas de controle e vigilância, mas também introduziu um paradigma onde a governança algorítmica se torna um vetor primordial de poder. Isso é particularmente relevante no contexto das cidades inteligentes, onde o potencial para monitoramento contínuo e análise comportamental se encontra ampliado pela infraestrutura tecnológica permeada no ambiente urbano.

A reflexão crítica sobre o tecnopoder implica reconhecer que as tecnologias implementadas nas cidades inteligentes carregam consigo não apenas o potencial para inovação e eficiência, mas também para uma intrusão sem precedentes na esfera privada dos indivíduos. Assim, a discussão sobre o tecnopoder exige uma análise cuidadosa dos mecanismos de regulação e fiscalização, como a LGPD, que buscam equilibrar os benefícios da inovação tecnológica com a proteção dos direitos fundamentais.

A implementação de tecnologias em cidades inteligentes não deve ocorrer sem uma consideração cuidadosa das implicações éticas e jurídicas, especialmente no que tange à privacidade e à proteção de dados pessoais. A Lei Geral de Proteção de Dados do Brasil surge, então, como um marco regulatório essencial para equilibrar os benefícios da inovação tecnológica com a proteção dos direitos fundamentais dos cidadãos.

5 O CASO DA CIDADE DO RECIFE

Ao investigar as implicações da tecnologia nas cidades inteligentes e na proteção de dados, é crucial considerar as reflexões de Evgeny Morozov (2011) em *'The Net Delusion*: *The Dark Side of Internet Freedom'*. Morozov adverte sobre o otimismo exagerado em relação ao papel da Internet e da tecnologia digital na promoção da liberdade e da democracia, argumentando que, sem a devida governança e salvaguardas, a mesma tecnologia que promete transparência e engajamento cívico pode também servir a fins autoritários e de vigilância.

Esse alerta é particularmente relevante ao contexto de cidades inteligentes, onde o tratamento e a gestão de dados devem ser equilibrados com a proteção da privacidade e liberdades individuais. Assim, ao analisar a cidade do Recife sob a ótica das cidades inteligentes, a obra de Morozov ressalta a necessidade de uma abordagem crítica que questione não apenas os benefícios, mas também os potenciais riscos que a implementação tecnológica pode acarretar para a governança urbana e a proteção dos dados pessoais.

Em '*To Save Everything, Click Here: The Folly of Technological Solutionism*', Morozov (2013) desafia a noção de que a tecnologia é uma solução onipotente para todos os problemas sociais e políticos. Esta crítica ao “solucionismo tecnológico” é especialmente relevante no contexto das cidades inteligentes, onde a coleta e análise massiva de dados são vistas como soluções para uma ampla gama de questões urbanas.

Morozov adverte contra a simplificação excessiva e a fé desmedida na tecnologia, argumentando que muitos desafios urbanos são intrinsecamente complexos e arraigados em contextos sociais, econômicos e políticos que não podem ser totalmente resolvidos por meio da tecnologia. Ao considerar a cidade do Recife e sua abordagem para cidades inteligentes e proteção de dados, os *insights* de Morozov incentivam uma avaliação crítica sobre a eficácia e as limitações das soluções tecnológicas, enfatizando a importância de abordagens holísticas e contextualizadas que levem em conta a complexidade dos problemas urbanos.

O tecno-otimismo e a suposta capacidade da tecnologia de resolver questões complexas de governança e privacidade. exigem um entendimento crítico das implicações políticas e sociais da tecnologia, soluções baseadas exclusivamente em inovações digitais podem falhar em abordar as nuances da vida urbana e os desafios

da proteção de dados. Portanto, ao analisar a efetividade da LGPD no contexto de Recife, deve-se ponderar um enquadramento crítico que vá além da mera implementação tecnológica e considere as dinâmicas políticas e sociais que moldam as cidades inteligentes.

Nelson Saldanha, em ‘O Jardim e a Praça’, oferece uma valiosa perspectiva sobre a relação entre o espaço privado (jardim) e o espaço público (praça), bem como a interação entre o indivíduo e a comunidade. Sobre cidades inteligentes e proteção de dados, especialmente no contexto do Recife, é possível estabelecer um paralelo com as reflexões de Saldanha para discutir como a tecnologia afeta a distinção entre os espaços privados e públicos e, consequentemente, a privacidade dos indivíduos. A implementação de tecnologias em cidades inteligentes, como sensores e câmeras de vigilância, pode obscurecer as fronteiras entre o que é privado e o que é público, transformando potencialmente “jardins” individuais em “praças” acessíveis, isto é, a relação entre espaços privados e públicos.

Em cidades inteligentes, a coleta massiva de dados pode transformar espaços anteriormente considerados privados em domínios públicos, desafiando assim as noções tradicionais de privacidade e consentimento.

O caso da cidade do Recife exemplifica essa transição, onde tecnologias de monitoramento e coleta de dados integram o tecido urbano, afetando a autonomia individual e a privacidade dos cidadãos. Ao adotar a perspectiva de Saldanha, é importante estabelecer mecanismos regulatórios e éticos que preservem a distinção entre o jardim (privacidade individual) e a praça (espaço público), garantindo assim que as inovações tecnológicas em cidades inteligentes não comprometam os direitos fundamentais dos indivíduos.

É o que se faz a seguir.

5.1 BREVES COMENTÁRIOS SOBRE A URBANIZAÇÃO DA CIDADE DO RECIFE

A história da urbanização da cidade do Recife é marcada por uma evolução significativa ao longo dos séculos, influenciada por diversos fatores históricos, sociais e econômicos. A tecnologia desempenhou um papel crucial nesse processo, moldando a configuração urbana e melhorando a qualidade de vida dos habitantes.

No século XVI, Olinda desempenhava o papel central na Capitania de Pernambuco. Contudo, a saída para o oceano estava situada ao sul, onde um porto natural formado por recifes servia como ponto de ancoragem. Sua função principal era exportar o açúcar produzido nos engenhos que ocupavam as planícies dos rios Capibaribe e Beberibe.

Devido a essa atividade portuária, um povoado surgiu na Ilha do Recife, originalmente conhecida como Povoação dos Arrecifes ou Ribeira Marinha dos Arrecifes, hoje denominada Bairro do Recife. Isto porque, conforme dados fornecidos pelo IBGE sobre a origem histórica da cidade, a cidade denominada Recife demonstrou condições propícias para abrigar um porto destinado ao recebimento e envio de mercadorias (IBGE, 2014).

O surgimento de Recife ocorre a partir de um pequeno grupo de marinheiros, carregadores e pescadores que, por volta de 1548, estabeleceram-se nas proximidades dos rios Capibaribe e Beberibe, próximos à vila de Olinda, que naquela época era a sede da capitania de Pernambuco. A cidade permaneceu sob domínio português até a independência do Brasil.

Entre 1630 e 1645, como é conhecido, os holandeses ocuparam a Capitania de Pernambuco, introduzindo um viés mais urbanizado à colonização. Conforme Reynaldo e Alves (2013), a ocupação do Recife efetivamente começa no século XVII. Na época de 1630, Olinda, a capital da Capitania de Pernambuco, era uma cidade com aproximadamente 5.000 residentes, enquanto o Recife, apesar dos 130 anos de presença portuguesa, apresentava apenas uma estrutura urbana incipiente, com destaque para um porto natural usado para o envio de açúcar para o continente europeu.

Assim que assumiu o controle do Recife, o governo holandês implementou melhorias no porto e estabeleceu um plano urbanístico que ampliou a ocupação para a Ilha de Santo Antônio, com a preocupação de conectar esta ilha à Ilha do Recife e à “margem” da Boa Vista, “criando, desse modo, novas vias sobre o rio, incluindo duas pontes” (Menezes, 1999, p. 218). Dessa maneira, a Cidade Maurícia, sob a liderança do Conde Maurício de Nassau, foi se desenvolvendo seguindo os padrões holandeses.

Nas palavras de Reynaldo e Alves (2013):

> O Recife cresce rapidamente pela presença do porto, pelo movimento gerado pelas tropas invasoras e pela transferência de parte da população de Olinda

> para este núcleo. A ocupação holandesa se expande sobre o istmo, seguindo as mesmas diretrizes do traçado português, ocupando os terrenos vazios entre o mar e o rio. Nos estreitos lotes de reduzidas quadras longitudinais e paralelas entre si, são erguidos os sobrados, apoiando-se, muitas vezes, sobre uma antiga construção portuguesa, ganhando em altura o que lhe falta de solo.

Durante esse tempo, as riquezas coloniais começaram a se multiplicar. Elas não se baseavam apenas na agricultura e pecuária, mas também em investimentos na construção de residências, armazéns e instalações administrativas no centro urbano.

Ao longo do século XIX, a cidade já era um dos principais polos de produção artística e cultural no Nordeste, destacando-se especialmente na área da música. Adicionalmente, a cidade é notoriamente reconhecida como um hub universitário e de geração de conhecimento.

Conforme Lacerda e Fernandes (2015):

> Conquanto o Bairro do Recife, no início do século XX, concentrasse o comércio açucareiro e as grandes firmas importadoras, era visto como um espaço degradado. Diante de realidades distintas – degradação e importância econômica –, esse bairro foi contemplado, no âmbito do projeto nacional de modernização do País, no início dos anos 1900, recebendo melhorias na sua infraestrutura portuária (Projeto de Melhoramentos do Porto do Recife) e sanitária (Plano de Saneamento do Recife, de autoria de Saturnino de Brito).

Reynaldo e Alves (2013) revelam que, na década de 1840, começou um processo de modernização e expansão da antiga cidade colonial, visando adequá-la às exigências do considerável aumento populacional e econômico. Esse desenvolvimento demandou a construção de instalações públicas, provisão de serviços urbanos, como transporte público, sistemas de abastecimento de água e esgoto, formulação de regulamentos de construção e planejamento viário, resultando em significativas intervenções durante o período.

Segundo os mesmos autores, a rede de transporte coletivo de tração animal foi criada pelo inglês Tomas Sayle e operou entre 1840 e 1914, cobrindo uma extensão de apenas 20 quilômetros e conectando os bairros do Recife, Santo Antônio, São José e Boa Vista a alguns pontos de interesse público, como o Cemitério de Santo Amaro, os hospitais D. Pedro II e Santo Amaro, e a Corrida Lucas, além das urbanizações de Afogados e Aflitos.

A tecnologia desempenhou um papel crucial na expansão urbana do Recife. No final do século XIX, o transporte coletivo urbano, como bondes de tração animal e

trens urbanos, começou a articular a cidade com suas áreas suburbanas e rurais, facilitando a mobilidade da população. Mais tarde, a introdução do bonde elétrico em 1914 representou um avanço tecnológico significativo, substituindo métodos de tração animal e melhorando a eficiência do transporte público. (Reynaldo; Alves, 2013).

A comunicação interna da cidade, originada no recinto portuário, percorria as ruas de Santo Antônio e São José, alcançando os antigos caminhos rurais e abrangendo as áreas de crescimento periférico. Gradualmente, a partir de 1914, a rede foi expandida, ampliando a conexão entre os diferentes territórios. Em 1932, um território periférico com cerca de 10 quilômetros de raio estava conectado por meio da rede de transporte coletivo ao recinto portuário. (Reynaldo; Alves, 2013).

Nas décadas de 1980 e 1990, a administração municipal do Recife implementou diversos planos com o intuito de reabilitar e revitalizar o Centro Histórico. No entanto, essas intervenções não foram sustentáveis ao longo do tempo. Somente em 2000, o Governo do Estado concebeu e executou o Porto Digital, um parque tecnológico destinado a atrair investimentos na área de tecnologia da informação, com o objetivo de impulsionar o desenvolvimento econômico e a requalificação urbana do bairro do Recife.

O projeto foi desenvolvido em parceria com o Centro de Informática da Universidade Federal de Pernambuco. O segundo critério foi resultado da visão dos fundadores, que viram na área tecnológica, ainda incipiente naquela época, uma oportunidade econômica, enquanto outros estados do Nordeste focavam em clusters de produção de grãos, frutas tropicais e turismo.

O Parque, que teve sua abertura no Recife no ano 2000 como parte do impulso às políticas públicas estaduais para as Tecnologias da Informação e Comunicação, está fundamentado nos pilares da Academia, Mercado e Governo. Aproximadamente R$ 44 milhões são alocados nesse empreendimento (Marques; Leite, 2008). No entanto, a concepção desse projeto remonta a 1990, quando foram implementadas iniciativas públicas voltadas para o avanço econômico do Estado, resultando na transformação do entorno em um bairro criativo por meio da mencionada tecnologia.

Na página de Ciência, tecnologia e inovação da Prefeitura do Recife (https://desenvolvimentoeconomico.recife.pe.gov.br/ciencia-tecnologia-e-inovacao), são destacadas as iniciativas para “articular o setor produtivo com o sistema de ciência, tecnologia e inovação”, através de ações para implementar iniciativas de

impacto que possam transformar Recife em uma *smart city* competitiva internacionalmente, integrando empreendimentos privados com a academia, o terceiro setor e o poder público.

A mesma página afirma que:

> A cidade promove tanto ações de difusão tecnológica (como o Programa Salto Tecnológico), quanto atividades de promoção da inovação. Nessa área, o Recife tem um dos mais diversificados programas de inovação aberta do país, contemplando desafios públicos, hackathons, sandbox regulatório no ambiente experimental da cidade e o Escritório de Parcerias Inovadoras com as universidades para estimular empreendedorismo tecnológico, propriedade intelectual e licenciamento e exploração de tecnologias.

5.2 ANÁLISE CRÍTICA DOS MARCOS LEGAIS MUNICIPAIS RELACIONADOS À *SMART CITY* E PROTEÇÃO DE DADOS

Dentre os elementos dessa iniciativa, o Município destaca o Marco Legal – Ciência, Tecnologia e Inovação, Lei Municipal n.º 18.974, de 31 de agosto de 2022, que dispõe sobre incentivos às atividades de ciência, tecnologia e inovação no Recife, a Inovação Aberta, EITA! Recife (Desafios públicos), EITA Labs (Sandbox regulatório), Programa de Incentivo Fiscal ao Porto Digital.

Quanto à inovação aberta, informa que:

> As iniciativas de inovação aberta visam promover a mobilização da comunidade local para o desenvolvimento de soluções inovadoras e criativas para os desafios da cidade, mediante realização de hackathons, encomendas tecnológicas, concursos e premiações. Trata-se de uma forma de atuação colaborativa entre poder público, cidadãos, fornecedores, empresas de tecnologia e institutos de pesquisa, para propor soluções digitais para demandas internas e externas à Prefeitura.

Sobre o EITA! Recife (Desafios públicos), define-se como:

> Programa que identifica desafios da cidade do Recife e cria um ambiente propício para realizar conexões capazes de implementar soluções inovadoras. O projeto está atrelado a Esquadrão de Inovação e Transformação Aberta, EITA. A iniciativa visa a obtenção de soluções inovadoras para desafios da cidade do Recife, órgão que tem como principal função servir ao cidadão. O processo seguirá os princípios da Inovação Aberta, contemplando três macro fases: desafios públicos, prototipagem e desenvolvimento de produto mínimo viável (MVP), em um período de aproximadamente 6 (seis) meses.

O EITA Labs (Sandbox regulatório) é:

> O Living Labs Recife, apelidado de EITA Labs, é mais uma iniciativa do E.I.T.A! Recife. Tem como principal objetivo criar um ambiente de experimentação, onde teremos um cenário de laboratório vivo,

> desburocratizando e permitindo ações de inovações que possam ser testadas e construídas com participação ativa dos atores da região e fora dela. O EITA Labs permitirá que o Recife se torne uma cidade aberta e conectada, por meio de cocriações de espaços públicos, possibilitando experimentações de soluções inovadoras a partir de uma rede conectada que busca impacto social, bem-estar e soluções digitais.

O EITA Labs é regulamentado pelo Decreto n.º 35.511/02/04/2022, que regulamenta a instituição de ambientes experimentais de inovação científica, tecnológica, urbanística e empreendedora, sob o formato de bancos de testes regulatórios e tecnológicos – “Eita Labs”. Ele é regulamentado pelo Decreto n.º 35.511, de 02/04/2022, que regulamenta a instituição de ambientes experimentais de inovação científica, tecnológica, urbanística e empreendedora, sob o formato de bancos de testes regulatórios e tecnológicos – “Eita Labs”.

Em 2022, foi editado o Decreto 35583/2022, o qual institui a Política Municipal de Proteção de Dados Pessoais do Poder Executivo Municipal, em consonância com a Lei Federal n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais, o qual tem como justificativa o fato de os dados pessoais integrarem o âmbito de proteção dos direitos fundamentais de liberdade, de privacidade, de intimidade e do livre desenvolvimento da personalidade da pessoa natural ou jurídica.

O Decreto reproduz, em seu art. 1º, o art. 6º da LGPD, enumerando os princípios da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. No seu art. 4º, o Decreto reproduz os conceitos trazidos pela LGPD no art. 5º.

Inova ao dispor as diretrizes da Política Municipal de Proteção de Dados Pessoais, quais sejam:

> I – as regras de boas práticas e governança estabelecidas pelo controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular; II – o atendimento simplificado e eletrônico das demandas do cidadão; III – o alinhamento e o equilíbrio com a promoção da transparência pública, em específico com a Lei Municipal nº 17.866, de 15 de maio de 2013; IV – o estabelecimento da proporcionalidade das medidas acerca de proteção de dados, privacidade e segurança da informação; V – o desenvolvimento do nível de maturidade dos tratamentos dos dados; VI – a manutenção da segurança jurídica dos instrumentos firmados; VII – a economicidade das ações; VIII – o alinhamento ao planejamento estratégico do Município;

Também tem redação própria o art. 4º do Decreto, inserto no capítulo II “Das Responsabilidades”, segundo o qual:

> A Administração Pública Municipal Direta e Indireta, nos termos da Lei Federal nº 13.709, de 14 de agosto de 2018, deve realizar e manter continuamente atualizados: I – o mapeamento dos dados pessoais existentes e dos fluxos de dados pessoais em suas unidades; II – a análise de risco; III – o plano de adequação, observadas as exigências constantes em norma específica; IV – o relatório de impacto à proteção de dados pessoais, quando solicitado. Parágrafo único. Para fins do inciso III, deste artigo, as unidades da Administração Pública Direta e Indireta do Município devem observar as diretrizes editadas pelo Conselho Gestor de Proteção de Dados Pessoais – CGPDP de que trata o art. 5º deste Decreto.

Referido Decreto, ainda, cria o Conselho Gestor de Proteção de Dados Pessoais – CGPDP, composto pelos Titulares dos seguintes órgãos: I – Secretaria de Planejamento, Gestão e Transformação Digital, que o presidirá; II – Controladoria-Geral do Município; III – Procuradoria-Geral do Município; IV – Secretaria de Governo e Participação Social; V – Empresa Municipal de Informática – EMPREL, bem como discrimina as competências e deveres de cada um desses órgãos no que se refere à proteção de dados.

No mesmo ano, foi editada a Lei Municipal n.º 18.974/2022, que dispõe sobre incentivos às atividades de ciência, tecnologia e inovação no Recife. No seu art. 1º, informa-se que o diploma legal

> Regulamenta o art. 218 da Constituição Federal e disciplina o incentivo às atividades de ciência, tecnologia e inovação na Cidade do Recife, com o objetivo de superar desafios científicos e tecnológicos concretos da realidade recifense por meio de articulação entre o Poder Executivo municipal, Instituições Científicas, Tecnológicas e de Inovação – ICTs, entidades privadas sem fins lucrativos e o setor produtivo.

O art. 2º prevê os instrumentos da política de ciência, tecnologia e inovação no âmbito municipal, quais sejam:

> I – encomenda tecnológica; II – desafio público; III – contratação pública para solução inovadora (CPSI); IV – bônus tecnológico; V – bolsa de estímulo à inovação no ambiente produtivo, para pesquisador, para atividades de extensão tecnológica, para proteção da propriedade intelectual, ou para transferência de tecnologia; VI – incentivos ao inventor independente; VII – estímulo à formação de ambientes promotores de inovação; VIII – acordos de parceria para pesquisa, desenvolvimento e inovação; IX – termos de colaboração ou de fomento de pesquisa, desenvolvimento e inovação; X – programa de ambiente regulatório experimental (sandbox regulatório), incluindo laboratórios abertos (living labs); XI – promoção e divulgação de pesquisas e tecnologias desenvolvidas localmente (vitrine tecnológica); XII – programas de investimento em pesquisa e desenvolvimento em contratos de concessão ou permissão de serviços públicos ou em regulações setoriais; XIII

> – transferência de tecnologia; XIV – Programa de Incentivo ao Porto Digital; XV – estímulo à inovação nas empresas do Recife; e XVI – Prêmio Recife de Inovação.

Ao que interessa ao presente trabalho, por se tratarem da relação entre dados colhidos publicamente e instituições privadas, destacam-se os instrumentos de encomenda tecnológica; contratação pública para solução inovadora (CPSI); acordos de parceria para pesquisa, desenvolvimento e inovação; termos de colaboração ou de fomento de pesquisa, desenvolvimento e inovação; programa de ambiente regulatório experimental (*sandbox* regulatório), incluindo laboratórios abertos (*living labs*); promoção e divulgação de pesquisas e tecnologias desenvolvidas localmente (vitrine tecnológica); programas de investimento em pesquisa e desenvolvimento em contratos de concessão ou permissão de serviços públicos ou em regulações setoriais; transferência de tecnologia; Programa de Incentivo ao Porto Digital; estímulo à inovação nas empresas do Recife.

O Capítulo II da Lei trata da Encomenda Tecnológica, segundo o qual

> órgãos e as entidades da Administração Pública Municipal poderão contratar diretamente ICT pública ou privada, entidades de direito privado sem fins lucrativos ou empresas, isoladamente ou em consórcio, voltadas para atividades de pesquisa e de reconhecida capacitação tecnológica no setor, com vistas à realização de atividades de pesquisa, desenvolvimento e inovação que envolvam risco tecnológico, para solução de problema técnico específico ou obtenção de produto, serviço, design ou processo inovador.

A legislação prevê diversas exigências para contratação, mas não estabelece nenhum requisito de priorização da privacidade desde a concepção (PdC) e avaliações de impacto da privacidade. Na verdade, em nenhum trecho é citada a palavra privacidade, consentimento ou proteção de dados. Tampouco se regula como os dados obtidos por empresas privadas devem ser tratados.

O art. 3º da Lei apenas conceitua entidades, públicas ou privadas voltadas para atividades de pesquisa como aquelas com ou sem fins lucrativos, que tenham experiência na realização de atividades de pesquisa, desenvolvimento e inovação, dispensadas as seguintes exigências. Exige, ainda, que contratada se dedique, exclusivamente, às atividades de pesquisa.

Prevê, no § 2º que, na contratação da encomenda, poderão ser incluídos os custos das atividades que precedem a introdução da solução, do produto, do serviço ou do processo inovador no mercado, dentre as quais, I – a fabricação de protótipos; II – o escalonamento, como planta piloto para prova de conceito, testes e

demonstração; e III – a construção da primeira planta em escala comercial. Nesse dispositivo poderia ser prescrita a exigência de que o projeto incluísse privacidade desde a concepção (PdC) e avaliações de impacto da privacidade, abarcando os custos dessa avaliação.

A privacidade desde a concepção (PdC) ou *Privacy by Design* incentiva a antecipação de potenciais riscos à privacidade durante o estágio de design, em vez de reagir a incidentes após sua ocorrência. É necessário exigir do agente privado Padrões de Privacidade, i.e., a integração de padrões e princípios de privacidade diretamente nas práticas e sistemas, buscando garantir que a privacidade seja uma parte intrínseca da solução.

Também deveria a lei ter previsto a exigência de adoção de mecanismos de consentimento informado, a fim de garantir que os usuários tenham informações claras sobre como seus dados serão utilizados, dando-lhes a oportunidade de consentir ou recusar.

A lei não prevê a segurança por padrão, não exige, expressamente, a adoção de práticas seguras desde o início para proteger as informações pessoais. Tais medidas são essenciais para promover a transparência no tratamento de dados pessoais e proporcionar aos usuários maior controle sobre suas informações.

O §5º do art. 3º dispõe que § 5º órgão ou a entidade da Administração Pública Municipal contratante poderá criar, por meio de ato de sua autoridade máxima, comitê técnico de especialistas para assessorar a instituição na definição do objeto da encomenda, na escolha do futuro contratado, no monitoramento da execução contratual e nas demais funções previstas nesta Lei. Por fim, destaca que os membros do comitê técnico deverão assinar declaração de que não possuem conflito de interesse na realização da atividade de assessoria técnica ao contratante; e que a participação no comitê técnico será considerada prestação de serviço público relevante, não remunerada.

Mais uma vez, o legislador perdeu a oportunidade de ter a privacidade como norte regulatório da relação entre tecnologia e gestão municipal. Poderia ter incluído nas atribuições do comitê técnico a avaliação e fiscalização da proteção de dados dos cidadãos recifenses em relação aos contratos firmados.

O § 8º do mesmo art. 3º prevê que “I – a negociação será transparente, com documentação pertinente anexada aos autos do processo de contratação, ressalvadas eventuais informações de natureza industrial, tecnológica ou comercial

que devam ser mantidas sob sigilo". Na redação da Lei, deveria o legislador ressalvar que não pode ser objeto de sigilo os mecanismos adotados pelo contratado para preservação da privacidade dos cidadãos e anonimização dos dados coletados.

O art. 4º, § 2º prevê as hipóteses de rescisão contratual, quais sejam: I – por ato unilateral dos órgãos e das entidades da Administração Pública Municipal; ou II – por acordo entre as partes. Seria o caso, também, de impor à administração a obrigatoriedade de rescisão no caso de violação à privacidade, impedindo a discricionariedade do administrador e evitando que o direito fundamental à proteção de dados esteja sujeito aos meandros da política ou mesmo da corrupção, considerando o alto valor econômico que possuem os dados na economia informacional.

O Capítulo IV trata da Contratação Pública para Solução Inovadora. O art. 10 da Lei permite que órgãos e as entidades da Administração Pública Municipal poderão contratem pessoas físicas ou jurídicas, isoladamente ou em consórcio, para o teste de soluções inovadoras por elas desenvolvidas ou a serem desenvolvidas, com ou sem risco tecnológico, por meio de licitação na modalidade especial, nos termos dos arts. 12 e 13 da Lei Complementar n.º 182.

Mais uma vez, nada se fala sobre proteção de dados ou privacidade. É óbvio que para que o contratado ou licitante possa desenvolver as soluções necessárias à administração precisa acessar dados da população, os quais não necessariamente serão públicos. O legislador precisa prever a quem cabe o processo de anonimização dos dados, se à administração ou ao contratado/licitante, bem como a forma de tratamento, inclusive nos casos em que a anonimização não for possível ou impeditiva da execução do objeto do contrato.

O capítulo IX regula o Acordo de Parceria para Pesquisa, Desenvolvimento e Inovação. No art. 18, a Lei permite aos órgãos e as entidades da Administração Pública Municipal, ICT's e instituições privadas celebrar acordo de parceria para pesquisa, desenvolvimento e inovação, a fim de realizar atividades conjuntas de pesquisa científica e tecnológica e de desenvolvimento de tecnologia, produto, serviço ou processo, sem transferência de recursos financeiros públicos para o parceiro privado.

A hipótese é bastante curiosa, posto que nenhum ator privado iria realizar uma parceria dessas de forma gratuita, sem receber nenhum bônus ou lucro, porque faz parte da lógica capitalista a necessidade de receita para manutenção da instituição.

Considerando o alto valor econômico dos dados coletados pela Administração Pública, o dispositivo pode ser um gargalo para mineração desses dados por instituições privadas, sobretudo porque, como dito anteriormente, a Lei não cita, em nenhum momento, mecanismos de proteção de dados, ficando a cargo da LGPD regular a questão.

O §1º do art. 18 prevê que:

> § 1º A celebração do acordo de parceria para pesquisa, desenvolvimento e inovação deverá ser precedida da negociação entre os parceiros do plano de trabalho, do qual deverá constar obrigatoriamente: I – a descrição das atividades conjuntas a serem executadas, de maneira a assegurar discricionariedade aos parceiros para exercer as atividades com vistas ao atingimento dos resultados pretendidos; II – a estipulação das metas a serem atingidas e os prazos previstos para execução, além dos parâmetros a serem utilizados para a aferição do cumprimento das metas, considerados os riscos inerentes aos projetos de pesquisa, desenvolvimento e inovação; III – a descrição, nos termos estabelecidos no § 3º, dos meios a serem empregados pelos parceiros; e IV – a previsão da concessão de bolsas, quando couber, nos termos estabelecidos no § 4º (Brasil, 2018).

Mais uma vez, seria o caso de obrigar o parceiro privado a prevê, no seu plano de trabalho, a instituição da privacidade desde a concepção (PdC) e avaliações de impacto da privacidade.

O § 6º do art. 18 prevê que o acordo de parceria para pesquisa, desenvolvimento e inovação poderá prever a transferência de recursos financeiros dos parceiros privados para os parceiros públicos, inclusive por meio de fundação de apoio, para a consecução das atividades previstas nesta Lei. É necessário dispor que, em hipótese alguma, o agente privado poderá “comprar”, através dessa transferência de recursos, o acesso aos dados coletados pela administração.

O capítulo X trata do Termo de Colaboração e do Termo de Fomento ara Pesquisa, Desenvolvimento e. Inovação, que são o instrumento jurídico celebrado entre os órgãos e as entidades da Administração Pública Municipal e as ICT públicas e privadas para execução de projetos de pesquisa, desenvolvimento e inovação, com transferência de recursos financeiros públicos (art. 21).

O art. 23 da Lei prevê as hipóteses de impedimento para celebração de colaboração ou termo de fomento para pesquisa, desenvolvimento e inovação a ICT privada. Em nenhuma delas está o impedimento no caso de vazamento, mineração de dados ou qualquer violação à privacidade.

O art. 24, que trata dos requisitos para a celebração do termo de colaboração ou do termo de fomento para pesquisa, desenvolvimento e inovação, também não prevê que a instituição privada apresente, no projeto, formas privacidade desde a concepção (PdC) e avaliações de impacto da privacidade. O mesmo acontece no art. 26, que trata do plano de trabalho do termo de colaboração ou termo de fomento de pesquisa. Nesse dispositivo deveria estar previsto, obrigatoriamente, que o projeto adotasse o PdC, avaliações de impacto da privacidade e mecanismos de consentimento Informado, esse último, sempre que possível e, quando não possível, que exigisse a anonimização dos dados.

O art. 27 vale ser transcrito na íntegra, dispõe que:

> Art. 27. A administração pública adotará medidas para promover a boa gestão dos recursos transferidos, entre as quais serão obrigatórias: I – a divulgação da lista completa dos projetos apoiados, de seus responsáveis e dos valores desembolsados; II – a divulgação de canal para denúncia de irregularidades, de fraudes ou de desperdício de recursos no seu sítio eletrônico oficial; III – a definição de equipe ou estrutura administrativa com capacidade de apurar eventuais denúncias; e IV – a exigência de que os participantes do projeto assinem documento do qual constem informações sobre como fazer denúncias, sobre o canal existente no sítio eletrônico da concedente e sobre a importância da integridade na aplicação dos recursos.

Conforme exposto na seção 4, a proteção da privacidade não é apenas um mandamento negativo perante o Estado, mas um comando constitucional positivo, o Estado tem a obrigação de atuar para garantir a privacidade dos cidadãos. Percebe-se que a Lei se preocupou apenas no aspecto orçamentário das contratações de tecnologia e inovação, mas não se preocupou com a privacidade em momento algum. Mesmo sob o aspecto econômico, ponto central desse dispositivo, não se atentou que os dados podem se transformar em mercadoria, conduta que precisa ser regulada e, sempre que possível, evitada.

O art. 28 dispõe que o parceiro privado terá responsabilidade exclusiva pelo gerenciamento administrativo e financeiro dos recursos recebidos, inclusive quanto às despesas de custeio, de investimento e de pessoal, e pelo pagamento dos encargos trabalhistas, previdenciários, fiscais e comerciais relacionados à execução do objeto previsto no termo de colaboração ou termo de fomento para pesquisa, desenvolvimento e inovação, hipótese em que a inadimplência do parceiro privado em relação ao referido pagamento não implicará responsabilidade solidária ou subsidiária da Administração Pública.

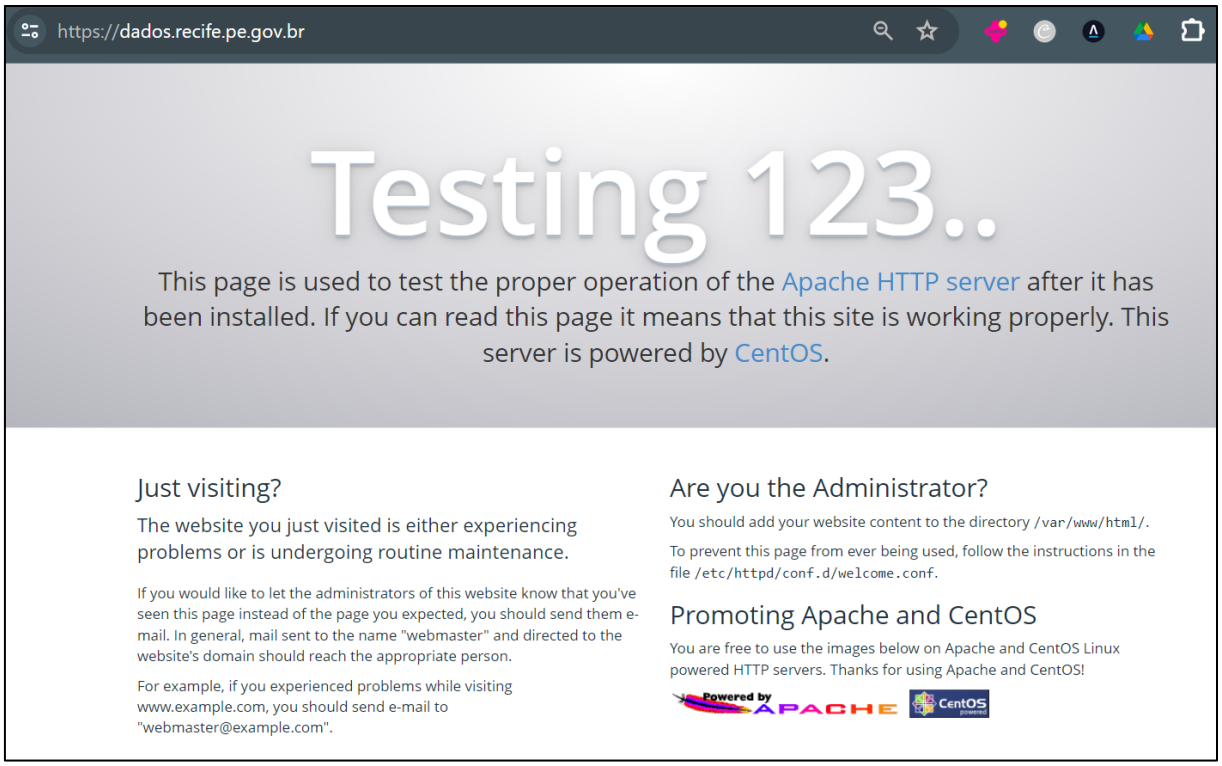
Mais uma vez, o legislador perdeu a oportunidade de regular de quem é a responsabilidade pelo tratamento dos dados dos cidadãos fornecidos ou coletados pelo Município ou pelo setor privado.

Portanto, nota-se que a legislação municipal não enfrenta dois problemas essenciais: 1) como o agente privado trata os dados fornecidos pela própria administração; 2) como o agente privado trata os dados coletados em razão do objeto de sua contratação/parceria.

5.3 A AUSÊNCIA DE DADOS ABERTOS NO MUNICÍPIO DE RECIFE

Em 22/12/2023, data da última tentativa de acesso, o site onde deveriam constar os dados abertos do Municípios estava fora do ar. Veja-se tela:

Figura 1 – Captura de tela



Fonte: Acervo pessoal (2023).

Também foram acessados todos os links disponíveis no endereço https://www2.recife.pe.gov.br/servico/dados-abertos, quais sejam: https://dados.recife.pe.gov.br/dataset, https://dados.recife.pe.gov.br/organization, https://dados.recife.pe.gov.br/group, https://dados.recife.pe.gov.br/, e todos estavam fora do ar.

Para Rezende *et al.* (2019), a ausência de dados abertos no Município afeta a transparência e confiança da administração. Disponibilizar dados de forma aberta permite transparência às cidades inteligentes, garantindo aos cidadãos que vejam e entendam como os dados são coletados, processados e utilizados.

Nesse sentido, garante-se empoderamento dos cidadãos, os quais poderiam acessar informações relevantes sobre a cidade, possibilitando uma participação mais ativa e informada na vida comunitária e na tomada de decisões e, consequentemente, estimulando a inovação ao fornecer a empreendedores e desenvolvedores que poderiam criar novos serviços, produtos e soluções que beneficiem a cidade e seus habitantes.

No cenário brasileiro, várias normas pautam a abertura dos dados governamentais. O Portal Brasileiro de Dados Abertos afirma que todo dado público tem vocação para ser dado aberto. Assim, como praticamente todo dado governamental é público, é fundamental que os governos implementem políticas para disponibilizá-los (Brasil, 2024).

Nesse sentido, estabelece a CRFB/88:

> Art. 5º, XXXIII: todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado;
> Art. 5º, LXXII – conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de 14 entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo (Brasil, 1988).

Em 1991, a Lei n.º 8.159 dispõe sobre a política nacional de arquivos públicos e privados estabelece, em seu 4º artigo, que:

> todos têm direito a receber dos órgãos públicos informações de seu interesse particular ou de interesse coletivo ou geral, contidas em documentos de arquivos, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujos sigilo seja imprescindível à segurança da sociedade e do Estado, bem como à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas (Brasil, 1991).

A Lei de Acesso à Informação (LAI) n.º 12.527 de 2011, dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações provenientes de suas entidades controladas direta ou indiretamente. Considera-se o principal marco legal

brasileiro a regulamentar a abertura de dados públicos provenientes de órgãos governamentais (Brasil, 2011). Leia-se os dispositivos pertinentes:

> Art. 2º: Aplicam-se as disposições desta Lei, no que couber, às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres.
>
> Art. 3º: Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública.
>
> Art. 4º: Para os efeitos desta Lei, considera-se: I – informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato; II – documento: unidade de registro de informações, qualquer que seja o suporte ou formato; III – informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; IV – informação pessoal: aquela relacionada à pessoa natural identificada ou identificável; V – tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; VI – disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados; VII – autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema; 15 VIII – integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino; IX – primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.
>
> Art. 5º: É dever do Estado garantir o direito de acesso à informação, que será franqueada, mediante procedimentos objetivos e ágeis, de forma transparente, clara e em linguagem de fácil compreensão.
>
> Art. 7º : O acesso à informação previsto nesta normativa não compreende as informações referentes a projetos de pesquisa e desenvolvimento científicos ou tecnológicos cujo sigilo seja imprescindível à segurança da sociedade e do Estado.
>
> Art. 8º: É dever dos órgãos e entidades públicas promover, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas.
>
> Art. 9º: O acesso a informações públicas será assegurado mediante: I – criação de serviço de informações ao cidadão, nos órgãos e entidades do poder público, em local com condições apropriadas

> Art. 10º: Qualquer interessado poderá apresentar pedido de acesso a informações
>
> Art. 11: O órgão ou entidade pública deverá autorizar ou conceder o acesso imediato à informação disponível.
>
> Art.12: O serviço de busca e fornecimento da informação é gratuito.
>
> Art. 13: Quando se tratar de acesso à informação contida em documento cuja manipulação possa prejudicar sua integridade, deverá ser oferecida a consulta de cópia, com certificação de que esta confere com o original.
>
> Art. 14: É direito do requerente obter o inteiro teor de decisão de negativa de acesso, por certidão ou cópia.
>
> Art. 31: O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: II – poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. § 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias: II – à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;
>
> Art. 32: Constituem condutas ilícitas que ensejam responsabilidade do agente público ou militar: I – recusar-se a fornecer informação requerida nos termos desta Lei, retardar deliberadamente o seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa; II – utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública; IV – divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal (Brasil, 2011).

Complementando as condições essenciais para a democratização do acesso às informações públicas geradas por entidades governamentais, o Decreto n.º 8.638/2016 institui a Política de Governança Digital no âmbito dos órgãos e das entidades da Administração Pública federal direta, autárquica e fundacional (Brasil, 2016).

O art. 1º decreta que fica instituída a Política de Governança Digital para os órgãos e as entidades da Administração Pública federal direta, autárquica e fundacional, com as seguintes finalidades:

> I – gerar benefícios para a sociedade mediante o uso da informação e dos recursos de tecnologia da informação e comunicação na prestação de

> serviços públicos; II – estimular a participação da sociedade na formulação, na implementação, no monitoramento e na avaliação das políticas públicas e dos serviços públicos disponibilizados em meio digital; III – assegurar a obtenção de informações pela sociedade, observadas as restrições legalmente previstas (Brasil, 2016).

O art. 3º afirma que a Política de Governança Digital observará os seguintes princípios:

> I – foco nas necessidades da sociedade; II – abertura e transparência; III – compartilhamento da capacidade de serviço; IV – simplicidade; V – priorização de serviços públicos disponibilizados em meio digital; VI – segurança e privacidade; VII – participação e controle social; VIII – governo como plataforma; e IX – inovação (Brasil, 2016).

De acordo com Avelino, Pompeu e Fonseca (2021), no Brasil, existe uma série de normas que guiam a implementação das políticas de dados abertos governamentais, como o Decreto n.º 8.777/2016, que institui a Política de Dados Abertos do Poder Executivo Federal (PDAPF).

No âmbito dessa política cada órgão deve elaborar, a cada 2 anos, seu Plano de Dados Abertos (PDA). O PDA planeja as ações que visam à abertura e sustentação de dados nas organizações públicas, indicando o conteúdo e o formato das bases que serão abertas, o cronograma de abertura, assim como se estão sujeitas ou não ao sigilo. Para os autores, a escolha das bases e dos cronogramas deve ser feita considerando os pedidos encaminhados via LAI, bem como a realização de consultas públicas à sociedade para melhor conhecer a demanda por dados.

Embora aplicáveis ao âmbito federal, referidos decretos norteiam como deveria se pautar a administração municipal.

No contexto das *smart cities*, os dados abertos não só são fundamentais para a inovação e melhoria da qualidade de vida urbana, mas também são essenciais para garantir a transparência, promover a confiança e assegurar a conformidade com a legislação de proteção de dados como a LGPD.

Embora a LGPD se concentre primordialmente na proteção de dados pessoais e na privacidade dos indivíduos, a promoção de dados abertos se alinha ao espírito da lei no que tange à transparência e ao uso ético de informações.

A LGPD destaca a transparência como um de seus pilares fundamentais. A falta de dados abertos compromete essa transparência, pois impede que os cidadãos tenham acesso claro e abrangente às informações sobre como os dados são coletados, processados e utilizados pela Administração Pública. Sem essa

transparência, os cidadãos têm menos meios para entender ou questionar como suas informações pessoais são tratadas, limitando sua capacidade de exercer direitos previstos pela LGPD, como o de verificar a exatidão dos dados ou solicitar a correção de informações incorretas.

Em um cenário onde dados abertos são negligenciados, há um risco maior de que os dados pessoais sejam utilizados de forma inadequada ou excessiva. Os dados abertos, quando devidamente anonimizados, permitem que a cidade se beneficie de informações valiosas sem comprometer a privacidade individual. Sem a estratégia de dados abertos, o município pode se tornar excessivamente dependente de dados pessoais, elevando o risco de violações de privacidade.

Dados abertos são fundamentais para uma sociedade democrática, pois permitem que os cidadãos acessem informações cruciais sobre a gestão pública, participem de maneira mais efetiva no debate público e tomem decisões informadas. A ausência desses dados limita a capacidade de escrutínio público, reduzindo a *accountability* das autoridades e enfraquecendo a própria democracia.

Em suma, a ausência de uma política robusta de dados abertos no Recife pode levar a uma violação dos princípios da LGPD, particularmente no que diz respeito à transparência e à proteção de dados. Ademais, tal carência afeta diretamente a qualidade da democracia e a eficiência da Administração Pública, além de restringir oportunidades de inovação e desenvolvimento que dados abertos podem fomentar.

É preciso destacar que a ausência de informações públicas sobre os parceiros com quem o município compartilha dados impede uma análise integral das práticas de proteção de dados, comprometendo a compreensão de como essas parcerias afetam a privacidade e a segurança dos dados dos cidadãos recifenses.

O fato é que não existe uma página de dados aberto no Município. Esse vácuo de informação limita a capacidade de avaliar a aderência do município à LGPD e de identificar possíveis riscos à privacidade dos indivíduos, sendo um impedimento substancial para o desenvolvimento acadêmico e prático do meu trabalho. Assim, a falta de transparência não apenas compromete a proteção de dados pessoais, mas também obstaculiza pesquisas acadêmicas que poderiam contribuir para o aprimoramento das políticas públicas de proteção de dados.

Se os dados não são abertos e há parcerias com instituições públicas e privadas, pode-se concluir que apenas algumas entidades têm acesso a dados

cruciais, o que cria barreiras para novos entrantes e pode resultar em oligopólios ou monopólios, limitando a diversidade de serviços e inovações para a sociedade.

Morozov (2021) nos alerta sobre a transição de um espaço político tradicional para um ambiente onde decisões automatizadas e algorítmicas ganham proeminência, muitas vezes à custa da transparência e da participação democrática. Na obra '*Big Tech: The Rise of Data and the Death of Politics*, examina como a ascensão dessas corporações não apenas remodelou a economia global, introduzindo novos modelos de negócios e deslocando setores tradicionais, mas também reconfigurou profundamente o espaço político e a governança.

Primeiramente, no âmbito econômico, Morozov destaca que as grandes empresas de tecnologia, ao acumular quantidades massivas de dados, adquiriram uma vantagem competitiva sem precedentes, posicionando-se como intermediárias essenciais em quase todas as transações econômicas e sociais. Essa centralização de poder e informação em poucas entidades impacta a concorrência, a inovação e, inclusive, a distribuição de riqueza.

Do ponto de vista político, a transformação é ainda mais profunda. Morozov argumenta que, à medida que essas empresas penetram cada vez mais em aspectos da vida cotidiana, elas começam a exercer funções que tradicionalmente pertenciam ao Estado, como a coleta e análise de dados, a infraestrutura de comunicação e até mesmo a regulação de normas sociais através de suas plataformas. Este fenômeno é particularmente evidente em contextos urbanos, onde cidades inteligentes dependem cada vez mais de tecnologias fornecidas por essas corporações para gerir tudo, desde o tráfego até serviços públicos e segurança.

Além disso, a capacidade dessas empresas de influenciar a opinião pública, moldar o discurso político e até mesmo afetar eleições, através do controle sobre as plataformas de comunicação, questiona a própria essência da democracia representativa. A manipulação de informações e a criação de câmaras de eco ideológicas comprometem a esfera pública, onde um debate informado e diverso é fundamental para o processo democrático.

Portanto, a reconfiguração do espaço político implica uma necessidade urgente de repensar as estruturas de governança para garantir que a transição para um mundo mais digital não comprometa valores democráticos fundamentais. Isso envolve desenvolver novas formas de regulamentação que sejam capazes de lidar

com a rapidez da inovação tecnológica e a complexidade dos dados, bem como fomentar a transparência e a responsabilidade das *Big Techs*.

Portanto, embora a tecnologia ofereça soluções inovadoras para problemas urbanos complexos, sua aplicação não é neutra e está intrinsecamente ligada a interesses econômicos e políticos poderosos. A ausência de dados públicos sobre quem são os atores cujos dados da cidade do Recife são compartilhados e a forma desse compartilhamento impede que se identifique e controle como esses atores podem influenciar as decisões políticas, a configuração dos espaços urbanos e a vida dos cidadãos, ao passo que os impede e realizarem essa influência.

A urgência de um novo marco regulatório e de governança que possa equilibrar os benefícios da inovação tecnológica com a necessidade de proteger os direitos fundamentais e fomentar uma sociedade mais justa. Para o Recife, isso significa investir na criação de políticas públicas que não apenas integrem tecnologias avançadas, mas que também priorizem a inclusão social, a transparência e a abertura de dados.

CONSIDERAÇÕES FINAIS

A presente dissertação visou estabelecer que, embora os impulsionadores políticos e econômicos das cidades inteligentes tendam à supremacia da tecnologia, as cidades inteligentes ainda sofrerão como projeto se não conseguirem obter a privacidade correta; e que, no momento, essa falha é muito provável, já que sofrem com a combinação de três das questões mais difíceis para a lei de privacidade moderna regular: a IoT, *Big Data* e infraestrutura baseada em nuvem.

Apesar de um longo período de lamentação da sociedade pela "morte da privacidade" na era das redes digitais, se diga que a LGPD cumpre o seu propósito e, em princípio, não precisa ser modificada para lidar com ameaças como a crescente dificuldade para o consentimento informado, em razão de fenômenos como *Big Data*, a IoT e a nuvem.

A privacidade em cidades inteligentes não pode ser protegida apenas por exortações para que se respeite a lei, particularmente quando essa lei se torna cada vez mais complexa de interpretar e aplicar. As soluções em arquiteturas de privacidade em cidades inteligentes, devem ser incorporadas ao código dessas cidades – não apenas seu *software* e *hardware*, mas seu *design*. Este é o princípio da "privacidade desde o projeto".

Diante desse quadro, é possível vislumbrar alguns caminhos. Primeiramente, deve-se priorizar a privacidade desde a concepção (PdC) e avaliações de impacto da privacidade. A privacidade desde a concepção é uma abordagem para proteger a privacidade incorporando-a nas especificações de design de tecnologias, práticas comerciais e infraestruturas físicas e se dão, e.g.: através da restrição ao mínimo a quantidade de aplicativos de dados coletados; criptografia de fluxos de dados como padrão; anonimização de dados pessoais; incorporação de sistemas de avisos de privacidade de maneira amigável em momentos apropriados; restrição dos períodos de retenção de dados ("expiração de dados"); fornecimento de menus de configurações de privacidade em uma linguagem clara e amigável, no qual os padrões são particularmente protetores para as crianças; atenção permanente dos projetistas de sistemas para pensarem sobre questões de privacidade enquanto constroem seus sistemas (Luger *et al.*, 2014).

A solução mais radical via PdC para os problemas em torno da IoT pode ser argumentar que os dados coletados por dispositivos sejam mantidos localmente (e,

na medida do possível, processados localmente) e, portanto, mantidos sob o controle do usuário, em vez de oferecidos aos controladores de dados, na nuvem ou de outra forma.

Hildebrandt e Koops (2010) argumentam que, onde o processamento é controlado localmente nos dispositivos, podem ser construídas restrições de código que reifiquem as regras da lei que protegem os usuários, um conceito que eles chamam de “inteligência ambiental”. No entanto, Koops e Leenes (2014) também expressaram dúvidas quanto à praticidade da arquitetura que incorpora regras de proteção de dados, argumentando que a codificação de disposições de privacidade na lei está longe de banal, mas, obviamente, há dificuldades como a textura aberta das leis de proteção de dados e a falta de uma “mentalidade de privacidade” nos designers de sistemas de TI.

À medida que a fé nas soluções legais de privacidade diminuiu no mundo da informação globalizada, as soluções PdC têm recebido cada vez mais visibilidade por parte de formuladores de políticas e reguladores de privacidade, bem como de acadêmicos.

Assim, deve haver na legislação a obrigação de que o princípio da proteção de dados desde o design seja incorporado em todo o ciclo de vida da tecnologia, desde o estágio inicial, até sua implantação, uso e descarte final. Como engenheiros e programadores comuns, sem treinamento substantivo ou consciência de privacidade em qualquer detalhe, muitas vezes trabalhando em pequenas empresas de IoT ou nuvem que não são voltadas para o cliente e com a tarefa de se concentrar na velocidade e economia, irão implementar violações em aplicativos de cidades inteligentes, representa um grande problema para o futuro.

As Avaliações de Impacto de Privacidade (AIP) são uma abordagem para tornar o PdC mais viável e eficaz. Ela está prevista no art. 50, inc. I, alínea d) da LGPD, leia-se:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. I – implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador

> em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; (Brasil, 2018).

Esse processo deve auxiliar as organizações na identificação e minimização dos riscos de privacidade de novos projetos ou políticas, sobretudo nas áreas de tecnologias médicas ou genéticas, para definir e prever ameaças à privacidade, a fim de desenvolver soluções nas fases iniciais de projetos ou programas.

Embora isto seja mais difícil no modelo do mundo ocidental de cidades inteligentes adaptadas, onde a computação ubíqua adquire tração por agregação lenta, o quadro é outro para um futuro em que cidades inteligentes são rotineiramente construídas de cima para baixo, como na Índia e na Coréia, o que nada impede de vir a acontecer no Brasil.

Em uma cidade inteligente, há imensos fluxos de dados interagindo, de múltiplos proprietários/controladores de dados e diferentes jurisdições de armazenamento e processamento, todos variando ao longo do tempo e criando ciclos de feedback uns com os outros. O gestor pode até sentir que tem o poder e o dever de controlar o projeto final – mas o controle real (embora talvez não legal), na maioria das vezes, é dos fornecedores ou investidores privados e seus subfornecedores na nuvem. Além disso, cidades do futuro podem até ter “arquiteturas adaptativas” que começam a decidir por si mesmas quais dados coletar e como processá-los.

Os algoritmos são opacos e mudam à medida que aprendem de maneiras que até mesmo os controladores de dados podem ter pouca ideia do que exatamente está acontecendo com os dados. Neste maquinário kafkiano que manipula vidas com base em justificativas rasas, é preciso pensar muito sobre como tornar as AIPs viáveis. Este será um trabalho tanto para planejadores urbanos, engenheiros e arquitetos (entre outros), quanto para juristas especialistas em privacidade.

Essa função, acredita-se, deve ficar a cargo do Autoridade Nacional de Proteção de Dados (ANPD), órgão da Administração Pública federal, integrante da Presidência da República, que pode ser transformada pelo Poder Executivo em entidade da Administração Pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República, nos termos do art. 55-A da LGPD.

Esse órgão, utilizando-se do AIP deve expandir sua regulação para outras áreas dos direitos humanos fundamentais, como para vedar e punir o perfil de *Big*

Data que realize práticas de discriminação, o violem devido processo e liberdade de expressão (como a utilização de opiniões políticas para manipulação eleitoral).

Deve-se impor um sistema de governança de algoritmos, tanto do ponto de vista normativo e regulatório e quanto do ponto de vista técnico, a fim de regular empresas privadas, tendo como ponto fundamental o interesse público e regulação estatal, para controlar o nível de transparência de ferramentas utilizadas pelo Estado, a fim de construir um espaço digital justo e democrático.

A aplicação do PdC às cidades inteligentes pode contribuir para solução do problema relativo à dificuldade de obter consentimento informado em ambientes de IoT. O consentimento é importante porque, embora não seja o único fundamento legítimo para processamento conforme a LGPD, é o padrão mais global de legitimidade e é o mais provável de gerar a confiança do usuário.

Além disso, quando dados confidenciais são coletados, como dados de saúde, o consentimento explícito geralmente será necessário. Conforme observado acima, obter consentimento significativo em ambientes de IoT é um problema. Tradicionalmente, o consentimento é fornecido quando os dados são coletados, mas ele pode ser melhorado através de algumas estratégias, como:

a) direcionar os clientes a tutoriais em vídeo para guiá-los através das páginas de configurações de privacidade ou, alternativamente, fornecer assistentes de “configuração” para obter as escolhas corretas de coleta de dados;
b) residências ou outros locais podem ter “painéis” ou “portais de gerenciamento” de controle detalhado, onde os consumidores podem revisar com alguma clareza quais dados eles escolheram compartilhar de vez em quando em diferentes aplicativos ou por meio de diferentes dispositivos;
c) colocar códigos QR no dispositivo IoT para conecta-se à Internet; diferentes ícones podem piscar para mostrar diferentes níveis de risco e/ou diferentes tipos de coleta de dados;
d) opção dos clientes para que as configurações de privacidade e segurança sejam enviadas a eles por e-mail ou mensagens de texto.

Contudo, essas respostas não são suficientes para o problema das cidades inteligentes. Não adianta esperar que os cidadãos parem para ler e considerar as políticas de privacidade em seus telefones, mesmo as mais reduzidas, mesmo se adquiridas por QR *codes*, enquanto tentam pegar um bonde inteligente ou chamar um

carro/táxi autônomo ou comprar uma pizza de um drone que esteja passando. É o que evidenciam a maioria das pesquisas não relacionadas à IoT sobre políticas de consentimento e privacidade, e os problemas só pioram na IoT.

O problema principal permanece, como já foi discutido, que, embora se possa encontrar métodos para fornecer algum tipo de aviso/informação, os consentimentos obtidos na IoT quase sempre serão ilusórios ou, na melhor das hipóteses, de baixa qualidade em termos das exigências da LGPD para consentimento livre, específico e informado. Se o uso de dispositivos inteligentes se torna inevitável em uma cidade inteligente, então “aviso e escolha” simplesmente se torna um paradigma inaplicável.

Uma abordagem alternativa que pode parecer mais promissora é reconsiderar como o consentimento pode ser dado no mundo da IoT, concebendo-o como um processo contínuo, ao invés de uma escolha única no ponto de coleta de dados, i.e., afastando-se da ideia de pré-consentimento.

Mais garantidor de privacidade seria se as escolhas de privacidade feitas anteriormente fossem lembradas pelos sistemas inteligentes e aplicadas na próxima vez que uma escolha precisasse ser feita. Poder-se-ia fazê-lo através de um único dispositivo em uma casa inteligente – um eletrodoméstico que atua como um *hub* – capaz de pôr em seu *display* as preferências do consumidor e ainda as aplicar a novos eletrodomésticos e novos usos.

Muitos autores estão se movendo em direção à noção de que o consentimento como uma base para legitimar o processamento é simplesmente equivocado. Os usuários, como já foi provado repetidamente, não têm recursos, oportunidade, inclinação ou motivação para dar consentimentos significativos no ambiente online atual e isso só é exacerbado pelo IoT; ainda assim, suas escolhas individuais são permitidas para estampar padrões de coleta de dados que são cada vez mais prejudiciais para a sociedade.

Restrições éticas sobre os coletores de dados, independentemente de os usuários darem ou não consentimentos sem sentido, estão sendo promovidas como uma nova abordagem. Não é incomum que profissionais como médicos, advogados e até mesmo arquitetos, engenheiros ou eletricistas sejam considerados em um nível de conduta mais elevado do que as exigências da lei básica, por códigos profissionais. Essas garantias de “*soft law*” são frequentemente vistas como eficazes em mercados competitivos voltados para o consumidor, onde o bom comportamento pode atrair negócios. No entanto, os mercados de coleta de dados até o momento não são

competitivos nesse sentido, como resultado de assimetrias de informação do consumidor.

É preciso admitir que o consentimento é apenas um primeiro passo para o processamento legal e que, independentemente dessa permissão, certos usos desses dados, no modelo ambiental, são nocivos e, portanto, proibidos. Exemplos óbvios de práticas possivelmente proibidas incluem direcionar publicidade às crianças, álcool, dietas e drogas aos viciados e anoréxicos e fazer uso de dados coletados em locais inerentemente privados, como banheiros.

Uma área distinta onde se pode procurar intervenção jurídica, em particular no que se refere à IoT, *Big Data* e cidades inteligentes, é a área da transparência algorítmica. Embora se possa alegar que tal transparência esteja indisponível no mundo de *Big Data* e algoritmos de aprendizagem, as técnicas de engenharia reversa sem dúvida irão melhorar, e é certamente uma das melhores ferramentas potenciais para esclarecer o que os criadores de perfil de dados estão realmente fazendo.

O direito pouco conhecido no LGPD dos titulares dos dados de obter conhecimento da lógica envolvida em qualquer processamento automático de dados relativos a ele deve ser conhecido de forma inequívoca e, de fato, explicitamente estendido para lidar com todo o processamento de *Big Data*.

Em suma, as cidades inteligentes podem oferecer soluções para problemas como a economia de energia, a proteção do meio-ambiente, segurança pública, reduzir mortes nas estradas. Mas, mesmo na solução de problemas tão sensíveis, a privacidade e segurança são importantes, não só como um direito fundamental, mas como um pré-requisito para manter a confiança e o engajamento dos moradores das cidades inteligentes.

Vê-se que a LGPD possui regulações até agora genéricas e tênues e parecem estar cada vez mais longe medidas mais rígidas. Diante desse quadro, apresentam-se quatro sugestões para pesquisas futuras e envolvimento legislativo e político:

a) Investigação sobre o potencial de afetação da privacidade de uma cidade;
b) Investigação sobre o potencial técnico e social dos métodos de dar “consentimento prévio” ou “consentimento permanente” para lidar com as restrições da IoT;
c) Legislar para transparência algorítmica e pesquisar maneiras de tornar os dados algorítmicos compreensíveis para os consumidores;

d) Afastar-se, pelo menos parcialmente, do consentimento ou “notificação e escolha” como mecanismo principal para validar a coleta e o processamento de dados; conexamente, proibindo atividades nocivas de processamento de dados, mesmo quando há consentimento.

A dissertação demonstrou, ainda, que nas cidades inteligentes, tecnologias como *Big Data*, computação em nuvem e reconhecimento facial são pilares fundamentais para otimizar a gestão urbana, melhorar a eficiência dos serviços públicos e a qualidade de vida dos cidadãos. O *Big Data* permite a análise de grandes volumes de dados gerados pelos diversos dispositivos conectados na cidade, proporcionando insights valiosos para a tomada de decisões. A computação em nuvem oferece a infraestrutura necessária para processar e armazenar essa imensidão de dados, garantindo escalabilidade e flexibilidade. O reconhecimento facial, por sua vez, é aplicado em diversas áreas, desde a segurança pública até o aprimoramento de serviços municipais.

Contudo, a dissertação apresenta uma crítica a essas tecnologias, no contexto do panoptismo na era digital, que se refere à capacidade de observação e monitoramento contínuos, criando uma sensação de vigilância constante nos indivíduos. Nas cidades inteligentes, essa vigilância é potencializada pelo uso intensivo de câmeras e algoritmos de reconhecimento facial, que podem monitorar e analisar comportamentos em grande escala.

Essa crítica destaca o risco de erosão da privacidade e da autonomia individual, onde cada movimento e ação podem ser rastreados, analisados e armazenados indefinidamente. Além disso, a centralização do controle e a falta de transparência sobre quem possui e processa os dados levantam preocupações significativas sobre o poder desproporcional concedido a entidades governamentais e corporações, assim como sobre a potencial discriminação e exclusão social.

Portanto, enfatiza-se a necessidade de equilibrar os benefícios das cidades inteligentes com a proteção dos direitos individuais, argumentando que a tecnologia deve ser implementada de forma a respeitar a dignidade e a liberdade das pessoas, evitando a criação de uma sociedade de vigilância onipresente que comprometa os valores democráticos e a privacidade.

Especificamente sobre a cidade do Recife, abordou-se a evolução histórica, urbanística e tecnológica, contextualizando-a no âmbito de uma cidade inteligente que busca integrar avanços tecnológicos à gestão urbana. No entanto, identificou-se um

desafio significativo que ameaça a integridade deste desenvolvimento: a falta de transparência e abertura dos dados municipais.

A ausência de dados abertos no Recife contradiz a filosofia e os requisitos legais estabelecidos pela Lei Geral de Proteção de Dados, subestimando a importância da transparência e da prestação de contas em um governo que se pretende moderno e inclusivo. Este cenário compromete não apenas a confiabilidade e a eficiência das iniciativas de cidade inteligente, mas também mina a confiança pública, restringindo a participação cidadã e a inovação colaborativa.

Além disso, a exclusividade no compartilhamento de dados com certas entidades cria um ambiente de desigualdade no acesso à informação, limitando a capacidade de diversos atores sociais de contribuir para o desenvolvimento e inovação da cidade. Isso não apenas fere princípios de equidade e justiça, mas também pode resultar em práticas anticompetitivas, contrariando os princípios de livre mercado e concorrência leal.

É essencial, portanto, que o município do Recife revise suas políticas e práticas de gestão de dados, alinhando-as com os padrões nacionais e internacionais de transparência, privacidade e abertura de dados. Tal alinhamento fortaleceria o compromisso da cidade com os direitos fundamentais de seus cidadãos, além de impulsionar o potencial inovador e democrático que as tecnologias da informação podem oferecer.

Para o futuro, Recife deve buscar uma cultura de governança digital que valorize a abertura, a colaboração e a transparência, estabelecendo um modelo de cidade inteligente que seja sustentável, inclusivo e responsivo às necessidades de todos os seus habitantes. Essa abordagem não só atenderia às exigências legais, como também fomentaria um ecossistema urbano vibrante, capaz de atrair talentos, investimentos e inovações, contribuindo para o bem-estar e a prosperidade da comunidade recifense.

Em decorrência da ausência de transparência quanto ao compartilhamento de dados com parceiros privados, quais são esses parceiros, não foi possível averiguar questões centrais para a proteção de dados no contexto da cidade do Recife, o que será possível em estudos futuros, adequando-se à metodologia para uma pesquisa de campo mais profunda, que ultrapasse as consultas em portais públicos, uma vez que essa imposição legal de transparência e publicidade não é observada pelo Município.

REFERÊNCIAS

AKAMAI. **AKAMAI'S State of the internet**: Q3 2014 Report. [*S. l.*]: Akamai, 2014. Disponível em: https://www.antel.com.uy/wps/wcm/connect/2e38bd0047ad6c9682d3e7af6890d810/q3-2014-state-of-the-internet-report+(2).pdf?MOD=AJPERES. Acesso em: 21 out. 2021.

ARAÚJO, Marcelo Labanca Corrêa de; COUTO, Walles Henrique de Oliveira. Novas Tecnologias e Proteção de Dados na Democracia Brasileira: entre a anarquia e controle normativo. **Brazilian Journal of Development**, São José dos Pinhais, v. 7, n. 6, p. 55444-55456, 2021. Disponível em: https://doi.org/10.34117/bjdv7n6-109. Acesso em: 19 maio 2024.

ARAYA, Elizabeth Roxana Mass; VIDOTTI, Silvana Aparecida Borsetti Gregório. **Criação, proteção e uso legal de informação em ambientes da World Wide Web**. São Paulo: Editora UNESP: Cultura Acadêmica, 2010.

AVELINO, Daniel Pitangueira de; POMPEU, João Cláudio; FONSECA, Igor Ferraz da. **Democracia digital**: Mapeamento de experiências em dados abertos, governo digital e ouvidorias públicas. Brasília, DF: Instituto de Pesquisa Econômica Aplicada, 2021. (Texto para Discussão, n. 2624).

BAECK, Peter; SAUNDERS, Tom. **Rethinking Smart Cities From The Ground Up**. London: Nesta, 2015. Disponível em: http://www.nesta.org.uk/publications/rethinking-smart-cities-ground. Acesso em: 21 out. 2021.

BARRIO ANDRÉS, Moisés. Retos y desafíos del Estado algorítmico de derecho. **Real Instituto Elcano**, Madri, n. 82, p. 1-6, 2020. Disponível em: https://www.realinstitutoelcano.org/analisis/retos-y-desafios-del-estado-algoritmico-de-derecho/. Acesso em: 21 dez. 2023.

BELTRÃO, Silvio Romero. **Direitos da Personalidade**. 2. ed. São Paulo: Atlas, 2014.

BENAKOUCHE, Tamara. Redes técnicas/redes sociais: pré-história da internet no Brasil. **Revista USP**, São Paulo, n. 35, p. 124-133, 1997. Disponível em: https://doi.org/10.11606/issn.2316-9036.v0i35p124-133. Acesso em: 10 abr. 2024.

BENJAMIN, Antônio Herman de Vasconcelos *et al*. **Código Brasileiro de Defesa do Consumidor**. Comentado pelos autores do anteprojeto. 9. ed. Rio de Janeiro: Forense Universitária, 2007.

BENNAMOUN, Mohammed; GUO, Yulan; SOHEL, Ferdous. Feature Selection for 2D and 3D Face Recognition. *In*: WEBSTER, J. G. (ed.). **Encyclopedia of Electrical**

and Electronics Engineering. Nova Jersey: Wiley, 2015. p. 1-28. Disponível em: https://onlinelibrary.wiley.com/doi/abs/10.1002/047134608X.W8257. Acesso em: 13 abr. 2023.

BERGSTEIN, Laís; ARAGÃO, Flávia Gama de Carvalho; CÂMARA, Maria Amália. Proteção de dados pessoais e as decisões automatizadas nas relações de consumo: os direitos à explicação e revisão. **Revista de Direito do Consumidor – RDC**, São Paulo, v. 31, n. 140, p. 359-385, 2022.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BITTAR, Carlos Alberto. **Os Direitos da Personalidade**. 8. ed. São Paulo: Saraiva, 2015.

BONFIM, Camila. Invasão a sistemas do CNJ: PF indicia Zambelli por dois crimes e hacker por quatro; veja quais. **G1**, [*s. l.*], 01 mar. 2024. Disponível em: https://g1.globo.com/politica/blog/camila-bomfim/post/2024/03/01/invasao-a-sistemas-do-cnj-pf-indicia-zambelli-por-dois-crimes-e-hacker-por-quatro-veja-quais.ghtml. Acesso em: 10 jun. 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. Câmara dos Deputados. **Cidades inteligentes**: uma abordagem humana e sustentável. Brasília, DF: Edições Câmara, 2021.

BRASIL. **Decreto nº 8.638, de 15 de janeiro de 2016**. Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional. Brasília, DF: Presidência da República, 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8638.htm. Acesso em: 10 abr. 2024.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Brasília, DF: SDE/DPDC, 2010. (Caderno de Investigações Científicas).

BRASIL. **Lei n.º 11.079, 30 de dezembro de 2004**. Institui normas gerais para licitação e contratação de parceria público-privada no âmbito da administração pública. Brasília, DF: Presidência da República, 2004. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/l11079.htm. Acesso em: 20 jan. 2024.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de

1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, 2011. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 15 fev. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 mar. 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 20 mar. 2019.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L8078.htm. Acesso em: 20 mar. 2019.

BRASIL. **Lei nº 8.159, de 8 de janeiro de 1991**. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. Brasília, DF: Presidência da República, 1991. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8159.htm. Acesso em: 20 mar. 2024.

BRASIL. Ministério da Pesca e Aquicultura. Dados Abertos. MPA, Brasília, 01 nov. 2024. Disponível em: https://www.gov.br/mpa/pt-br/acesso-a-informacao/dados-abertos-2. Acesso em: Acesso em: 02 nov. 2024.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 4.424 Distrito Federal**. Relator: Min. Marco Aurélio, 09 de fevereiro de 2012.

BROWN, Ian. Regulation and the Internet of Things. **GSR Discussion Paper**, [*s. l.*], p. 1-34, 2015. Disponível em: http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf. Acesso em: 20 out. 2021.

BUCKLEY, Chirs; MOZUR, Paul; RAMZY, Austin. How China turned a city into a prision: a surveillance state reaches new Heights. **The New York Times**, Xinjiang, 04 abr. 2019. Disponível em: https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html. Acesso em: 01 abr. 2021.

CACHAPUZ, Maria Cláudia. **Intimidade e vida privada no novo código civil brasileiro**: uma leitura orientada no discurso jurídico. Porto Alegre: Sergio Antonio Fabris Ed., 2006.

CALDAS, Max Silva; SILVA, Emanoel Costa Claudino. Fundamentos e aplicação do Big Data: como tratar informações em uma sociedade de yottabytes. **Bibliotecas Universitárias**: pesquisas, experiências e perspectivas, Belo Horizonte, v. 3, n. 1, p. 65-83, jan./jun. 2016.

CANCELIER, Mikhail Vieira de Lorenzi. O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro. **Sequência**, Florianópolis, n. 76, p. 213-239, maio 2017.

CARDULLO, Paolo; KITCHIN, Rob. Smart Urbanism and Smart Citizenship: The Neoliberal Logic of 'Citizen-Focused' Smart Cities in Europe. **Environment and Planning C**: Politics and Space, United Kingdom, v. 37, n. 5, p. 813-830, 2018.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da Internet no Brasil**: do surgimento das redes de computadores à instituição dos mecanismos de governança. 2006. 259 f. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Programa de Pós-Graduação em Engenharia, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2006.

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

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2002. v. 1.

CASTRO, Gilberto Ramos de. **Discussão conceitual sobre Dado, Informação e Conhecimento**: perspectiva dos alunos concluintes do Curso de Biblioteconomia da UFPB. 2011. 51 p. Monografia (Graduação em Biblioteconomia) – Centro de Ciências Sociais Aplicadas, Universidade Federal da Paraíba, João Pessoa, 2011.

CAVOUKIAN, Ann. Privacy by Design: The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices. **UCSC**, Santa Cruz, 2012. Disponível em: https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf. Acesso em: 10 jan. 2024.

CERRUDO, Cesar. An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks. **IOActive Labs,** Seattle, p. 1-20, 2015. (White Paper). Disponível em: http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf. Acesso em: 10 out. 2021.

CHEN, Stephen. China to build giant facial recognition database to identify any citizen within seconds. **South China Morning Post**, Beijing, 12 out. 2017. Disponível

em: https://www.scmp.com/news/china/society/article/2115094/china-build-giant-facial-recognition-database-identify-any. Acesso em: 1 abr. 2021.

CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. **Washington Law Review**, Washington, v. 89, n. 1, p. 1-33, 2014. Disponível em: https://digitalcommons.law.uw.edu/cgi/viewcontent.cgi?article=4796&context=wlr Acesso em: 20 mar. 2024.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. São Paulo: Saraiva, 2002.

CREEMERS, Rogier. China's Social Credit System: an evolving practice of control. **SSRN Electronic Journal,** Amsterdam, p. 1-32, maio 2018. Disponível em: http://dx.doi.org/10.2139/ssrn.3175792. Acesso em: 30 jan. 2024.

DAL MAGRO, Diogo; FORTES, Vinícius Borges. O reconhecimento facial nas *smart cities* e a garantia dos direitos à privacidade e à proteção de dados pessoais. **Revista de Direito Internacional**, Brasília, v. 18, n. 2, p. 301-329, 2021.

DAMERI, Renata Paola; COCCHIA, Annalisa. Smart City and Digital City: Twenty Years of Terminology Evolution. *In*: CONFERENCE OF THE ITALIAN CHAPTER OF AIS, 10, 2013, Milan. **Proceedings** […]. Milan: ITAIS, 2013. Disponível em: http://www.itais.org/proceedings/itais2013/pdf/119.pdf. Acesso em: 28 out. 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

ECHARRI, Miquel. 150 demissões em um segundo: os algoritmos que decidem quem deve ser mandado embora. **El País**, Barcelona, 10 out. 2021. Disponível em: https://brasil.elpais.com/tecnologia/2021-10-10/150-demissoes-em-um-segundo-assim-funcionam-os-algoritmos-que-decidem-quem-deve-ser-mandado-embora.html. Acesso em: 25 out. 2021.

EHRHARDT JÚNIOR, Marcos; FRANÇA NETTO, Milton Pereira de; MALHEIROS, Guilherme Maciel. Os riscos da discriminação algorítmica na utilização de aplicações de inteligência artificial no cenário brasileiro. **Revista Jurídica Luso-Brasileira**, Lisboa, v. 8, n. 3, p. 1271-1318, 2022.

EUROPEAN UNION. **Europe 2020**: a strategy for smart, sustainable and inclusive growth. Brussels: EUR-Lex, 2020a. Disponível em: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC2020. Acesso em: 28 out. 2021.

EUROPEAN UNION. The History of the General Data Protection Regulation. **European Data Protection Supervisor**, Brussels, 2020b. Disponível em:

https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. Acesso em: 10 mar. 2024.

FINCH, Kelsey; TENE, Omar. Welcome to the Metropticon – Protecting Privacy in a Hyperconnected Town. **Fordham Urban Law Journal**, New York, v. 41, n. 5, p. 1581-1615, 2014. Disponível em: https://ir.lawnet.fordham.edu/ulj/vol41/iss5/4/. Acesso em: 15 abr. 2024.

FOUCAULT, Michel. **Vigiar e punir**: nascimento da prisão. Tradução: Ligia de M. Pondé Vassalo. Rio de Janeiro: Vozes, 2002.

FTC. **Internet of Things**: Privacy and Security in a Connected World. [*S. l.*]: FTC Staff Report, 2015. Disponível em: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. Acesso em: 20 out. 2021.

FUSTER, Gloria González; SCHERRER, Amandine. **Big Data and smart devices and their impact on privacy**. Brussels: European Union, 2015. Disponível em: https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536455/IPOL_STU(2015)536455_EN.pdf. Acesso em: 28 out. 2021.

G1. Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. **G1**, [*s. l.*], 02 dez. 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 20 abr. 2024.

GOERGE, Robert M. Data for the Public Good: Challenges and Barriers in the Context of Cities. *In*: LANE, Julia *et al*. **Privacy, Big Data, and the Public Good**. Cambridge: Cambridge University Press, 2014. p. 153-172. Disponível em: https://assets.cambridge.org/97811070/67356/frontmatter/9781107067356_frontmatter.pdf. Acesso em: 20 mar. 2024.

GOMES, Maria Cecília. Programa Embarque Seguro: reconhecimento facial em aeroportos no Brasil. **IRIS**, Belo Horizonte, 2 dez. 2020. Disponível em: https://irisbh.com.br/programa-embarque-seguro-questionamentos-sobre-reconhecimento-facial-em-aeroportos-no-brasil/. Acesso em: 28 set. 2023.

GOMES, Orlando. **Introdução ao Direito Civil**. Rio de Janeiro: Forense, 2016.

GREENBERG, Andy. The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse. **WIRED**, [*s. l.*], 1 ago. 2016. Disponível em: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/. Acesso em: 25 out. 2021.

GREENFIELD, Adam. **Radical Technologies**: The Design of Everyday Life. London: Verso Books, 2017.

HILDEBRANDT, Mireille; KOOPS, Bert-Jaap. The Challenges of Ambient Law and Legal Protection in the Profiling Era. **Modern Law Review**, United Kingdom, v. 73, n. 3, p. 428-460, 2010.

HILDEBRANDT, Mireille. Defining profiling: A new type of knowledge. *In*: HILDEBRANDT, Mireille; GUTWIRTH, Serge. **Profiling the European Citizen**: cross-disciplinary perspectives. London: Springer, 2008. p. 17-44. Disponível em: https://www.researchgate.net/publication/226744267_Defining_Profiling_A_New_Type_of_Knowledge. Acesso em: 10 set. 2023.

HOJDAA, Alexandre; MARTINS, Pedro; FARINIUK, Tharsila Maynardes. Da cidade inteligente à inteligência nas operações urbanas: o caso do Centro de Operações Rio. **Revista LIDER**, Osorno, v. 22, n. 36, p. 104-131, 2020.

HOVEN, Jeroen van den. Privacy and the Varieties of Informational Wrongdoing. *In*: SPINELLO, Richard A.; TAVANI, Herman T. **Readings in Cyberethics**. Sudbury: Jones and Bartlett Publishers, 2004. p. 488-500.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). Cidades e Estados. Recife. **IBGE**, Rio de Janeiro, 2020. Disponível em: https://www.ibge.gov.br/cidades-e-estados/pe/recife.html. Acesso em: 30 fev. 2023.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). História. Recife. **IBGE**, Rio de Janeiro, 2014. Disponível em: https://cidades.ibge.gov.br/brasil/pe/recife/historico. Acesso em: 25 fev. 2024.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **Smart Cities**: Preliminary Report 2014. Geneva: ISO, 2015. Disponível em: http://www.iso.org/iso/smart_cities_report-jtc1.pdf. Acesso em: 21 out. 2021.

JESUS, Damásio de; MILAGRE, José Antonio. **Marco civil da internet**: comentários à Lei n. 12.965/14. São Paulo: Saraiva, 2014.

JUNQUEIRA, Thiago. **Tratamento de dados pessoais e discriminação algorítmica nos seguros**. São Paulo: Revista dos Tribunais, 2020.

KITCHIN, Rob. From a Single Line of Code to an Entire City: Reframing Thinking on Code and the City. **The Programmable City Working Paper**, [*s. l.*], n. 4, p. 1-15, 2014. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2520435. Acesso em: 22 out. 2021.

KITCHIN, Rob. The Ethics of Smart Cities and Urban Science. **Philosophical Transactions A**, London, v. 374, n. 2083, 2016. Disponível em: https://doi.org/10.1098/rsta.2016.0115. Acesso em: 30 jan. 2023.

KITCHIN, Rob. The Promises and Perils of Smart Cities. **Society for Computer & Law**, Bristol, 7 jun. 2015. Disponível em: http://www.scl.org/site.aspx?i=ed42789. Acesso em: 20 out. 2021.

KOOPS, Bert-Jaap; LEENES, Ronald. Privacy Regulation Cannot Be Hardcoded: A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law. **International Review of Law, Computers & Technology**, United Kingdom, v. 28, n. 2, p. 159-171, 2014. Disponível em: https://ssrn.com/abstract=2564791. Acesso em: 25 fev. 2024.

KOOPS, Bert-Jaap. On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy. **Politica e Società**, Torino, v. 3, n. 2, p. 247-264, 2014. Disponível em: https://ssrn.com/abstract=2581726. Acesso em: 10 abr. 2024.

LACERDA, Norma; FERNANDES, Ana Cristina. Parques tecnológicos: entre inovação e renda imobiliária no contexto da cidade do Recife. **Cadernos Metrópole**, São Paulo, v. 17, n. 34, p. 329-354, nov. 2015. Disponível em: https://doi.org/10.1590/2236-9996.2015-3402. Acesso em: 15 fev. 2024.

LESSIG, Lawrence. **Code 2.0**. New York: Basic Books, 2006.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 2010.

LÉVY, Vanessa. **Le droit à l'image**: définition, protection, exploitation. Zürich: Schulthess, 2002.

LI, Jane. China's facial-recognition giant says it can crack masked faces during the coronavirus. **Quartz**, [*s. l.*], 18 fev. 2020. Disponível em: https://qz.com/1803737/chinas-facial-recognition-tech-cancrack-masked-faces-amid-coronavirus/. Acesso em: 1 abr. 2021.

LIANG, Fan *et al*. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. **Policy & Internet**, United States, v. 10, n. 4, p. 415-453, ago. 2018. Disponível em: http://dx.doi.org/10.1002/poi3.183. Acesso em: 5 abr. 2021.

LIMA, Caio César Carvalho. **Marco Civil da Internet**: Garantia da privacidade e dados pessoais à luz do marco civil da internet. São Paulo: Atlas, 2014.

LUGER, Ewa *et al.* Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process. *In*: CONFERENCE ON HUMAN

FACTORS IN COMPUTING SYSTEMS, 15., 2014, Seoul. **Proceedings** […]. New York: ACM, 2014. p. 457-466.

MACSITHIGH, Daithi. Virtual walls? The law of pseudo-public spaces. **International Journal of Law**, Cambridge, v. 8, n. 3, p. 394-412, 2012. Disponível em: https://doi.org/10.1017/S1744552312000262. Acesso em: 30 mar. 2024.

MARQUES, Juliana; LEITE, Carlos. Clusters como novas possibilidades de regeneração urbana e reestruturação produtiva: o caso do Porto Digital, Recife. **Cadernos de Pós-Graduação em Arquitetura e Urbanismo**, Recife, v. 5, n. 1, p. 1-17, 2008.

MATTERN, Shannon. **Code and clay, data and dirt**. Minneapolis: University of Minnesota Press, 2017.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**: A Revolution That Will Transform How We Live, Work and Think. London: John Murray, 2013.

MAYER-SCHÖNBERGER, Viktor. General development of data protection in Europe. *In*: AGRE, Phillip; ROTENBERG, Marc (org.). **Technology and Privacy**: The New Landscape. Cambridge: MIT Press, 1997. p. 219-242.

MENEZES, José Luiz da Mota. A cidade do Recife – urbanismo lusitano e holandês. *In*: ANDRADE, Manuel Correia de Oliveira; FERNANDES, Eliane Moury; CAVALCANTI, Sandra Melo. (org.). **Tempos dos flamengos e outros tempos**: Brasil século XVII. Brasília: CNPq; Recife: Fundação Joaquim Nabuco/Massangana, 1999.

MORAES, Lucas. Porto Digital: veja as empresas que mais empregaram e faturaram em 2022. **JC**, [*s. l.*], 16 mar. 2023. Disponível em: https://jc.ne10.uol.com.br/tecnologia/2023/03/15199459-porto-digital-veja-as-empresas-que-mais-empregaram-e-faturaram-em-2022.html. Acesso em: 17 mar. 2023.

MORAIS, José Luis Bolzan de; SALDANHA, Paloma Mendes; PIMENTEL, Alexandre Freire. Estado de Direito e Tecnopoder. **Revista Justiça do Direito**, Passo Fundo, v. 35, n. 3, p. 6-43, 2021.

MOROZOV, Evgeny. **The Net Delusion**: How Not to Liberate the World. New York: PublicAffairs, 2011.

MOROZOV, Evgeny. **To Save Everything, Click Here**: The Folly of Technological Solutionism. New York: PublicAffairs, 2013.

MOZUR, Paul; FU, Claire; CHIEN, Amy Chang. How China's Police Used Phones and Faces to Track Protesters. **The New York Times**, New York, 02 dez. 2022.

Disponível em: https://www.nytimes.com/2022/12/02/business/china-protests-surveillance.html. Acesso em: 25 mar. 2024.

MÜLLER, Benedikt (org.). **Cyberspace and International Relations**: Theory, Prospects and Challenges. New York: Springer Heidelberg, 2014.

MUNDIE, Craig. Privacy Pragmatism: Focus on Data Use, Not Data Collection. **Foreign Affairs**, [*s. l.*], 12 fev. 2014. Disponível em: https://www.foreignaffairs.com/articles/2014-02-12/privacy-pragmatism. Acesso em: 20 out. 2021.

OHM, Paul. **Broken promises of privacy**: responding to the surprising failure of anonymization. UCLA Law Review, 2009.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **OECD Science, Technology and Industry Outlook 2014**. Paris: OECD, 2014. Disponível em: http://www.oecd.org/sti/oecd-science-technology-and-industry-outlook-19991428.htm. Acesso em: 28 out. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). ONU prevê que cidades abriguem 70% da população mundial até 2050. **ONU News**, [*s. l.*], 19 fev. 2019. Disponível em: https://news.un.org/pt/story/2019/02/1660701. Acesso em: 25 out. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Pacto Internacional de Direitos Civis e Políticos**. Adotado pela Assembleia Geral das Nações Unidas em 16 de dezembro de 1966. Nova York: ONU, 1966.

PASCUAL, Manuel. Quem vigia os algoritmos para que não sejam racistas ou sexistas? **El Pais**. [*s. l.*], 17 mar. 2019. Disponível em: https://brasil.elpais.com/brasil/2019/03/18/tecnologia/1552863873_720561.html. Acesso em: 03 maio 2024.

PATZ, Stéfani Reimann; PIAIA, Thami Covatti. Vigilância, perfilamento e tratamento de dados pessoais no contexto do controle migratório. **Revista Direito Público**, Brasília, v. 18, n. 100, p. 690-720, 2021. Disponível em: https://doi.org/10.11117/rdp.v18i100.5999. Acesso em: 22 fev. 2024.

PIMENTEL, Alexandre Freire; NUNES, Juliana Montarroyos Lima. O problema da proteção da privacidade diante da vulnerabilidade dos dados pessoais digitais: diagnóstico sobre o poder da governança algorítmica e os vieses cognitivos. **Humanidades & Inovação**, Palmas, v. 8, n. 48, p. 161-174, 2021. Disponível em: https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/5688. Acesso em: 22 fev. 2024.

PIMENTEL, Alexandre Freire. Tratado sobre as TICS - Direito e processo tecnológico. *In*: PIMENTEL, Alexandre Freire. **Cidadania digital e vulnerabilidade**

cibernética: LGPD e cibersegurança, redes sociais e publicidade digital. Recife: Editora Públius, 2023. v. 4.

QIN, Amy. Chinese city uses facial recognition to shame pajama wearers. **The New York Times**, Beijing, 21 jan. 2020. Disponível em: https://www.nytimes.com/2020/01/21/business/china-pajamas-facial-recognition.html. Acesso em: 11 abr. 2023.

RAMOS, Cristina de Melo. O direito fundamental à intimidade e à vida privada. **Revista de Direito da Unigranrio**, Rio de Janeiro, v. 1, n. 1, 2008.

REYNALDO, Amélia; ALVES, Paulo Reynaldo Maia. Origem da expansão do Recife: divisão do solo e configuração da trama urbana. *In*: SEMINARIO INTERNACIONAL DE INVESTIGACIÓN EN URBANISMO, 5., 2013, Barcelona, Buenos Aires. **Anais** [...]. Barcelona: DUOT, 2013. p. 877-890.

REZENDE, Laura Vilela R.; LIMA, Meyrielle R. de. Governança na internet: um estudo sobre o Marco Civil brasileiro. **Palabra Clave**, Chia, v. 19, n. 1, p. 133-155, jan. 2016. Disponível em: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0122-82852016000100006&lng=en&nrm=iso. Acesso em: 11 jun. 2023.

REZENDE, Vilela Rodrigues *et al.* Dados abertos em cidades inteligentes: uma análise da fronteira entre acesso e privacidade. **e-LiS**, [*s. l.*], 2019. Disponível em: http://eprints.rclis.org/38639/. Acesso em: 10 fev. 2024.

RIBEIRO, Laura Talho. Olhares vivos em olhos de vidro: a vigilância por meio de câmeras de monitoramento no bairro de Botafogo. **CSOnline** – Revista Eletrônica de Ciências Sociais, Juiz de Fora, n. 25, p. 1-296, 2017.

RIBEIRO, Rene. Inteligência artificial da Amazon exercitava preconceito. **Olhar Digital**, [*s. l.*], 10 out. 2018. Disponível em: https://olhardigital.com.br/2018/10/10/noticias/inteligencia-artificial-da-amazon-exercitava-preconceito/. Acesso em: 08 ago. 2023.

RIGAUX, François. **La protection de la vie privée et des autres biens de la personnalité**. Brussels: Bruylant, 1990.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução: Sanilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RONCOLATO, Murilo. O uso ilegal de dados do Facebook pela Cambridge Analytica. E o que há de novo. **Nexo Jornal**, [*s. l.*], 19 mar. 2018. Disponível em: https://www.nexojornal.com.br/expresso/2018/03/19/O-uso-ilegal-de-dados-do-Facebook-pela-Cambridge-Analytica.-E-o-que-h%C3%A1-de-novo. Acesso em: 16 nov. 2021.

SALDANHA, Nelson. O Jardim e a Praça. Campinas, SP: Yendis, 2005.

SALDANHA, Raphael de Freitas; BARCELLOS, Christovam; PEDROSO, Marcel de Moraes. Ciência de dados e big data: o que isso significa para estudos populacionais e da saúde? **Cadernos de Saúde Coletiva**, Rio de Janeiro, v. 29, n. esp., p. 51-58, 2021. Disponível em: https://doi.org/10.1590/1414-462X202199010305. Acesso em: 25 out. 2021.

SÁNCHEZ BRAVO, Álvaro A. **La protección del derecho a la libertad informática en la Unión Europea**. Sevilla: Universidad de Sevilla, 1998.

SCHREIBER, Anderson. **Direitos da personalidade**. 2. ed. São Paulo: Atlas, 2013.

SEMIDÃO, Rafael Aparecido Moron. **Dados, informação e conhecimento enquanto elementos de compreensão do universo conceitual da ciência da informação**: contribuições teóricas. 2014. 198 f. Dissertação (Mestrado em Ciência da Informação) – Programa de Pós-Graduação em Ciência da Informação, Faculdade de Filosofia e Ciências, Universidade Estadual Paulista, Marília, 2014.

SERAPIÃO, Fabio. PF mistura Inteligência Artificial e trabalho manual para identificar vândalos do Três Poderes. **Uol**, São Paulo, 24 jan. 2023. Disponível em: https://www1.folha.uol.com.br/poder/2023/01/pf-mistura-inteligencia-artificial-e-trabalho-manual-para-identificar-vandalos-dos-tres-poderes.shtml. Acesso em: 08 maio 2024.

SMITH, Sam. Barcelona named ‘Global Smart City – 2015’. **Juniper Research**, Hampshire, 17 fev. 2015. Disponível em: https://www.juniperresearch.com/press/barcelona-named-global-smart-city-2015/. Acesso em: 20 out. 2021.

SOLOVE, Daniel. The taxonomy of privacy. **Formerly American Law Register**, Pennsylvania, v. 154, n. 3, p. 477-560, 1996. Disponível em: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1376&context=penn_law_review. Acesso em: 06 mar. 2024.

SOMA, John T. **Privacy law**. St. Paul: Thomson/West, 2008.

TAYLOR, Linnet; RICHTER, Christine. Big Data and Urban Governance. *In*: GUPTA, Joyeeta *et al.* (ed.). **Geographies of Urban Governance**. Edward Elgar Publishing, 2017. p. 175-191.

TOWNSEND, Anthony. Smart Cities: buggy and brittle. **Places Journal**, [*s. l.*], out. 2013. Disponível em: https://placesjournal.org/article/smart-cities/. Acesso em: 23 out. 2021.

UNIÃO EUROPEIA. Política da Europa em matéria de Internet das Coisas. **Comissão Europeia**, Bruxelas, 2013. Disponível em: https://digital-strategy.ec.europa.eu/pt/policies/internet-things-policy. Acesso em: 10 jun. 2024.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. **Jornal Oficial da União Europeia**, Bruxelas, p. 1-88, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 1 abr. 2019.

URBAN SYSTEMS. Ranking Connected Smart Cities. **Urban Systems**, São Paulo, 2023. Disponível em: https://www.connectedsmartcities.com.br/. Acesso em: 20 out. 2023.

VALE, Maria do Socorro Costa; COSTA, Denise Coutinho; ALVES JÚNIOR, Nilton. **Internet**: Histórico, Evolução e Gestão. **CBPF**, [*s. l.*], p. 1-32, 2001. Disponível em: https://mesonpi.cat.cbpf.br/naj/InternetHEG5C.pdf. Acesso em: 20 jul. 2020.

VERMA, Pramit; RAGHUBANSHI, Akhilesh Singh. Urban sustainability and smart cities. **Environmental Sustainability**, United States, v. 1, n. 4, p. 309-320, 2018.

VIGILÂNCIA automatizada: uso de reconhecimento facial pela Administração Pública. **LAPIN**, [*s. l.*], 7 jul. 2021. Disponível em: https://lapin.org.br/2021/07/07/vigilancia-automatizada-uso-de-reconhecimento-facial-pela-administracao-publica-no-brasil/. Acesso em: 20 set. 2023.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. **Harvard Law Review**, Cambridge, v. 4, n. 5, p. 193-220, dez. 1890.

WISMAN, Tijmen H. A. Purpose and function creep by design: transforming the face of surveillance through the Internet of Things. **European Journal of Law and Technology**, Belfast, v. 4, n. 2, 2013.

ZANINI, Leonardo Estevam Assis. O surgimento e o desenvolvimento do right to privacy nos Estados Unidos. **Revista Jus Navigandi**, Teresina, ano 22, n. 5130, 18 jul. 2017. Disponível em: https://jus.com.br/artigos/57228. Acesso em: 22 jan. 2024.

ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do Right of Privacy nos Estados Unidos. **Justitia**, São Paulo, v. 70-71-72, n. 204-205-206, p. 231-250, jan./dez. 2013-2015.

ZANON, João Carlos. **Direito à proteção dos dados pessoais**. São Paulo: Revista dos Tribunais, 2013.

ZUBOFF, S. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.