ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

LGPD, CIDADES INTELIGENTES E PRIVACIDADE

Gabriel de Oliveira Cavalcanti Neto
Universidade Católica de Pernambuco, Pernambuco, Brasil
gabriel.cavalcanti.neto@gmail.com

RESUMO

Este artigo discute como e se a Lei Geral de Proteção de Dados (LGPD) controla possíveis ameaças à privacidade pessoal de cidades inteligentes e sugere pesquisas adicionais sobre duas soluções possíveis, centradas na avaliação de impacto de privacidade holística e soluções de código para sinalizar a necessidade e consequências de dar consentimento para a coleta de dados em ambientes ambientais. Segue o método dedutivo e usa como instrumentos de pesquisa a bibliográfica e monográfica.

Palavras-chave: Privacidade; LGPD; Proteção de dados; Cidades inteligentes.

ABSTRACT

This paper discusses how and if the General Data Protection Law (LGPD) controls possible threats to personal privacy in smart cities and suggests further research on two possible solutions, focusing on holistic privacy impact assessment and code solutions to signal the need and consequences of giving consent for data collection in environmental environments. It follows the deductive method and uses bibliographic and monographic research tools as research tools.

Keywords: Privacy; LGPD; Data Protection; Smart cities.

1 INTRODUÇÃO

Em termos de governança e Direito Digital, o tema “Cidades inteligentes” (CI) é um dos que ganha mais destaque no cenário jurídico. Nada obstante, a maioria das discussões acadêmicas estão centralizadas no campo tecnológico de estudos urbanos,

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

ambientais e sociológicos, em vez de jurídicos, de modo que não se preocupam prioritariamente com o aspecto regulatório do fenômeno, mas com os benefícios sociais das *smart cities*. Diante disso, persiste a necessidade de analisar a questão da privacidade e vigilância dos cidadãos.

A principal questão é a ausência de mecanismos de consentimento para o processamento de dados pessoais, além do estabelecimento de regras diretas sobre como as cidades inteligentes coletam dados privados oriundos de interações públicas, a "privatização" da propriedade da infraestrutura e dos dados, a redefinição de "big data" extraídos da IoT em cidades inteligentes e o armazenamento desses dados na nuvem.

Diante dessas questões, o presente artigo analisa eventuais ameaças que as cidades inteligentes trazem à privacidade pessoal, bem como a eficácia da regulamentação da LGPD em torno do fenômeno relacionado à Internet das Coisas (IoT); "computação ubíqua"; "Big Data"; e a nuvem.

A proposta é debater sobre como a Lei Geral de Proteção de Dados (LGPD)[1] protege ameaças à privacidade pelas cidades inteligentes e vislumbrar estudos futuros sobre dois caminhos possíveis para garantir o direito à privacidade, quais sejam: a) uma avaliação integral do impacto da privacidade para cidades inteligentes e b) formas de dar consentimento para a coleta de dados em ambientes tecnológicos.

2 O SURGIMENTO DAS CIDADES INTELIGENTES

De acordo com a ONU[2], atualmente, 55% da população mundial vive em cidades, número que chegará a 70% em 2050. Esse processo de urbanização tornou-se tão proeminente que em alguns países (p.e., Coréia do Sul) a capital gera até metade do PIB do país. Dessa forma, pode-se afirmar que algumas cidades estão se tornando mais importantes do que os países nos quais estão localizadas.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Como se sabe, globalmente, a alta densidade urbana leva inevitavelmente a problemas como o congestionamento, problemas de abastecimento e consumo de energia, emissão de gases de efeito estufa, desenvolvimento não planejado, resíduos e criminalidade. A necessidade política e social de combater esses problemas, combinada com o potencial lucrativo para empresas de tecnologia e telecomunicações que desenvolvem soluções digitais e em rede, deu origem ao conceito de cidades inteligentes[3].

De acordo com a Câmara dos Deputados[4], 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.

Esta ideia foi endossada por autoridades nacionais e municipais, grandes corporações globais de tecnologia e instituições e organizações internacionais como a Comissão Europeia[5], *Organisation for Economic Co-Operation and Development* (OCDE)[6] e *International Organization for Standardization*[7] (ISO). De acordo com Kitchin[8], 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.

Segundo a Câmara dos Deputados[4],

> 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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

As cidades inteligentes não são, portanto, apenas uma questão de produzir cidades menos poluídas ou mais eficientes, mas também 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 tecnologia. Além disso, a implementação desses recursos tende a ser por Parceria Público-Privada (PPP), que assim é definida, conforme art. 2º da Lei 11.079/2004[9]:

> 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.

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 uma das 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[10].

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

O sistema municipal do Centro, integrando dados de cerca de 30 agências, é como 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[11].

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, p.e., 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[11]. 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 viverá 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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

3 CIDADES INTELIGENTES: SEGURANÇA E PRIVACIDADE

De acordo com o Baeck e Saunders[12], 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[13]. Mesmo um simples bug pode ter um grande impacto na infraestrutura urbana[14].

A insegurança e vulnerabilidade dos sistemas de cidades inteligentes são fenômenos comuns e até reconhecidos, 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[15]. P.e., 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[15]. Carros conectados (ou “veículos autônomos”) são outro caso de uso de IoT em que a vulnerabilidade a hackers externos já foi

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

demonstrada: p.e., a Wired relatou em 2016 como o Jeep Cherokees poderia ser confiavelmente "sequestrado" por hackers externos enquanto na estrada[16].

Brown[17], 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[18]. 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"[14].

O FTC[15], 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.

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[14] afirma que a maioria das cidades está implementando novas tecnologias com pouco ou nenhum teste de segurança cibernética, o que significa que, p.e., sensores de controle de tráfego podem ser facilmente atacados.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Brown[17] acrescenta que as vulnerabilidades das CI 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.

Diante desse contexto, 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[1], 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.

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[1]. Em contraste, as cidades parecem essencialmente um espaço público, onde as expectativas de privacidade (exceto pelo anonimato) têm sido historicamente

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

reduzidas a zero. Mas, como MacSithigh[19] 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

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[19], lugares “pseudo-privados”). Koops[20] 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: p.e., 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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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[20] aponta a problemática em áreas como processo criminal. P.e., 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[21] 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, p.e., 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, p.e., 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*[22].

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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 terceiros.

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.

4 A LGPD E AS CIDADES INTELIGENTES

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

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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 um 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 NEST 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 para 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, é 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

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

que, em tais sistemas, o esquema de consentimento na LGPD não serve de salvaguardas para a privacidade do cidadão.

O art. 7º da LGPD[1] 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. – g.n.

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[1] como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada”. 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

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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[1] 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.
> 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.

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, p.e., 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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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[1], que seria uma maneira preocupantemente fácil de evitar qualquer aparência de controle do usuário. As empresas podem alegar que os dados coletados dos usuários 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[1] 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.

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 aos 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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Agora, imagine que o mesmo usuário tem 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 § § 4 e 5º do art. 7º da LGPD[1], segundo os quais:

> Art. 7º da LGPD. [...] § 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.

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, p.e., 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

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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, p.e., 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* (p.e., iniciativas de ciência cidadã).

Hoje, muitos desses dados vivem em silos; mas cada vez mais serão combinados por gestores públicos municipais e 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.

Esses enormes volumes de dados granulares gerados a partir de sistemas IoT permitem 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[23], 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 – p.e., quantidade de pessoas pisando em uma praça públicas (*fottfall*) - a relativa

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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[24]. 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 (p.e., “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[1].

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”[25], semelhante ao que acontece no episódio Nosedive, da terceira temporada da série Black Mirror.

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; à exclusão de televenda de certos produtos de luxo ou de ponta; compartilhamento de inferências comprometedoras com agências estaduais; ou mesmo a exclusão total dos mercados de

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

serviços e utilidades essenciais para aqueles que não desejam compartilhar dados pessoais.

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[8] 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.

5 BIG DATA A LGPD

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” [1]. São diversos os dispositivos nesse sentido[1].

[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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Essa 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-Schonberger e Cukier[26] dissertam, "na era do Big Data, os usos secundários mais inovadores não foram imaginados quando os dados são coletados pela primeira vez".

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[1], 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.

No entanto, em cada caso, parece evidente que a solução, é de fato, ilusória. Um consentimento geral para todas as reutilizações possíveis seria tão vago a ponto de 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.

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;

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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, p.e., 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 dados, 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[1].

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[1];

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

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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"[1].

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[27] 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.

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.

Conforma já mencionado anteriormente, 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, p.e., pelas mídias sociais e mecanismos de pesquisa para fornecer publicidade

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

direcionada, ainda permitem que os indivíduos sejam “selecionados” e sujeitos a tratamento discriminatório[27].

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[28], de certos setores da ciência[29] 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 CF.

6 A NUVEM

Obviamente, a maior parte dos dados gerados pelas cidades inteligentes será 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 sub-provedores, 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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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[1]:

> 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**. – g.n.

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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

7 CONSIDERAÇÕES FINAIS

É impressionante como, 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, p.e.: 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[30].

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

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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[31] argumentam que, quando o processamento é controlado localmente nos dispositivos, podem ser construídas restrições de código que as regras da lei que protegem os usuários, um conceito que eles chamam de "inteligência ambiental". No entanto, Koops e Leenes[32] 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,

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

> 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[1];

Esse processo deve auxiliar as organizações na identificação e minimização dos riscos de privacidade de novos projetos ou políticas, especialmente 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 isso 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 onde 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, com todos estes 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 sub-fornecedores 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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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).

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 dado no momento em que 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;

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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 persiste, 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 por meio 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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Por fim, 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.

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.

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 como um pré-requisito para manter a confiança e o engajamento dos moradores das cidades inteligentes.

O presente artigo 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

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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.

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;

f) 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.

8 REFERÊNCIAS BIBLIOGRÁFICAS

[1] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

[2] ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). ONU prevê que cidades abriguem 70% da população mundial até 2050. **ONU**, Brasil, 19 fev. 2019. Disponível em: https://news.un.org/pt/story/2019/02/1660701. Acesso em: 25 out. 2021.

[3] 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:

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

Università Commerciale Luigi Bocconi, 2013. Disponível em: https://www.academia.edu/9937385/ITAIS_2013_Dameri_Cocchia. Acesso em: 28 out. 2021.

[4] BRASIL. Câmara dos Deputados. **Cidades inteligentes**: uma abordagem humana e sustentável. 1. ed. Brasília, DF: Edições Câmara, 2021. p. 15, 21

[5] EUROPEAN UNION. European Commission. **Europe 2020**: A strategy for smart, sustainable and inclusive growth. COM(2010) 2020 final. Brussels: EUR-Lex, 2020. Disponível em: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC2020. Acesso em: 28 out. 2021.

[6] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (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.

[7] ISO; IEC JTC. **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.

[8] KITCHIN, Rob. The Promises and Perils of Smart Cities. **Smart Cities**: special focus, England, p. 1, jul. 2015. Disponível em: http://www.scl.org/site.aspx?i=ed42789. Acesso em: 20 out. 2021.

[9] BRASIL. **Lei nº 11.079, de 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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

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

[11] 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.

[12] BAECK, Peter; SAUNDERS, Tom. Rethinking Smart Cities From The Ground Up. **Nesta**, London, 2015. Disponível em: http://www.nesta.org.uk/publications/rethinking-smart-cities-ground#sthash.398wQeB1.dpuf. Acesso em: 21 out. 2021.

[13] TOWNSEND, Anthony. Smart Cities: buggy and brittle. **Places Journal**, San Francisco, 2013. Disponível em: https://placesjournal.org/article/smart-cities/. Acesso em: 23 out. 2021

[14] CERRUDO, Cesar. **An Emerging US (and World) Threat**: Cities Wide Open to Cyber Attacks. [*S. l.*]: IOActive, 2015. Disponível em: http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf. Acesso em: 10 out. 2021.

[15] FEDERAL TRADE COMMISSION (FTC). **Internet of Things**: Privacy and Security in a Connected World. USA: FTC, 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.

[16] GREENBERG, Andy. The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse. **Wired**, United States, 01 ago. 2016. Disponível em:

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/. Acesso em: 25 out. 2021.

[17] BROWN, Ian. GSR discussion paper. **Regulation and the Internet of Things**. Geneva: ITU, 2015. Disponível em: https://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf. Acesso em: 20 out. 2021.

[18] AKAMAI. State of the internet: report. **Antel**, Urugay, 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.

[19] MACSITHIGH, Daithi. Virtual walls? The law of pseudo-public spaces. **International Journal of Law in Context**, Cambridge, v. 8, n. 3, p. 394-412, 2012.

[20] KOOPS, Bert-Jaap. On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy. **Politica e Società**, Italy, v. 3, n. 2, p. 247-264, 2014.

[21] 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.

[22] 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.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

[23] WISMAN. Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things. **European Journal of Technology**, Kenya, v. 4, n. 2, p. 1-19, 2013.

[24] OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. **UCLA Law Review**, California, p. 1701-1777, 2009.

[25] CITRON, Danielle K.; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions **Washington Law Review**, Washington, v. 89, n. 1, p. 1-33, 2014.

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

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

[28] MUNDIE, Craig, Privacy Pragmatism: Focus on Data Use, Not Data Collection. **Foreign Affairs**, New York, 2014. Disponível em: https://www.foreignaffairs.com/articles/2014-02-12/privacy-pragmatism. Acesso em: 20 out. 2021.

[29] GEORGE, Robert M. Date for the Public Good: 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**: Frameworks for Engagement. Cambridge: Cambridge University Press, 2014.

ISSN: 2595-8402
DOI: 10.5281/zenodo.8077515

Publicado em 25 de junho de 2023
REVISTA SOCIEDADE CIENTÍFICA, VOLUME 6, NÚMERO 1, ANO 2023

[30] LUGER, Ewa *et al.* Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process. *In*: ANNUAL CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 33., 2015, Seoul. **Proceedings** […]. Seoul: ACM, 2015.

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

[32] 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**, London, v. 28, n. 2, p. 159-171, 2014.