UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO DO RECIFE

MARIA EDUARDA LEITE LOPES

PRIVACIDADE ENTRE 4 PAREDES: as casas inteligentes e os desafios frente aos princípios de proteção de dados pessoais

Recife
2024

MARIA EDUARDA LEITE LOPES

PRIVACIDADE ENTRE 4 PAREDES : as casas inteligentes e os desafios frente aos princípios de proteção de dados pessoais

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, como requisito parcial para a obtenção do título de bacharela em Direito.

Área de concentração: Direito Digital. Direito Internacional.

Orientador: Artur Stamford da Silva

Recife
2024

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Lopes, Maria Eduarda Leite.
Privacidade entre 4 paredes : as casas inteligentes e os desafios frente aos princípios de proteção de dados pessoais / Maria Eduarda Leite Lopes. - Recife, 2024.
55

Orientador(a): Artur Stamford da Silva
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, Direito - Bacharelado, 2024.

1. Casas inteligentes. 2. Proteção de dados pessoais. 3. Internet das Coisas. 4. Princípios de proteção de dados. 5. Sociedade da informação. I. Silva, Artur Stamford da . (Orientação). II. Título.

340 CDD (22.ed.)

MARIA EDUARDA LEITE LOPES

PRIVACIDADE ENTRE 4 PAREDES: as casas inteligentes e os desafios frente aos princípios de proteção de dados pessoais

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Universidade Federal de Pernambuco, Centro de Ciências Jurídicas, como requisito parcial para a obtenção do título de bacharela em Direito.

Aprovado em: 04/03/2024

BANCA EXAMINADORA

_____

Profº. Dr. Artur Stamford da Silva (Orientador)
Universidade Federal de Pernambuco

_____

Profº. Dra. Catarina Almeida de Oliveira (Examinador Externo)
Universidade Católica de Pernambuco

_____

Profº. Dra. Maria Antonieta Lynch de Moraes (Examinador Interno)
Universidade Federal de Pernambuco

AGRADECIMENTOS

A melhor parte, no final de tudo, é agradecer a quem esteve presente durante toda a jornada, porque pra tudo isso acontecer teve muita coisa por trás.

Agradeço primeiramente aos meu anjinhos por sempre cuidarem e estarem ao meu lado e por escutarem meus pedidos e desabafos. A Deus e ao seu Universo que me abraça todo dia. Às estrelas que me fazem sonhar e ao vento que me fala. À Nossa Senhora, mãe das mães que me fortalece na minha jornada.

E agora à minha mãe, Lourdes, meu primeiro lar, meu colo seguro, minha fortaleza, a que tem o abraço mais precioso. Lembro no 1º período da faculdade, quando tinha dúvidas juvenis de se ia conseguir enfrentar esse curso, e você como sempre, me fez relembrar quem eu era e tudo que já havia conquistado. Você estava certa, eu consegui, e muito por você. Te amo, te amo, te amo.

Ao meu pai que, quando eu era criança e estava querendo ser bióloga porque queria falar com os animais que nem a Xuxa no filme dela, me mostrou uma alternativa: um curso chamado "direito", que até então nunca tinha ouvido falar, e que a partir daí virou um sonho. Como você me disse no primeiro dia que pisei na FDR, eu conheci muito de um mundo opressor, e espero que com essa formação eu consiga defender o oprimido. Obrigada por sempre incentivar minha trajetória acadêmica.

Aos meus avós Dulce e Dário, eles não puderam estudar, mas sempre quando iam me dar alguma felicitação me desejavam boa sorte em meus estudos. Acho que por isso que eles sempre foram tão abençoados. Eu amo muito vocês. E a meus avós Terezinha e Noel, com quem não posso compartilhar essa vitória pessoalmente, mas espero que daí de cima vocês consigam me sentir.

Aos meus primos, que são meus irmãos, meus parceiros: Heitor, Heloísa, Thalles, Déborah, Yasmin, Isabel, Isadora, Ana Luisa, Anthony e Théo. Quando foi que a gente parou de brincar no quintal de vovó para ter conversas de adulto no sofá? Dividir essa conquista com vocês é muito especial. Agradeço também a meus tios: Socorro, Edival, Dário, Taciana, Maria José, Noilton, Teofilo, Milana e minha tia do coração, Etiene, por toda torcida e apoio durante toda minha vida.

Aos meus presentes da Casa de Tobias, meus piscineiros: Evelyn, Carol,

Ana Luísa, Dandara, Isabella, Carla, Luis Felipe, Lavínia, Caio, Pedro Coelho, Pedro Henrik, Lucas, Kleyton, Gabriela, Julio, Alexandre. Foram eles que dividiram angústias pré-prova, intervalos indo comprar coxinha, celebrações de aniversários com a torta da padaria por trás da faculdade, muita fofoca, a incerteza do período de modificação, e todas as outras histórias que me fizeram ter certeza que as pessoas certas foram colocadas na minha vida. Tinha que ser vocês.

Aos meus amigos que não dividiram a sala de aula da faculdade, mas dividem a vida fora dela comigo. Eles que já devem está cansados de me ouvir falar para ter cuidado na hora de compartilhar os dados, e que me fazem sentir abençoada. Com certeza vai faltar o nome de alguém aqui, mas eu preciso mencionar Paula, Tatiane, Ariane, Fernanda, Renata, Guilherme, Mendes e meus outros amigos do CMR que levo pra vida; a todos do meu grupinho do "EITA" que já considero família e compartilho tanta coisa (a gente sempre esteve na vida um do outro de uma forma ou de outra, por isso que tudo sempre flui tão fácil e é tão especial); às minhas meninas "cadaumers" que me fazem tão bem, e a todos os outros amigos que me acompanham na jornada da vida.

Ao meu orientador,Stamford, e a todos os professores que tive na vida, que me ensinaram coisas que vou levar para sempre. Aos profissionais de proteção de dados, direito digital e tecnologia com quem cruzei e que me auxiliaram a ter conhecimento e experiência na área. À LGPD, porque sim, essa lei definiu toda minha trajetória acadêmica e me permitiu ter oportunidades incríveis.

À Faculdade de Direito do Recife, por ser minha casa durante os últimos tempos. Lembro quando entrei lá pela primeira vez e me encantei, e de todos os dias que subi aquela escadaria e não acreditava que estava entrando na minha faculdade. Os momentos naqueles corredores nunca serão esquecidos e todo ensinamento adquirido ali também não.

E por último, mas definitivamente não menos importante: a mim. Por sempre me agarrar firme a quem eu sou, por ir atrás do que sonho e por todos os momentos que a minha companhia me basta e me leva adiante. Esse TCC é um pouco disso, do conhecimento que fui buscar sozinha e acabou virando parte de mim.

“The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.”

(WEISER,Mark. The computer for the 21st Century)

"Ela acreditava em anjos e, porque acreditava, eles passaram a existir" (LISPECTOR, Clarice. A hora da estrela.)

RESUMO

Na sociedade da informação, o dado pessoal é o elemento principal advindo da hiperconectividade entre pessoas, sensores e objetos. Nesse contexto, a Internet das Coisas, sendo uma tecnologia que permite ainda mais a ligação do mundo online e offline, rompe diversas barreiras e pode ser utilizada em diversas aplicações. Um exemplo são as smart houses, ou casas inteligentes, que oferecem mais conveniência no dia a dia, porém trazem consigo uma série de problemáticas relacionadas à privacidade e proteção de dados pessoais no sentido em que não conseguem se adaptar totalmente aos princípios de proteção de dados. Com isso, questionou-se quais são os principais desafios à proteção de dados pessoais em uma casa inteligente frente aos princípios de proteção de dados pessoais, sendo abordado conceitos como o de big data, privacy-by design, capitalismo de vigilância, segurança da informação e no que isso afeta a vulnerabilidade de direitos do cidadão dentro de sua própria casa. Para levantar as discussões, este trabalho utilizou do método indutivo-dedutivo, através da pesquisa bibliográfica e legislativa, procurou compreender os principais pontos que devem ser observados na criação e funcionamento da IoT dentro de casas inteligentes com base nos princípios de proteção de dados, refletiu desde a hiperconectividade, a problemática da coleta massiva de dados, transparências em políticas de privacidade, até questões de segurança da informação. O que consequentemente, levou a refletir sobre formas de como esses desafios podem ser superados para não haver nenhuma violação de direitos para que os usuários estejam inseridos em um ambiente conectado, mas também eficiente e confiável.

Palavras-chave: Sociedade informacional; Princípios de proteção de dados; Internet das Coisas; Casas inteligentes.

ABSTRACT

In the information society, personal data is the main element stemming from the hyperconnectivity between individuals, sensors, and objects. In this context, the Internet of Things, as a technology that further enables the connection of the online and offline worlds, breaks various barriers and can be utilized in diverse applications. An example is smart houses, which offer more convenience in daily life, but bring along a series of issues related to privacy and personal data protection, in the sense that they cannot fully adapt to data protection principles. Therefore, questions arise regarding the main challenges to personal data protection in a smart home concerning data protection principles, addressing concepts such as big data, privacy-by-design, surveillance capitalism, information security, and how this affects the citizen's rights vulnerability within their own home. To initiate discussions, this work employed the inductive-deductive method, through bibliographic and legislative research, seeking to understand the main points that must be observed in the creation and operation of IoT within smart homes based on data protection principles. It reflected on aspects ranging from hyperconnectivity and the issue of massive data collection to transparency in privacy policies and information security concerns. Consequently, this led to reflections on ways in which these challenges can be overcome to prevent any rights violations so that users are immersed in a connected yet efficient and reliable environment.

Keywords: Informational society; Data protection principles; Internet of Things; Smart homes.

SUMÁRIO

1 INTRODUÇÃO

Comodidade, funcionalidade, praticidade. Todas essas palavras podem ser relacionadas com a tecnologia, pois existe uma ideia de que uma de suas funções é justamente facilitar a vida dos usuários. Ao longo do tempo ela foi se inserindo em diversos cenários, como em indústria, comunicação, entretenimento, e até mesmo dentro das casas.

A união de diversos aparelhos, sensores e uma conexão com a internet faz com que uma casa "normal" torne-se uma casa inteligente, na medida em que permite que o seu morador com simples comandos ou às vezes até mesmo sem precisar deles, possa desfrutar de uma automação residencial a seu serviço. Tudo isso graças à tecnologia de internet das coisas.

Exemplo são os dispositivos de assistência pessoal/virtual como o Amazon Echo e o Google Home, que conectam diferentes dispositivos entre si por meio da Internet das Coisas (IoT) por comando de voz. Isso é chamado de uma casa inteligente, permitindo com que não seja necessário alternar entre diferentes aplicativos para operar vários eletrodomésticos como TV, forno, sistema de entretenimento ou ar condicionado, promovendo uma maior comodidade ao usuário[1].

Objetos como robô aspirador, fechadura eletrônica, luzes com controle de voz, assistente virtual se conectam entre si e trocam dados e informações, compondo esse cenário de *smart houses*. Cenário este que está em uma constante crescente, com uma taxa de crescimento anual de 10,2%, segundo dados da empresa de pesquisas internacional ReportLinker[2].

Uma vez que é uma questão atual, é necessário que regras sejam estabelecidas para que nenhum direito seja violado mediante o uso dessas tecnologias. Uma maneira bastante relevante de fazer isso é estabelecendo princípios de proteção de dados que devem ser seguidos em um tratamento de

---

[1] PANDEY, Sakshi et al. IOT based Home automation and analysis using machine learning. **SSRN**, mar 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3353476

[2] Report Linker. **Global Smart Home Services Market Size, Share & Industry Trends Analysis Report By Type**. KBV Research, fev. 2024. Disponível em: https://www.reportlinker.com/p06364748/Global-Smart-Home-Services-Market-Size-Share-Industry-Trends-Analysis-Report-By-Type-By-Regional-Outlook-and-Forecast.html?utm_source=GNW

dados. Estamos inseridos em uma sociedade hiperconectada, em que a informação tem um grande valor, e por isso os dados dos usuários passam cada dia mais a necessitar de proteção.

Porém, no cenário de tecnologia da internet das coisas, as casas conectadas enfrentam desafios à proteção de dados pessoais sob a perspectiva dos princípios de proteção de dados, tanto relacionados a limitações da própria tecnologia, quanto à falta de responsabilidade das próprias empresas.

2 PROTEÇÃO DE DADOS NA SOCIEDADE DA INFORMAÇÃO

A rápida mudança da sociedade e avanço de suas tecnologias impactam diretamente no modo de viver da população, e entender as características tecnológicas de uma sociedade é entender seu funcionamento e organização, sendo o desenvolvimento tecnológico o fator gerador das revoluções industriais.

Em um breve resumo, a 1ª Revolução Industrial foi marcada pela introdução da máquina a vapor, que teve como impacto o uso da água e do vapor para mecanização da produção que antes era meramente artesanal; a 2ª pelo advento da energia elétrica, a qual facilitou as linhas de produção e a produção em massa; a 3ª pela implementação de componentes eletrônicos e tecnologias que permitiram a automação dos processos produtivos[3].

Já a 4ª Revolução Industrial, que teve início com o século XXI, é marcada pela internet mais ubíqua e móvel, com a presença de sensores menores, mais poderosos e baratos, além da inteligência artificial, no que, com isso, foi possível a criação de sistemas e máquinas inteligentes conectados possibilitando um sistema de produção de personalização em massa[4].

É justamente aí que surge tecnologias com a internet das coisas, ou *internet of things* (IoT) em inglês, que pode ser definida como "a transformação de objetos tradicionais em inteligentes, fazendo com que os objetos físicos vejam, ouçam, tomem decisões, executem tarefas, “conversem”, compartilhem informações e coordenem decisões[5].

Quanto mais dispositivos conectados, mais dados poderão ser coletados através de diversas fontes, ou seja, um aumento tanto qualitativo, quanto quantitativo na extração de informação, sendo cada vez mais factível extrair cada vez mais conhecimento e de forma variável, e além de isso poder ser feito com maior velocidade. O que é compreensível com o fenômeno do Big Data, que não só é um grande volume de dados, mas representa muito uma atual sociedade que

---

[3] AIRES, Regina Wundrack do Amaral; MOREIRA, Fernanda Kempner Moreira; Freire Patrícia de Sá. Indústria 4.0: competências requeridas aos profissionais da quarta revolução industrial. **VII Congresso Internacional de Conhecimento e Inovação**, Foz do Iguaçu/PR, set. 2017. Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/314/153.

[4] Ibid.

[5] AL-FUQAHA, A et al. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. **IEEE Communications Surveys & Tutorials**, v. 17, ed. 4, p. 2347-2376, 15 jun. 2015. DOI 10.1109/COMST.2015.2444095. Disponível em: https://ieeexplore.ieee.org/document/7123563.

pode ser denominada da informação, em que há um fluxo contínuo de produção de dados com uma dimensão cada vez maior[6].

Logo, é possível perceber que assim como, se olharmos para trás, entende-se a influência da tecnologia em cada período da sociedade, a atual 4ª Revolução que estamos vivendo já modificou e muito a atual sociedade. Ademais, com o avanço tecnológico, o fluxo informacional foi tomando cada vez mais espaço e se tornando determinante no ciclo econômico. A informação processada e transformada em conhecimento aplicado se tornou a principal engrenagem de uma economia baseada na informação, sendo o elemento central para o desenvolvimento desta[7].

Há um fluxo cada vez maior e contínuo de geração de dados e consequente extração de informação deles, o que aumenta a hiperconexão, já que cada vez mais dispositivos estão conectados, nos acompanhando rotineiramente, coletando, armazenando e compartilhando informação[8].

Uma vez levado em conta esse cenário, é importante perceber o que tudo isso acarreta, as grandes responsabilidades e impactos de uma modernização, que influencia inevitavelmente até mesmo o cenário legislativo.

Isso porque, além de ter influenciado em uma nova revolução industrial, a internet influenciou também na concepção dos direitos fundamentais, o que para muitos doutrinadores já se pode falar em uma espécie de quarta onda/dimensão dos direitos fundamentais relacionados com a sociedade da informação, incluindo os direitos de liberdade de expressão, proteção de dados pessoais, privacidade ou direitos como do usuário da internet no mundo virtual e direito à identidade digital, sendo esses dois últimos exemplos de direitos que são muito debatidos por serem considerados completamente novos que surgiram somente porque surgiu a internet[9].

---

[6] ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização da informação. **Tecnopolíticas de vigilância**: perspectivas da margem. BRUNO, Fernanda e et al (coord). São Paulo: Boitempo, 2018.

[7] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: funções e limites do consentimento. Rio de Janeiro: Forense, 2 ed. 2020.

[8] MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV editora, 2018.

[9] MARTINEZ-VILLALBA, Juan Carlos Riofrío. La Cuarta Ola De Derechos Humanos: Los Derechos Digitales. **Revista Latinoamericana de Derechos Humanos**, [S.l.], v. 25, n. 1, p. 107-126, 2014. ISSN 1659-4304. Disponível em: https://ssrn.com/abstract=2515038.

Vale ressaltar que não é toda a doutrina que reconhece os direitos de quarta dimensão, mas a globalização inegavelmente influenciou muito os direitos já existentes que se tornaram imprescindíveis, além de trazer à tona inúmeras situações antes não previstas pelo direito, a exemplo do direito à intimidade e privacidade em decorrência da globalização e da evolução tecnológica[10].

2.1 Privacidade e proteção de dados pessoais

Com a hiperconexão, as barreiras físicas e geográficas no mundo são quase inexistentes, é possível se conectar com alguém do outro lado do mundo sem necessariamente ter que estar lá. Bem como, surgem novas funcionalidades e conveniências, a exemplo de ser possível estar fora de casa, mas poder acompanhar câmeras instaladas lá em tempo real por conta de um sistema de segurança inteligente instalado na residência. Sem deixar de mencionar a possibilidade de permitir, mesmo a distância, o acesso de uma pessoa à sua casa através de algum comando, tudo isso graças à internet.

Contudo, tais aspectos também propiciaram uma considerável ameaça aos direitos de personalidade que versam sobre privacidade e intimidade, sobretudo, em razão dos avanços tecno-científicos, podendo-se concluir que os direitos de quarta dimensão, embora fundamentais, acarretam uma série de situações que acabam por violar outros direitos indispensáveis[11].

Logo, a noção de privacidade mudou com o tempo, tendo diversos sentidos nas mais variadas sociedades e épocas, começando com um contexto mais individualista e elitista, mas logo com o crescente fluxo de informações pessoais um outro aspecto da privacidade veio à tona, que foi a sua importância para a sociedade democrática como um pré-requisito para exercício de outras liberdades fundamentais[12].

---

[10] SUKINO, Letícia Sayuri Uemura; IMAMURA, Mayara Saory. Direito à privacidade e intimidade frente aos direitos fundamentais de quarta dimensão. **ETIC - Encontro de iniciação científica**, v. 13, n. 13, 2017. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/6159.

[11] Ibid.

[12] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters, 2 ed. 2019. p. 29-31

Ou seja, à medida que ia acontecendo um crescimento do fluxo informacional, houve um aumento da capacidade técnica de recolher, processar e utilizar dados e ,com isso, obter informação. Nesse sentido, a temática da privacidade passou a se estruturar em torno da informação e mais especificamente dos dados pessoais, pois a proteção de dados pessoais traz o tema da privacidade, mas modifica seus elementos e toca nos pontos centrais dos interesses em questão[13].

Se olhado o cenário mundial atualmente, a proteção de dados pessoais é um tema que se encontra cada vez mais regulado, uma demonstração disso é que de acordo com um estudo feito pelo UNCTAD – United Nations Conference on Trade and Development 66% dos países no mundo possuem legislação de privacidade e outros 10% estão com lei em fase de aprovação[14], o que demonstra ser um tema que possui atenção e preocupação global e é inerente a atual sociedade. Sem deixar de mencionar que em um contexto de tecnologia, as barreiras geográficas são quase inexistentes, como já apontado, o que possibilita a aparição de problemas comuns a vários ordenamentos.

2.1.1 PRINCÍPIOS DE PROTEÇÃO DE DADOS

A tecnologia ocupa cada vez mais um papel importante na sociedade, e que está cada vez mais difícil separar a vida real da vida virtual, pois no dia a dia das pessoas está cada vez mais recorrente fazer uso de aparelhos tecnológicos que se comunicam e trocam informações entre si. Com isso, é preciso uma resposta rápida às mudanças na tecnologia que aumentaram a coleta, disseminação e uso de informações pessoais.

Uma vez que não é possível estar atualizando leis a todo momento, uma base principiológica desempenha um importante papel na interpretação e aplicação de casos concretos em defesa da proteção de dados pessoais.

---

[13] DONEDA, op. cit., p. 136, 172, 173.

[14] United Nations Conference on Trade and Development. **Data Protection and Privacy Legislation Worldwide**, dez. 2021. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em 14 set. 2022.

Os princípios servem para incorporar o espírito do regime geral de proteção de dados, e estar em conformidade com o espírito deles é um alicerce fundamental para boas práticas de proteção de dados[15].

Apesar de existirem países com legislação de proteção de dados, contendo disposições detalhadas específicas de cada um, é possível perceber que internacionalmente há uma convergência no que diz respeito aos princípios guias para proteção de dados.

Exemplo disso são os frameworks de privacidade, que são utilizados como ferramentas para ajudar a pensar e enquadrar discussões sobre privacidade e a compreender os requisitos de privacidade, tendo como relevante destaque os Princípios de Privacidade da OCDE (*Organisation For Economic Co-Operation And Development*), que estão refletidos nas leis de privacidade e proteção de dados existentes e emergentes e servem como base para a criação de outros programas de privacidade e princípios adicionais[16].

Como também a Convenção 108, que tem como objetivo reconhecer a necessidade de promover a nível global, os valores fundamentais do respeito pela privacidade e da protecção dos dados pessoais, contribuindo assim para o livre fluxo de informação entre as pessoas[17]. Sem deixar de mencionar a LGPD (Lei Geral de Proteção de Dados), e a GDPR (*General Data Protection Regulation*), legislações de proteção de dados brasileiras e da União Europeia, respectivamente. Em todos eles podem ser observados princípios orientativos para a proteção dos dados pessoais. Alguns deles são:

- Minimização
- Integridade e confidencialidade (segurança)
- Transparência, justiça e legalidade
- Limitação de propósito
- Acurácia

---

[15]ICO (Information Commissioner 's Office). **A guide to data protection principles**. Londres: ICO, [s.d.]. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/. Acesso em 11 jan. 2024

[16] GERBER, Ben. **OECD Privacy Principles**. OECD, 2020. Disponível em: http://oecdprivacy.org/

[17] Convenção 108 do Conselho da Europa. **Convenção para a Proteção das Pessoas em Relação ao Tratamento Automatizado de Dados de Caráter Pessoal**. Número da Convenção: 108. Data de Assinatura: 28 de janeiro de 1981. Local de Assinatura: Estrasburgo. Ratificação pelo Brasil: 10 de setembro de 2003. Promulgação pelo Brasil: Decreto nº 4.509, de 10 de dezembro de 2002. Publicação: Diário Oficial da União, Seção 1, de 11 de dezembro de 2002.

- Limitação de armazenamento
- Responsabilidade/ Deveres das Partes

Logo, estes princípios devem estar no centro da abordagem ao tratamento de dados pessoais em todas as fases.

3 INTERNET DAS COISAS E AS *SMART HOUSES*

A IoT é quase como uma conexão entre todas as coisas e a Internet. O conceito IOT foi cunhado por um membro da Rádio Comunidade de desenvolvimento de identificação de frequência (RFID) em 1999, e vem se tornando mais e mais relevante, em grande parte devido ao crescimento dos dispositivos móveis, comunicação incorporada e onipresente, computação em nuvem e análise de dados[18].

Essa tecnologia cria um novo mundo, na medida em que permite com que

> bilhões de objetos possam sentir, comunicar e compartilhar informações, todas interligadas redes públicas ou privadas de protocolo da Internet (IP). Esses objetos interconectados têm dados regularmente coletados, analisados e usados para iniciar a ação, fornecendo uma riqueza de inteligência para planejamento, gestão e tomada de decisão. Isto é o mundo da Internet das Coisas (IOT)[19]

A tecnologia de IoT possui diversas aplicações, uma delas é a de que a presença de dispositivos IoT em uma casa faz com que ela se torne o que é chamado de *smart house,* nela estão presentes sensores e atores que supervisionam o ambiente da casa e do habitante, se conectando com outros dispositivos e auxiliando e assistindo os moradores nas suas atividades diárias[20].

O termo *smart house* foi primeiro utilizado em 1999, por Kevin Ashton, cofundador do Laboratório Auto-ID do MITO, usando-o para descrever um sistema onde a Internet está conectada ao mundo físico por meio de sensores onipresentes, incluindo RFID (Identificação por radiofrequência)[21].

Nelas é possível notar a conexão de diversos dispositivos que estão presentes no lar, como a televisão, as lâmpadas, celular, geladeira, assistentes virtuais, entre outros. Logo, a conexão com a mesma rede de internet permite uma integração entre eles, oferecendo mais conveniência no dia a dia. Isso vai desde receber um alerta no celular de quando está ficando sem comida na

---

[18]PATEL, Keyur K.; PATEL, Sunil M.; SCHOLAR, P. Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. I**nternational journal of engineering science and computing**, v. 6, n. 5, 2016. Disponível em: http://www.opjstamnar.com/download/Worksheet/Day-110/IP-XI.pdf

[19] Ibid

[20] HAIGH, Karen Zita; YANCO, Holly A. Automation as caregiver: a survey of issues and technologies. **AAAI Technical Report** WS-02-02. Disponível em: https://www.aaai.org/Papers/Workshops/2002/WS-02-02/WS02-02-007.pdf.

[21] ASHTON, Kevin. That “Internet of Things” thing. **RFiD journal**, v. 22, p. 97-114, 2009.

geladeira, a começar a passar o jornal matinal na televisão no instante que a pessoa se acorda.

Isso se relaciona a ideia defendida pelo futurista Jason Morgan[22], de que o conceito de IoT se refere basicamente a conectar qualquer dispositivo com um botão liga e desliga à Internet (e/ou entre si). O que pode ser visto aplicado nas casas inteligentes, pois inclui desde celulares, cafeteiras, máquinas de lavar, fones de ouvido, lâmpadas, dispositivos vestíveis e muitos outros, o que leva à conhecida máxima "tudo que pode ser conectado, será conectado".

Sem contar que é uma tecnologia em ascensão, como pode ser percebido em pesquisas como a da IoT Analytics, que concluiu que o número de dispositivos IoT conectados em 2023 foi de 16,7 bilhões a nível global, o que representa um crescimento de 16% em relação ao ano anterior, e a estimativa é a de que até 2027 provavelmente existam mais de 29 bilhões de conexões IoT[23].

É importante ressaltar que uma casa inteligente é uma casa conectada, mas nem toda casa conectada é uma casa inteligente. Isso porque a casa conectada necessita de comandos do usuário para que as atividades sejam executadas e na casa inteligente podem ser feitas programações para que elas sejam realizadas de forma automática em determinados momentos[24], é como se a casa inteligente fosse uma evolução da casa conectada. Logo, quando utilizado nesse trabalho o termo "casa inteligente" ou "smart house" se fala também das casas conectadas visto que estão inclusas no conjunto maior, apesar de estas não possuírem algumas problemáticas que são decorrentes justamente da automatização que caracteriza as casas inteligentes.

Porém, a tendência que se pode perceber nessas casas é a de um lugar em que tudo funciona de forma automática e não exige esforço do usuário, uma presença ubíqua. A "computação ubíqua", termo que foi usado pela primeira vez pelo cientista de informática norte americano Mark Weiser, em seu artigo "The

---

[22] MORGAN, Jacob. A Simple Explanation Of 'The Internet Of Things'. **Forbes**, 13 mai. 2014. Disponível em: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=4db41a221d09. Acesso em: 20 nov. 2023.

[23] SINHA, Satyajit. **State of IoT 2023. I**ot analytics, 24 mai. 2023. Disponível em: https://iot-analytics.com/number-connected-iot-devices/. Acesso em 30 nov. 2023

[24] EXISTE diferença entre casa conectada e casa inteligente?. **Desktop blog**, 25 abr. 2023. Disponível em: https://www.desktop.com.br/blog/casa-conectada-e-casa-inteligente/. Acesso em: 30 nov. 2023

Computer for the 21st Century[25], traz a ideia de que assim como fios nas paredes, centenas de computadores tornar-se-ão invisíveis à consciência comum e as pessoas simplesmente os usarão inconscientemente para realizar tarefas diárias e que existirão centenas de computadores em uma única sala.

3.1 Problemáticas relacionadas à privacidade

Pode-se entender a ideia de ubiquidade como diretamente relacionada às casas inteligentes, porém essa comodidade traz consigo algumas problemáticas, principalmente no que se refere à privacidade.

> Além de mostrar algumas das maneiras pelas quais os computadores podem entrar de forma invisível na vida das pessoas, esta especulação aponta algumas das questões sociais que a virtualidade incorporada irá gerar. Talvez o principal deles seja a privacidade: centenas de computadores em cada sala, todos capazes de detectar pessoas próximas e ligados por redes de alta velocidade, têm o potencial de fazer com que o totalitarismo até agora pareça a mais pura anarquia. Assim como uma estação de trabalho em uma rede local pode ser programada para interceptar mensagens destinadas a outras pessoas, uma única aba não autorizada em uma sala poderia potencialmente registrar tudo o que aconteceu lá.
> Ainda hoje, embora os crachás ativos e as agendas de compromissos auto-escritas ofereçam todo o tipo de conveniência, nas mãos erradas as suas informações podem ser sufocantes[26].

Isso porque pode ser feito um uso fora da legítima expectativa dos titulares dos dados coletados, com a utilização do conjunto das informações que justamente tornam os computadores invisíveis tão convenientes. A medida que cada vez mais dispositivos estão sendo conectados com cada vez mais velocidade e baixa latência (isto é, o tempo que uma solicitação leva para ser transferida de um ponto a outro) a ideia de ubiquidade fica cada vez mais possível de ser percebida e por isso os possíveis impactos que isso pode ocasionar à proteção de dados necessita ser avaliado.

O que está vinculado com a ideia de privacidade pois, como disse Danilo Doneda[27], há uma mudança na clássica ideia de privacidade como um direito a

---

[25] WEISER, Mark. The Computer for the 21st Century. **Scientific American**, v. 265, n. 3, p. 94-104, 1991. Disponível em: https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf

[26] Ibid.

[27] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters, 2 ed. 2019.

"ser deixado só", já que agora se fala do isolamento e da reclusão em um cenário no qual há um grande fluxo de informações que cresce cada vez mais. Com isso, as demandas que moldam o perfil da privacidade mudam de ordem e começam a ser relacionadas à informação pessoal e condicionadas pela tecnologia.

O exemplo mencionado pelo autor é o de que "a exposição indesejada de uma pessoa aos olhos alheios se dá hoje com maior frequência através da divulgação de seus dados pessoais do que pela intrusão em sua habitação"[28]. Todavia, uma vez que a tecnologia está sendo inserida até mesmo dentro de casa, como no caso das *smart house*s, a exposição desses dados pode revelar ainda mais questões relacionadas à esfera íntima do indivíduo. Isso porque muitos dispositivos os quais normalmente não se conectavam a rede, estarão presentes nas casas, podendo coletar dados, gerar informações para análises e monitoramentos, bem como automatizar tarefas ou prover alguma facilidade ao usuário[29].

> Atualmente, existem sensores para capturar quase todas as informações do meio ambiente. Alguns exemplos de sensores são imagem, vídeo, som, proximidade de local, temperatura, umidade, aceleração, pressão, gás e batimentos cardíacos, Em um mundo onde os dados se tornaram um ativo lucrativo, o universo da Internet das Coisas está cada vez mais cheio de sensores que se apresentam como uma legítima ameaça. A coleta descontrolada de informações em ambientes sensíveis, como nas Smart Homes, que requerem forte proteção de dados e controles de privacidade, é um exemplo típico. Não adianta se cercar do que há de melhor em tecnologia avançada, comodidades totais para o bem-estar, exuberantes processos de automação, integração e interatividade, se o inimigo está literalmente dentro de casa[30].

Tudo isso faz com que essa problemática tome maiores proporções e mereça ser discutida e mais aprofundada, pois um tratamento de dados deve seguir regras visando proteger o usuário, como seguir princípios de proteção de dados. Todavia, existem algumas barreiras até mesmo técnicas para essa conformidade, que é o que passará a ser melhor abordado posteriormente.

---

[28] Ibid., p.23

[29] SINGER, 2012 apud OLIVEIRA, Nairobi Spiecker de; et al. Segurança da Informação para Internet das Coisas (IoT): uma abordagem sobre a Lei Geral de Proteção de Dados (LGPD). **Revista Eletrônica de Iniciação Científica em Computação**, v. 17, n. 4, p.4, 2019. Disponível em: https://seer.ufrgs.br/reic/article/view/88790. Acesso em 11 ago. 2022.

[30] ALVES, Davi; PEIXOTO, Mário; ROSA, Thiago. **Internet das coisas (iot)**: segurança e privacidade de dados pessoais. Rio de Janeiro: Alta books, 2021.

4 PRINCÍPIOS DE PROTEÇÃO DE DADOS E APLICAÇÃO NAS CASAS INTELIGENTES

Como já falado anteriormente, em uma casa inteligente, há uma série de dispositivos que irão interagir entre si oferecendo uma espécie de comodidade para o habitante. Todavia, é importante mencionar que por trás dessas facilidades, existem problemáticas que atingem esferas de direitos dos usuários de maneiras diferentes, e que muitas vezes nem se passa na cabeça das pessoas na hora de adquirir os produtos, ou se passa, são ignoradas em prol de uma vida mais prática e fácil.

Isso porque permite, por exemplo, não precisar mais se preocupar em esquecer a chave de casa já que esta possui uma fechadura eletrônica na residência, ou não ter a necessidade de se levantar para acender as luzes, pois é só dizer um comando em voz alta para a assistente pessoal, entre outros.

Destarte, é importante falar de como ter uma casa inteligente pode impactar nos direitos de privacidade e proteção de dados das pessoas, isso porque as 4 paredes de uma casa pressupõem segurança, uma vez que alguém estando dentro de sua casa, estaria teoricamente segura. Porém, o uso desses dispositivos pode estar afetando essa segurança de uma maneira invisível disfarçada de comodidade e inovação, o que vai contra os princípios norteadores de um tratamento de dados.

Muitos acordos foram implementados num grande número de países, e a níveis globais, para regular as práticas de informação pessoal no interesse da protecção da privacidade e de outros direitos humanos dos indivíduos, sendo aplicados alguns princípios de proteção de dados que podem ser vistos como uma aplicação de normas éticas e de direitos humanos ao caso do processamento de informações[31]. Sem deixar de mencionar que:

> Os sistemas reguladores para a privacidade foram construídos com base num conjunto tradicional de princípios, que dão origem a regras e diretrizes para a recolha e tratamento justos de dados pessoais, assumindo um tanto heroicamente que “dados pessoais” é um conceito razoavelmente claro[32]. (tradução nossa)

---

[31] RAAB, Charles D. Regulating surveillance: The importance of principles. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David. **Routledge handbook of surveillance studies**. Nova Iorque: Routledge, 2012.
[32] Ibid.

Embora os países possam diferir na numeração e na redação dos princípios, em várias interpretações nacionais existem requisitos para que os dados sejam tratados de maneira a seguir os princípios mencionados no tópico 2.2.1.

Por isso, a partir de agora será analisado o que deve ser observado no tratamento de dados em uma casa inteligente em relação aos princípios. Para o propósito e limitação desta tese, o foco será no princípio da minimização, segurança, transparência e delimitação de propósito, os quais serão analisados exemplos de situações, problemáticas jurídicas e possíveis soluções.

4.1 Minimização

A minimização de dados é um princípio de privacidade que estabelece que os dados pessoais coletados não devem ser mais do que o necessário para a finalidade específica autorizada pelo usuário[33].

Pode ser encontrada referência a esse princípio em regulamentos como:

- LGPD no art.6, III : "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".[34]
- OCDE: “Os dados pessoais devem ser relevantes para os fins em que são utilizados e, na medida do necessário para aqueles propósitos, devendo ser precisos, completos e mantidos atualizados[35].”
- Convenção 108 no artigo 5, 4, c: “Os dados pessoais submetidos a tratamento serão adequados, relevantes e não excessivos em relação aos fins para os quais são processados[36].”

---

[33] PINISETTY, Srinivas et al. Monitoring data minimisation. **arXiv**, v. 1, jan. 2018. Disponível em: https://arxiv.org/abs/1801.02484

[34] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

[35]ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). Manual de Oslo: Diretrizes para a coleta e interpretação de dados sobre inovação. 3 edição. Paris: OCDE, 2005.

[36] Convenção 108 do Conselho da Europa. op cit.

- GDPR no art 5, 1, c: “Os dados pessoais serão adequados, relevantes e limitados a o que é necessário em relação aos fins para os quais são processados[37]."

Ou seja, transmite a ideia de que para determinada função, os dados coletados devem ser os mínimos possíveis, coletando somente o que é realmente necessário, e os dados coletados para além disso que não teriam justificativa para a coleta, sendo um tratamento indevido e excessivo, devendo então ter a garantia de que os dados coletados não são mais do que o necessário para os fins para os quais os dados serão usados.

4.1.1 O PRINCÍPIO DA MINIMIZAÇÃO EM CASAS INTELIGENTES

Quando se fala em casas inteligentes, se parte da ideia de que quanto mais dispositivos estiverem conectados entre si, mais inteligente é essa casa, e quanto mais dispositivos, maior a coleta e fluxo de dados, o que é oposto do que é a minimização.

Existe nessas casas uma troca de informações entre os diversos dispositivos presentes nela para que eles atuem na funcionalidade da residência. Ou seja, um dispositivo que por si só iria coletar determinados dados, acaba por coletar mais, uma vez que recebe informações de outros dispositivos para poder exercer alguma funcionalidade dentro da casa.

Por exemplo, há sensores equipados em dispositivos do dia a dia capazes de captar aspectos do mundo real, como temperatura, umidade, presença, etc, enviá-los a centrais que recebem estas informações e as utilizam de uma forma inteligente[38], como deixar a temperatura da casa sempre a mais "agradável possível".

Isso está relacionado à lógica da comodidade de uma casa inteligente, na medida em que "os objetos inteligentes e interconectados podem efetivamente nos ajudar na resolução de problemas reais. Do ponto de vista dos consumidores,

---

[37] UNIÃO EUROPEIA. Regulação 2016/679, de 27 de abril de 2016. Regulamento Geral de Proteção de Dados. Jornal Oficial da União Europeia, 04 mai. 2016.

[38] NASCIMENTO, Rodrigo. O que, de fato, é internet das coisas e que revolução ela pode trazer? **IT forum**, 12 mar. 2015. Disponível em: https://itforum.com.br/noticias/o-que-de-fato-e-internet-das-coisas-e-que-revolucao-ela-pode-trazer/. Acesso em 12 dez. 2023

os produtos que hoje estão integrados com a tecnologia da IoT são das mais variadas áreas e têm funções diversas, como eletrodomésticos[39]".

> O refrigerador Samsung RF28HMELBSR/AA, por exemplo, é equipado com uma tela LCD capaz de reproduzir a tela de seu smartphone no refrigerador. É possível reproduzir vídeos e músicas, consultar a previsão do tempo e até mesmo fazer compras online enquanto verifica na geladeira os itens que precisam ser comprados. O refrigerador traz ainda um app chamado Epicurious, que permite a consulta de receitas online[40].

Por isso que estar em conformidade com o princípio da minimização se encontra como uma questão a ser analisada e, com o aumento cada dia mais da capacidade computacional dos dispositivos e a ascensão do 5G, o número de dados coletados tende a aumentar, influenciando na adequação ao princípio discutido.

4.1.1.1 A ascensão do 5G e o impacto na capacidade de coleta de dados na indústria de Internet das Coisas

A tecnologia 5G está cada dia em ascensão, e isso cria impacto em diversos setores, afetando a capacidade e velocidade da coleta de dados. Uma vez que uma casa inteligente se encontra equipada com uma série de dispositivos ligados à internet, a ascensão do 5G irá impactar diretamente essa capacidade de processamento e, consequentemente, haverá uma coleta de dados ainda maior, o que interfere no princípio da minimização de coletar o mínimo de dados possível.

A informação e as TIC 's (tecnologias de comunicação) podem ser consideradas ingredientes chaves para o desenvolvimento social e econômico, isso porque vem criando novas conveniências e benefícios que não eram experimentados anteriormente[41]. Por exemplo, desde que o serviço de rede sem fio 4G foi introduzido, as pessoas começaram a ser capazes de usufruir de serviços de banda larga com seus dispositivos móveis como *smartphones* e

---

[39] MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV editora, 2018, p. 46.
[40] NASCIMENTO op cit.
[41] HEEJUNG, Yu; HOWON, Lee; HONGBEOM, Jeon. What is 5G? Emerging 5G Mobile Services and Network Requirements. **Sustainability**, [S.l.], v. 9, n. 10, p. 1848, 2017. DOI: 10.3390/su9101848. Disponível em: https://www.mdpi.com/2071-1050/9/10/1848.

tablets, e isso fez com que a experiência do usuário final se tornasse quase equivalente à das conexões sem fio[42].

Ou seja, tudo isso começou a fazer cada vez mais parte do dia a dia das pessoas, não sendo mais possível separar uma experiência da outra, pode-se dizer até que é como se uma vida offline não existisse mais, pois a tecnologia passou a ser parte do dia a dia e até mesmo essencial para realizar tarefas cotidianas.

> Isso fez com que aumentasse a necessidade de um serviço com alta velocidade, resposta rápida, alta confiabilidade e eficiência energética, e consequentemente esses recursos tornaram-se requisitos essenciais para serviços futuros na era 5G, já que as redes 4G/LTE não podem fornecer serviços de nuvem instantâneos, Internet tátil, Internet das coisas (IoT) e comunicação com drones e robôs, garantindo ao mesmo tempo qualidade de experiência aos usuários móveis. Além disso, as redes LTE podem fornecer experiência de vídeo de alta qualidade apenas para um número limitado de usuários móveis simultaneamente (tradução nossa).[43]

Logo, pode-se perceber que há um impacto direto na tecnologia IoT, já que a evolução das redes de quinta geração (5G) está se tornando mais prontamente disponível como um dos principais impulsionadores do crescimento das aplicações IoT, acompanhado de novos critérios de desempenho, como conectividade massiva, segurança, confiabilidade, cobertura de comunicação sem fio, latência ultrabaixa, rendimento, ultra confiável, etc. fornecendo novas interfaces de conectividade para as futuras aplicações IoT[44].

Tudo isso leva a necessidade de espectro de banda larga para atender às demandas do tráfego em rápido crescimento, que será mais atendida com o 5G, uma vez que aborda os principais desafios de uma rede de forma mais eficaz em comparação com seus antecessores, permitindo maior largura de banda e consequentemente maior taxa e coleta de dados, conectividade massiva, maiores capacidades computacionais dos dispositivos, baixa latência de ponta a ponta e serviços inteligentes prestados pelos dispositivos[45].

---

[42] Ibid.
[43] Ibid.
[44] LI, Shancang; XU, Li Da; ZHAO, Shanshan Zhao. 5G Internet of Things: A survey. **Journal of Industrial Information Integration**, v. 10, p. 1-9, jun. 2018. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S2452414X18300037
[45] SHAFIQUE Kinza et al. Internet of things (IoT) for next-generation smart systems: a review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. **IEEE Access**, vol. 8, p. 23022-23040, 2020. Disponível em: https://ieeexplore.ieee.org/abstract/document/8972389

Isso é facilmente percebido em um contexto de casas conectados, pois de acordo com pesquisa da IDC, o mercado de dispositivos para casas inteligentes cresceu 11,7% em 2021 e o esperado é que mantenha um crescimento a dois dígitos até 2026, com principal destaque a produtos de entretenimento, segurança/monitoramento doméstico e controle de Iluminação.

> com a chegada do 5G, que será um grande impulsionador dessa tecnologia, esses equipamentos, uma vez interconectados, poderão realizar funções e atividades combinadas a fim de facilitar a vida de seus usuários, baseando-se em seus gostos, desejos, atividades recomendadas e outras informações que os apoiarão em tomadas de decisões inteligentes, conhecimentos que serão adquiridos através de inteligência artificial e aprendizado de máquina — machine learning[46]

Isto é, a medida que o mercado da tecnologia IoT aumenta em geral, aumenta também o do seu uso no cenário doméstico, o que necessita cada vez mais de redes de conexão mais robustas que permitam essa múltipla troca de dados e informações cada vez maior à medida que possui mais dispositivos conectados e oferecendo serviços. Ou seja, uma conectividade para além da telefonia, a internet de todas as coisas.

É inegável que o avanço do 5G tenha contribuído para uma maior propagação da tecnologia de IoT e consequentemente sua aplicação em smart houses, trazendo com isso o desafio de desenvolvimento de aplicações seguras e que preservem os direitos de seus usuários. Porém, com essa maior capacidade de coleta de dados, percebe-se uma ideia de maior preocupação com poder coletar uma grande quantidade de informações, mas sem se preocupar com as consequências disso para os usuários, sem contar que vai contra a minimização estabelecida para uma coleta de dados adequada.

Dessa maneira o 5G contribui ainda mais para o Big Data, o que impacta diretamente na coleta do mínimo de dados necessários.

4.1.1.2 Big data x minimização

O princípio da minimização propõe utilizar a menor quantidade de dados possível, o que é justamente o oposto do que acontece com a Internet das Coisas. O conceito de necessidade implica uma avaliação de se o mesmo

---

[46] ALVES, Davis; PEIXOTO, Mário; ROSA, Thiago. **Internet das coisas (iot)**: segurança e privacidade de dados pessoais. Rio de Janeiro: Alta books, 2021.

objetivo poderia ser alcançado de uma forma menos intrusiva, ou seja, usando menos dados, um equilíbrio entre o meios utilizados e o objetivo pretendido [47].

Essa grande quantidade de dados apresenta diversos desafios, uma vez que requerem armazenamento e processamento significativos para permitir que a Internet das Coisas (IoT) alcance todo o seu potencial, estando relacionado com o fenômeno de Big Data, uma vez que são processados extensos conjuntos de informações.

No contexto atual os volumes de dados pessoais gerados e coletados em ambientes de big data são enormes, surgindo o dilema entre a exploração eficiente desses dados e a garantia da privacidade dos indivíduos, criando um cenário de maior responsabilidade na manipulação de informações pessoais[48].

Portanto, realizar uma filtragem de dados focada na minimização, seja no momento da coleta ou do armazenamento dos dados, restringindo apenas ao mínimo necessário, ao que realmente será utilizado e terá utilidade para a necessidade específica em que a ação se propõe o uso dos dados é o principal desafio que se pode enfrentar no uso da tecnologia IoT nas smart houses[49]. Isso porque "em cenários de big data, esta análise focada na minimização dos dados se demonstra complexa devido aos múltiplos propósitos que a organização pretende empregar na sua coleta e processamento"[50].

Vejamos um exemplo, em casas inteligentes podem ser utilizados alguns sensores

> Ao detectar o menor sinal de vazamento de gás ou fumaça em um ambiente, estes aparelhos são acionados e emitem avisos sonoros para alertar o usuário. Com a finalidade de tornar a residência ainda mais segura, a tecnologia envia notificações – em tempo real – para o smartphone, alertando os moradores do problema mesmo quando eles não estão em casa. [...] Por ser conectado diretamente à rede Wi-Fi, o

---

[47]https://edps.europa.eu/sites/edp/files/publication/16-06-16_necessity_paper_for_consultation_en.pdf

[48]DOS SANTOS, Ranieri Alves; SCANDOLARA, Daniel Henrique; MOHR, Eduarda Talita Bramorski. Desafios da lgpd na governança de dados pessoais em cenários de big data. in: DALMARCO Eduardo Monguilhott; FANTONELLI Miliane; WAZLAWICK Raul (coord.) **Mostra Científica da Proteção de Dados na Saúde, Tecnologia e Poder Público**.Florianópolis: UFSC, 2023. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/251199/ebook2023_final.pdf?sequence=1#page=9https://repositorio.ufsc.br/bitstream/handle/123456789/251199/ebook2023 _final.pdf

[49] Ibid

[50] Ibid

> usuário não precisa providenciar uma central de comando à parte, garantindo maior praticidade e conforto[51].

Esses sensores, de maneira inicial, podem ser focados em uma ou duas variáveis, como por exemplo, verificação da temperatura, vibração etc. Porém, a quantidade de informações coletada por todos os equipamentos na linha de produção pode ser gigantesca, pois estão incluídas várias variáveis. Quando as máquinas podem coletar múltiplas variáveis, a quantidade de dados é ainda maior.

Outro caso é o de adaptadores de tomada inteligente:

> A ferramenta bivolt (110V e 220V) permite controlar e agendar remotamente o funcionamento de dispositivos e eletrodomésticos como luminárias, cafeteiras e umidificadores de ar, entre outros. Gerenciado por comando de voz via assistentes virtuais ou por aplicativo, o sistema permite que o usuário acompanhe o consumo de energia em tempo real e programe o uso para economizar nos gastos.
> Com o smartphone, é possível desligar os eletrônicos de forma remota, dentro ou fora de casa, e, ainda, criar rotinas programadas para, por exemplo, ativar a cafeteira todos os dias no mesmo horário e garantir um café fresco todas as manhãs.

Isso também pode ser feito com instalação de sensores sensores de consumo de energia instalados em dispositivos como geladeira, máquina de lavar, televisão etc.

Nesse caso, a finalidade do tratamento é a economia de energia, porém além de realizar esse monitoramento do consumo de energia, também haverá a coleta de dados sobre a rotina dos moradores, podendo gerar inferências relacionadas a horários de refeições, hábitos de sono, entre outros.

Ou seja, os dados coletados não estão sendo somente os necessários para a finalidade, indo contra o princípio da minimização, realizando uma coleta excessiva.

4.1.1.3 Inferências de dados

Ademais da grande quantidade de informações coletadas, incluindo as além das realmente necessárias para atingir o fim, esses dispositivos também

---

[51] CARMEN, Gabriela Del. Smart Home: 10 tecnologias essenciais para deixar a sua casa mais inteligente. **Forbes Tech**, ago. 2021. Disponível em: https://forbes.com.br/forbes-tech/2021/08/smart-home-10-tecnologias-essenciais-para-deixar-a-sua-casa-mais-inteligente/#foto9. Acesso em 19 jan. 2024

podem criar inferências a partir dos dados coletados (o que gera mais informações).

Tudo isso é baseado no objetivo principal de uma casa inteligente, que é o de que o sistema de automatização de uma smart house ter que ser capaz de prever o comportamento do usuário com base nos dados coletados, desenvolvendo uma consciência situacional, ou seja, compreender as intenções do usuário em um determinado momento e ajustar parâmetros de acordo[52].

Uma maneira de fazer isso possível é através do *machine learning* (aprendizado de máquina) e mineração de dados, que são utilizados para transformar um sistema comum de automação residencial em um Sistema de Automação Residencial Inteligente, prevendo o comportamento do usuário[53].

Ou seja, para além dos dados já coletados, é possível que se gere outros tipos de informação. Isso porque o dado em si é como um fato bruto, que quando aplicada uma inteligência por cima, ou organizando, processando, se converte em algo a mais, algo inteligível do qual pode-se extrair informações e gerando uma dinâmica de um sistema de informação, permitindo com que conhecimento seja produzido e revertido para uma tomada de decisão[54].

Um exemplo seria o de entender os hábitos do morador da casa para saber que ele trabalha de segunda a sexta, acordando sempre às 8h, mas só chega na cozinha às 8h30, pois é o tempo que toma banho. Neste caso, às 8h da manhã vai soar o alarme para acordar a pessoa, as cortinas vão se abrir, e às 8h30 o café vai estar pronto na máquina, estando ainda quente quando a pessoa for tomá-lo.

> A aprendizagem de máquina e a mineração de dados podem utilizar esses dados fornecidos pelos sensores para compreender a atividade dos usuários, analisar o problema e fornecer padrões apropriados como saída. Por fim, o sistema toma decisões considerando todos os parâmetros[55].

Essa questão mostra mais uma vez o grande volume de dados, pois o Big Data seria como uma espécie de êxtase desse processo, permitindo que um volume descomunal de dados seja estruturado e analisado para uma gama

---

[52] PANDEY, Sakshi et al. IOT based Home automation and analysis using machine learning. **SSRN**, mar 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3353476
[53] Ibid
[54] BIONI, op cit
[55] PANDEY, op cit (tradução nossa)

indeterminada de finalidades[56]. Está assim, associado a 3 (três) V 's: Volume, Variedade e Velocidade, pois excede a capacidade de tecnologias tradicionais de processamento, conseguindo organizar quantidades antes inimagináveis e em diversos formatos em alta velocidade[57].

Essa questão acaba impactando também em um caso de possível vazamento de dados (tópico a ser abordado posteriormente). A quantidade de informações de um usuário que serão divulgadas por conta de uma falha de segurança será muito grande, contendo informações super detalhadas da rotina de uma pessoa em sua casa, seus hábitos, costumes, etc.

Isso é bastante perigoso e coloca o titular em uma situação de bastante vulnerabilidade, pois não se sabe quem terá acesso a essas informações e o que será feito a partir disso, sendo suscetível a ser vítima de extorsão, golpes e ameaças.

4.1.1.4 Privacy by design como um aliado à minimização

O *privacy by design* é um termo criado por Ann Cavoukian, e é utilizado para definir a ideia de valorizar a privacidade desde a concepção do produto, tendo ela como parte do sistema e incorporada ao design do produto. Composto por 7 princípios[58], o *privacy by design*, visa incorporar a privacidade a todos os processos, sistemas, ferramentas, produtos e serviços, minimizando o impacto da tecnologia na privacidade das pessoas, criando assim um produto que beneficie todos os lados.

Um dos princípios do *privacy by design* é o *privacy by default*, que seria a implementação de padrões para que os dados pessoais sejam automaticamente protegidos em qualquer sistema de TI ou prática comercial, de maneira em que se um indivíduo não fizer nada, sua privacidade ainda permanece intacta[59]. Ou seja, nenhuma ação seria necessária por parte do indivíduo para proteger sua privacidade pois ela é incorporada no sistema, por padrão.

---

[56] BIONI, op. cit
[57] Ibid
[58]CAVOUKIAN, Ann. Privacy by design: the 7 foundational principles. **Information and Privacy Commissioner of Ontario**. Toronto, 2009. Disponível em: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
[59] Ibid

O *privacy by default* também é composto de princípios, e um deles é justamente a ideia de minimização, pois a coleta de dados deve ser limitada ao necessário para os fins especificados e a coleta de informações pessoalmente identificáveis deve ser restrita ao mínimo[60]. Isso busca assegurar que somente os dados pessoais essenciais para alcançar um determinado propósito sejam coletados, utilizados, armazenados e eliminados de maneira apropriada.

Além disso, "o design de programas, tecnologias da informação e comunicação, e sistemas devem começar com interações e transações não identificáveis como padrão. Sempre que possível, a identificabilidade, observabilidade e possibilidade de vinculação de informações pessoais devem ser minimizadas[61]". Ou seja, a utilização de técnicas de anonimização e pseudonimização para proteger a identidade dos usuário

Isso é uma maneira de garantir mais privacidade para os usuários pois, a quantidade de dados coletados é muito grande, a quantidade de informações que se teria de uma pessoa é alta, e caso haja um vazamento de dados, o impacto será bem maior.

A identificação é um risco, pois essa associação de um conjunto específico de dados à identidade de alguém é uma ameaça à privacidade de proteção de dados, e as tecnologias de IoT estão mais sujeitas a esse risco devido às possibilidades de identificação facial e por meio de digitas do indivíduo[62].

Mas vale pontuar que:

> Um dos principais problemas de privacidade nos produtos inseridos no cenário de IoT seria a ilusão da anonimização. É bem verdade que a problemática da falsa anonimidade dos dados não é um problema exclusivo deste tipo de tecnologia, estando presente na maior parte dos serviços e produtos de que os indivíduos fazem uso cotidianamente. O teórico Paul Ohm, ao tratar dos riscos para a privacidade, já criticava o fato de se acreditar piamente na anonimização dos dados.
> Ainda que um dado tenha sido suprimido para garantir a privacidade do usuário, um adversário (como é chamado na literatura científica) pode identificá-lo (ou desanonimizá-lo) por meio do cruzamento de outras informações sobre o usuário disponíveis na rede. Isso pode, inclusive, acarretar a descoberta da identidade real da pessoa[63].

Um dos motivos pelos quais isso acontece é que "os sensores podem captar uma multiplicidade de informações de forma tão rica, correlacionando

[60] Ibid
[61] Ibid
[62] MAGRANI, op cit.
[63] Ibid

diferentes tipos de dados, que cada indivíduo possui uma espécie de "marca" que o diferencia dos outros usuários"[64]. Ou seja, a implementação dessa técnica é recomendada, mas devido a coleta de tantos dados (*Big Data*) e ao processamento que é feito em cima deles (*machine learning*), ela já não é mais tão eficaz.

Com isso, uma possível solução para as empresas responsáveis pelos produtos presentes em uma casa inteligente continua sendo o compromisso com o *privacy by design*. Isso inclui, além do já mencionado, a definição clara dos propósitos pelos quais os dados estão sendo coletados e a certificação de que cada tipo de informação está sendo coletada exclusivamente para atender a uma finalidade específica e legítima. Isso pode ser demonstrado em políticas de privacidades com fins também de garantir transparência (que será melhor abordada no seguinte tópico).

4.2 Integridade e confidencialidade

Esse princípio diz respeito à segurança e proteção aos dados pessoais durante todo o tratamento.

Pode ser encontrado referência a ele em regulações como:

- OCDE: "Os dados pessoais devem ser protegidos por salvaguardas de segurança razoáveis contra riscos como perda ou acesso não autorizado, destruição, uso, modificação ou divulgação de dados[65]."
- Convenção 108 no artigo 7, 1[66]: "Cada Parte deve dispor que o controlador, e, quando aplicável, o processador, adote medidas de segurança apropriadas contra riscos como acesso acidental ou não autorizado, destruição, perda, uso, modificação ou divulgação não autorizada de dados pessoais."
- LGPD no artigo 6, VII - "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de

---

[64] Ibid

[65] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). Manual de Oslo: Diretrizes para a coleta e interpretação de dados sobre inovação. 3 edição. Paris: OCDE, 2005.

[66] Convenção 108 do Conselho da Europa. op cit.

situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"[67].

- No artigo 5, 1, f da GDPR: "Os dados pessoais devem ser processados de maneira que garanta a segurança apropriada dos dados pessoais, incluindo proteção contra processamento não autorizado ou ilegal e contra perda, destruição ou dano acidental, utilizando medidas técnicas ou organizacionais apropriadas"[68].

Ou seja, pode-se entender como o objetivo de proteger os dados por meio de medidas de segurança contra riscos como por exemplo, acesso, uso e divulgação não autorizados, sem deixar de mencionar a perda e destruição.

A segurança da informação é composta justamente do fundamento da confidencialidade, que "é o modo de assegurar que as informações trocadas entre os dispositivos sejam trafegadas de um modo seguro, garantindo que apenas pessoas autorizadas tenham acesso a tal informação[69]", e também da ideia de integridade. Esse processo pode ser entendido como uma garantia de que uma determinada ação executada pelo sistema ocorra de forma inteira, ou seja, que durante o processamento os dados e o fluxo da informação não tenham sido alterados[70].

4.2.1 SEGURANÇA EM CASAS INTELIGENTES

Mais uma vez ressalta-se que a casa é para ser o lugar seguro de uma pessoa, então o princípio da segurança merece uma especial atenção. O uso de tecnologias IoT que compõem uma casa e a fazem ser inteligente devem observar medidas de segurança para proteger os dados e garantir a segurança das informações coletadas, sem deixar o usuário em situação de vulnerabilidade e sujeito a vazamentos, acesso indevido, entre outras falhas de segurança.

> Em um mundo cada vez mais conectado, surgem riscos relacionados às ameaças virtuais, vulnerabilidades e a ataques cibernéticos que a IoT pode trazer consigo. Além dos riscos relacionados, também será

[67] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018.
[68] UNIÃO EUROPEIA. Regulação 2016/679, de 27 de abril de 2016. Regulamento Geral de Proteção de Dados. Jornal Oficial da União Europeia, 04 mai. 2016.
[69] MORAES, Alexandre de; HAYASHI Victor Takashi. **Segurança em IoT**: entendendo os riscos e ameaças em internet das coisas. Rio de Janeiro: Alta books, 2021.
[70] Ibid

> necessário o envolvimento dos fabricantes de tecnologia com o objetivo de aprimoramento dos níveis de segurança de seus produtos a fim de evitar possíveis violações, ataques e consequências aos seus consumidores.[71]

É importante ressaltar também que a proteção dos dados em uma *smart house* é uma questão muito importante, uma vez que os dispositivos contêm uma grande camada de informação sobre os usuários (como abordado no tópico anterior) e também inclui dados sensíveis[72] (como a biometria coletada em uma fechadura eletrônica). Isso faz com que esses dispositivos se tornem um dos alvos mais importantes para hackers, sem contar que eles contêm algumas das principais razões que ajudam os hackers a acessá-los e integrar programas maliciosos, como falta de conscientização sobre as ameaças e riscos associados a esses dispositivos e contam com a facilidade de disseminação e aquisição de dispositivos inteligentes em todos os lugares[73].

Logo, é importante garantir a segurança e proteção dos dados e informações tanto quando em movimento (quando a informação trafega entre os distintos sistemas) quanto nos dados armazenados (em repouso)[74].

Como ressaltado por Eduardo Magrani[75], estudioso da temática de IoT, a interconectividade pode gerar uma série de problemáticas e revelar fragilidades em relação à privacidade e segurança dos usuários. A tecnologia está avançando mas as empresas não conseguiram garantir de maneira suficiente a segurança e privacidade dos dados. Isso impacta também na responsabilidade de cada empresa que opera na cadeia dos dispositivos conectados, pois uma vez que há mais dispositivos, há um maior volume de dados coletados e de operadores que atuam na cadeia econômica.

4.2.1.1 Violações de dados

Um dos possíveis incidentes de segurança é o vazamento/violação de dados, a ICO (International Commissioner's Office) - órgão de regulação de

---

[71] ALVES, Davis; PEIXOTO, Mário; ROSA, Thiago. op cit
[72] São dados de categoria especial, relacionados à cor, raça, dados de saúde, biométricos etc.
[73] ALBANY, Mada et al. A review: Secure Internet of thing System for Smart Houses. **Procedia computer science,** v. 201, p. 437-444, 2022. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877050922004707
[74] MORAES, Alexandre de; HAYASHI Victor Takashi. op cit
[75] MAGRANI, Eduardo, op cit.

proteção de dados no Reino Unido e referência mundial - define vazamento de dados como

> um incidente de segurança que afeta a confidencialidade, integridade ou disponibilidade de dados pessoais. Em resumo, haverá um vazamento de dados pessoais sempre que algum dado pessoal for perdido, destruído, corrompido ou divulgado acidentalmente; se alguém acessar os dados ou os repassar sem a devida autorização; ou se os dados ficarem indisponíveis e essa falta de disponibilidade tiver um efeito significativamente negativo sobre os indivíduos[76].

Em uma casa inteligente há uma grande quantidade de informações coletadas e acontecem inúmeros tratamentos, estando suscetível a alguma violação ou incidente de segurança.

Isso sem contar que a vulnerabilidade aumenta uma vez que os dispositivos IoT em si possuem riscos. Por exemplo, em relação a falta de atualização

> Muitos destes dispositivos não passam por atualização durante toda a sua vida útil, ou seja, criam vulnerabilidades no sistema operacional, no seu gerenciamento web, nos protocolos de comunicação, acabam sendo possíveis de serem exploradas. Muitos fabricantes simplesmente não geram atualizações com receio de quebrar alguma funcionalidade[77].

Se os dispositivos não são atualizados eles estão mais sujeitos a ataques que exploram suas vulnerabilidades e permitem seu acesso. Outro problema é a baixa capacidade computacional desses dispositivos já que, como ressaltado pelos teóricos "os protocolos tradicionais e a criptografia atual demandam uma grande quantidade de memória e recursos de computador, o que dificulta sua implementação em alguns objetos que fazem uso da tecnologia de IoT"[78].

Tudo isso demonstra uma maior preocupação para caso haja uma violação de dados pessoais, e isso já é uma realidade. Em 2021, um estudo da Universidade da Carolina do Norte, nos Estados Unidos apontou que a Alexa, assistente pessoal da Amazon apresentava falhas que facilitariam o vazamento de dados dos usuários. Isso estava relacionado ao processo processo de aprovação das skills, que são os softwares feitos para a assistente virtual[79].

---

[76]ICO (Information Commissioner 's Office). **Personal data breaches: a guide**. Londres: ICO, [s.d.]. Disponível em: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

[77] MORAES, Alexandre de; HAYASHI, Victor Takashi op cit.

[78] MAGRANI, Eduardo op cit.

[79] ALVES, Paulo. Estudo aponta falhas na Alexa que podem revelar informações importantes. **Techtudo**. Disponível em: https://www.techtudo.com.br/noticias/2021/03/estudo-aponta-falhas-na-alexa-que-podem-revelar-informacoes-importantes.ghtml. Acesso em 30 jan. 2024

> Alguns aplicativos poderiam, por exemplo, funcionar como espiões acionados por comando de voz, o que tornaria a falha ainda mais perigosa, principalmente para quem utiliza a assistente virtual para consultar a conta bancária. Ao abrir o aplicativo, portanto, o usuário poderia, sem perceber, entregar os dados de acesso a um hacker.
> [...]
> O sistema poderia induzir o usuário a acreditar que está usando um aplicativo de seu serviço de streaming de música ou sistema de iluminação inteligente acionado via Alexa, quando, na verdade, estaria diante de uma cópia perigosa do app[80].

Outra situação[81] envolvendo esse mesmo dispositivo aconteceu quando milhares de funcionários da Amazon que puderam ouvir gravações de voz de usuários da Alexa, no período entre agosto de 2018 e setembro de 2019. Os áudios captados pelos alto-falantes ativados por voz da assistente pessoal vazaram para 30 mil funcionários, e muitos deles sequer trabalhavam em produtos habilitados para Alexa. A empresa permitiu aos funcionários acesso excessivamente amplo aos dados pessoais e não divulgou a prática aos usuários, o que configura uma violação/vazamento de dados.

Tudo isso auxilia para demonstrar que uma vez que os dispositivos conectados a uma casa inteligente passam a ter cada vez mais importância no cotidiano das pessoas, é fundamental que eles garantam uma segurança e confiabilidade. As empresas precisam proteger as informações e os dados coletados pelos seus dispositivos, oferecendo requisitos mínimos de segurança em seus produtos[82].

Uma possível solução é, da mesma maneira que o Inmetro faz em suas áreas de atuação, emitir um selo que, para ser recebido, os fabricantes teriam que seguir à risca as melhores práticas, sendo estipulado um patamar mínimo de segurança para os dispositivos e aplicando penalidade para os fabricantes e desenvolvedores que tivessem incidentes de segurança sem ter seguido as melhores práticas[83].

---

[80] Ibid
[81] ÁUDIOS da Alexa vazam para 30 mil funcionários da Amazon de forma indevida. **Invest news**, 3 jun. 2023. Disponível em: https://investnews.com.br/geral/audios-da-alexa-vazam-para-30-mil-funcionarios-da-amazon-de-forma-indevida/. Acesso em 30 jan. 2024
[82] CANDIDO, Enzo Raian Teixeira; MOURA, José Antão Beltrão. **Segurança e privacidade em assistentes pessoais**. Tese (bacharelado em ciência da computação) - Centro de engenharia e informática, Universidade Federal de Campina Grande. Campina Grande, 2023. Disponivel em: http://dspace.sti.ufcg.edu.br:8080/xmlui/bitstream/handle/riufcg/29302/ENZO%20RAIAN%20TEIXEIRA%20CANDIDO%20-%20TCC%20ARTIGO%20CI%c3%8aNCIA%20DA%20COMPUTA%c3%87%c3%83O%20CEEI%202023.pdf?sequence=1&isAllowed=y
[83] Ibid

O que é fundamental de ser cumprido também e já é trazido pelos mais diversos regulamento de proteção de dados, é o comunicado aos titulares em caso de algum incidente de dados que afete o titular, "a comunicação dos incidentes é de suma importância, ela iria alertar os usuários dos dispositivos sobre as falhas, além de orientá-los sobre como mitigar o problema, seja com uma simples alteração de senha ou com atualizações de software fornecidas pelos fabricantes"[84].

É muito importante que essa segurança seja garantida, uma vez que

> Em pouco tempo, provavelmente teremos nosso cotidiano monitorado, em sua grande parte, por meio dos produtos de IoT. Dessa maneira, a privacidade do consumidor é um importante tópico de discussão: caso os dados obtidos não sejam submetidos a um processo de proteção confiável, isso pode causar graves violações à privacidade[85].

Logo, seguir à risca o princípio da segurança é primordial em uma casa inteligente, com fins a não afetar os direitos de privacidade e proteção de dados do titular.

4.2.1.2 Capitalismo de vigilância e privacidade entre 4 paredes

Uma outra ameaça a segurança da informação que os usuários de uma casa inteligente estão sujeitos é uma vigilância constante.

Com o avanço tecnológico, o fluxo informacional foi tomando cada vez mais espaço e se tornando determinante no ciclo econômico, a informação processada e transformada em conhecimento aplicado se tornou a principal engrenagem de uma economia baseada na informação, sendo o elemento central para o desenvolvimento desta[86], e como bem dito por Danilo Doneda[87], "a tecnologia, juntamente com as mudanças que ocorrem no tecido social definem o contexto em que a informação e a privacidade se relacionam".

Contudo, tais aspectos também propiciaram uma considerável ameaça aos direitos de personalidade que versam sobre privacidade e intimidade, sobretudo, em razão dos avanços tecno-científicos.

---

[84] Ibid
[85] MAGRANI op cit
[86] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: funções e limites do consentimento. Rio de Janeiro: Forense, 2 ed. 2020.
[87] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters, 2 ed. 2019.

O que acontece é que atualmente, essa enorme quantidade de dados (big data) gera uma nova lógica de acumulação, profundamente intencional e com importantes consequências, que pode ser chamado de "capitalismo de vigilância"[88]. Isso deixa o usuário vulnerável, e, quando se fala em casas inteligentes, o lar de uma pessoa é o lugar em que ela deveria se sentir mais segura, pois ela teoricamente estaria protegida pelas 4 paredes da vista dos outros.

Mas existe uma nova forma de capitalismo que busca de certa forma prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado, e vem se formando gradualmente durante a última década, incorporando novas políticas e relações sociais que ainda não haviam sido bem delineadas ou teorizadas[89]. Com isso, "o capitalismo de vigilância, mediante o uso de tecnologias algorítmicas, consegue não só monitorar o comportamento dos indivíduos, mas submetê-los a um novo controle que se instala no interior de suas mentes[90], o que acaba por afetar a segurança do usuário, pois não possui mais controle do que é feito com seus dados e também se encontra vigiado dentro de sua própria casa.

Pode-se perceber uma vigilância constante por parte das empresas através da coleta de inúmeros dados dentro da residência de uma pessoa, que acontece por meio de inúmeros dispositivos, permitindo que se saiba preferências e hábitos dos usuários[91].

É o que acontece em cenários normais do dia a dia, comuns em uma casa inteligente, como assistir televisão em uma *smart TV*, utilizar computador para realizar as atividades de escola ou trabalho e também para fazer buscas pessoais, ou até mesmo pedir para uma assistente pessoal colocar uma música. São situações habituais e que em uma smart house tornam-se até mesmo sinônimo de conveniência, mas por trás dessa facilidade há o risco da vigilância.

> O que muitos não sabem é que os alto-falantes inteligentes são capazes de monitorar e entender a fala dos seus usuários e através da detecção

[88] ZUBOFF,Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda et al. **Tecnopolíticas da vigilância**. São Paulo, Boitempo, 2018.p. 17-68
[89] Ibid.
[90] CRUZ, Sylvio Augusto de Mattos.Big data e o fim do livre arbítrio: a democracia manipulada. **Pensar acadêmico**, Manhuaçu, v.19, n.3, p.1083-1102, set.-dez., 2021. Disponível em: https://www.pensaracademico.unifacig.edu.br/index.php/pensaracademico/article/view/2536/2091.
[91] MAGRANI op cit.

> acústica eles conseguem informações sobre o que a pessoa está fazendo, em qual cômodo ou local ela está inserida no momento e até mesmo dados de consumo que posteriormente podem ser negociados para grandes empresas que querem anunciar para seus consumidores.[92]

Logo, assistir uma televisão pode estar gerando um monitoramento do perfil de consumo, e as televisões inteligentes (*smart tvs*) também podem estar utilizando esses dados para diversos propósitos que não deixam claro em suas políticas de privacidade[93]. O que se percebe então é que, a privacidade pode estar por sofrer ameaças em diversos aspectos da vida cotidiana até mesmo dentro de uma residência.

4.2.1.3 Security by design: um olhar sobre a segurança desde o princípio

O privacy by design, como abordado anteriormente, tem o objetivo de implementar a privacidade desde a concepção de um produto, e um dos seus princípios é justamente o "end-to-end security":

> Medidas de segurança robustas são essenciais para a privacidade, desde o início até o fim. Isso garante que todos os dados sejam retidos de forma segura e, posteriormente, destruídos de maneira segura ao final do processo, de maneira oportuna. Assim, a Privacidade por Design assegura uma gestão segura do ciclo de vida da informação, de ponta a ponta, do início ao fim[94].

A criadora do privacy by design ainda afirma que o princípio da segurança tem uma especial relevância, pois sem uma segurança forte não é possível ter privacidade, e ressalta que as entidades devem assumir a responsabilidade pela segurança das informações pessoais, além da importância de os padrões de segurança aplicados têm que assegurar a confidencialidade, integridade e disponibilidade dos dados pessoais ao longo de todo o seu ciclo de vida, incluindo, métodos de destruição segura, criptografia adequada e métodos robustos de controle de acesso e registro[95].

Ao lado do privacy by design, já está se falando em um conceito de *security by design*, com a ideia de pensar a segurança de um dispositivo desde a sua concepção. A ver a definição da Agência de cibersegurança e infraestrutura de segurança dos Estados Unidos:

---

[92] CANDIDO, Enzo Raian Teixeira; MOURA, José Antão Beltrão. op cit.
[93] GHIGLIERI, Marco; VOLKAMER, Melanie; RENAUD, Karen. Exploring consumers' attitudes of smart TV related privacy risks. *In*: TRYFONAS, Theo. (Ed.) **Human Aspects of Information Security, Privacy and Trust**. Vancouver: Springer, 2017, p. 656-674.
[94] KAVOUKIAN, op cit.
[95] Ibid

> São aqueles nos quais a segurança dos clientes é uma exigência central do negócio, não apenas uma característica técnica. Os princípios de "Secure by Design" devem ser implementados durante a fase de design do ciclo de desenvolvimento de um produto para reduzir drasticamente o número de falhas exploráveis antes de serem introduzidos no mercado para uso ou consumo generalizado[96].

Pode-se perceber então o quanto a segurança é valorizada e primordial em um produto ou serviço, e mostra que as medidas de segurança devem ser consideradas, sendo promovida a utilização de repositórios de informação de segurança, relacionando soluções, ameaças, vulnerabilidades e políticas de segurança e encorajando a incorporação das melhores práticas nos processos de desenvolvimento[97].

Dessa maneira, a organização deve adaptar os seus processos, métodos e ferramentas, para que os conceitos tanto de Security by Design quanto o de Privacy by Design passem a fazer parte as metodologias de desenvolvimento[98], fazendo com que as organizações consigam obter um maior nível de segurança nas suas aplicações e, com isso, maior confiabilidade e proteção ao usuário.

4.3 Princípio da Justiça, legalidade e transparência e Princípio da Finalidade

Justiça, legalidade e transparência é mais um princípio de proteção de dados, e diz respeito aos dados pessoais serem processados de maneira legal, transparente e justa.

A Justiça e a Transparência são essenciais para garantir que os dados das pessoas não sejam usados de maneiras que elas não esperariam. Já a Legalidade significa que os dados devem ser processados de maneira que respeite o estado de direito e que atenda a uma base legal para o processamento.

---

[96] CISA (Cybersecurity and Infrastructure Security Agency). **Shifting the balance of cybersecurity risk**: principles and approaches for secure by design software. [s.l.] abr. 2023. Disponível em: https://www.cisa.gov/resources-tools/resources/secure-by-design

[97] OLIVEIRA, Manuel Maria Marques Pinto da Costa. **Privacidade no ciclo de vida do desenvolvimento seguro**. Tese (mestrado em engenharia informática) - Faculdade de ciências, Universidade de Lisboa. Lisboa, 2019. Disponível em: https://repositorio.ul.pt/handle/10451/40204

[98] Ibid

Vale ressaltar que uma "base legal" é uma justificativa para o processamento dos dados das pessoas estabelecida por lei.[99]

Esse princípio se relaciona com o da finalidade/delimitação de propósito, no qual estabelece que os dados devem ser processados apenas para fins específicos, explícitos e legítimos. Esse princípio impede que haja uma excessiva liberdade de quem coletou os dados em relação aos dados pessoais dos indivíduos. Dessa forma, o princípio promove transparência, equidade e legitimidade, se conecta ao princípio que foi primeiramente definido.[100]

Pode ser encontrada referência a esses princípios em regulamentos como:

- OCDE[101]: "Deveria haver limites para a coleta de dados pessoais e tais dados deveriam ser obtidos por meios legais e justos" e "Os propósitos para os quais os dados pessoais são coletados devem ser especificados até o momento da coleta de dados, e o uso subsequente deve ser limitado ao cumprimento desses propósitos ou de outros que não sejam incompatíveis com esses propósitos e que sejam especificados em cada ocasião de mudança de propósito".
- Convenção 108 no artigo 5 (3) e (4)(a)[102]: "Os dados pessoais em processo de tratamento devem ser processados de maneira legal" e "Os dados pessoais em processo de tratamento devem ser processados de maneira justa e transparente". E Artigo 5 (4)(b): "Os dados pessoais em processo de tratamento devem ser coletados para fins explícitos, especificados e legítimos e não processados de forma incompatível com esses propósitos".
- GDPR[103]: "Os dados pessoais devem ser processados de maneira legal, justa e transparente em relação ao titular dos dados" no Artigo 5 (1)(a). E no Artigo 89, 1: "Os dados pessoais devem ser coletados para fins

---

[99] PRIVACY INTERNATIONAL. **A guide for policy engagement on data protection**. Londres, set. 2018. Disponível em: https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf

[100]HÄRDLING, Emma. **Data protection in the smart home**: do data subjects have control over the AI-generated inferences drawn about them from the smart devices in their homes?. Tese (mestrado em direito da União Europeia) - Departamento de direito, Universidade de Uppsala. Uppsala, 2022. Disponível em: https://www.diva-portal.org/smash/get/diva2:1716359/FULLTEXT01.pdf

[101] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). Manual de Oslo: Diretrizes para a coleta e interpretação de dados sobre inovação. 3 edição. Paris: OCDE, 2005.

[102] Convenção 108 do Conselho da Europa. op cit.

[103] UNIÃO EUROPEIA. Regulação 2016/679, de 27 de abril de 2016. Regulamento Geral de Proteção de Dados. Jornal Oficial da União Europeia, 04 mai. 2016.

específicos, explícitos e legítimos e não devem ser processados posteriormente de maneira incompatível com esses propósitos"

- LGPD[104] art 6, inciso VI: "transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial". E inciso I: "finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades".

4.3.1 APLICAÇÃO DOS PRINCÍPIOS EM CASAS INTELIGENTES

A ideia desses princípios é de garantir um tratamento de dados legal, o que significa garantir confiabilidade ao titular, informando-o do que está sendo feito com seus dados, e garantindo que só será feito com eles o que lhe foi informado.

Na IoT[105], o processamento transparente se torna mais complexo, pois os dados "pulam" de um dispositivo para outro muito mais vezes do que o habitual antes de chegarem ao seu destino, onde serão armazenados permanentemente. Portanto, para as empresas, será mais difícil rastrear onde cada bloco de dados está, não apenas para visualização e transparência, mas também para fins de apagamento.

4.3.1.1 Políticas/Aviso de privacidade

As políticas de privacidade possuem cunho orientativo e funcionam como um instrumento legal do fabricante para com o cliente, sendo um mecanismo de comunicação que além de informar, ajuda o usuário a entender o que de fato poderá ser absorvido perante a utilização de seus produtos e serviços, tudo isso de forma explicativa[106]. A disponibilização da política de privacidade é uma forma mais direta de demonstrar ao usuário o que está sendo feito com seus dados,

---

[104] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018.
[105] ALVES, Davi; PEIXOTO, Mário, ROSA, Thiago. op cit.
[106] ALVES, Davi; PEIXOTO, Mário, ROSA, Thiago. op cit.

informando-o quais os dados coletados, a finalidade da coleta, como os dados serão utilizados, com quem serão compartilhados etc.

> Uma vez conectados, os serviços geralmente têm uma política de privacidade, na qual afirmam que tipos de dados coletam e para que fins. Geralmente é obrigatório aceitar esse documento antes de se usar o serviço, e isso é considerado consentimento, mas esse é um documento estático, que não se encaixa na dinâmica da natureza da IoT[107].

É necessário que as organizações implementem abordagens mais seguras e transparentes nos processos que envolvam dados pessoais, sendo necessária a revisão, ou criação de políticas de privacidade, para garantir mais segurança e transparência no processamento dos dados volumosos[108].

Todavia, existem desafios técnicos para tal, pois "muitos objetos carecem de uma interface (como uma tela ou um teclado) que possibilite ao usuário interagir com o software do objeto, conhecendo a política de tratamento de dados e consentindo no uso de suas informações. Em razão dessa dificuldade, algumas empresas do setor optam por explicitar a política de privacidade em seus sites"[109]. Ou seja, diante desse cenário, o usuário acaba por não ter acesso a essa política, e fica sem saber o que está sendo feito com seus dados.

O que acontece também é que raramente essas políticas são publicadas por todos os fabricantes, e quando são, não ficam facilmente disponíveis ou fáceis de serem encontradas, e ainda existem os casos em que nem política de privacidade o fabricante tem. Isso impossibilita que o cidadão-usuário que adquiriu, por exemplo, uma Smart TV tenha conhecimento daquilo a que poderia estar vulnerável, como sua informação a ser captada, absorvida, até mesmo antes de adquirir sua Smart TV, pois se houvesse algum recurso em que ele pudesse consultar, poderia se informar melhor antes de decidir pela compra[110].

Um ponto que merece destaque é que, em uma casa inteligente, uma pessoa nem sempre é um usuário ativo do serviço que esteja coletando seus dados, sendo por exemplo um visitante ou funcionário. Essa pessoa não fornece nenhum tipo de aceite para o tratamento e pode estar completamente inconsciente de que seus dados estão sendo coletados e o que está sendo feito

---

[107] Ibid.
[108] SCARAMUZZA, Lara Vitória Silva; GODOY, Henri Alves de. Segurança da informação aplicada em big data. **FatecSeg-Congresso de segurança da informação**. 2022. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/70
[109] MAGRANI op cit.
[110] ALVES, Davis; PEIXOTO, Mário; ROSA, Thiago. op cit

com eles, sendo a única solução para isso muitas vezes, desligar o(s) sensores(s), e isso faz com que que efetivamente interrompa completamente o sistema e a funcionalidade da casa[111].

Outra problemática é o de que existe uma omissão nessas políticas, pois algumas empresas falham no dever de informação, já que não informam na política questões importantes como de quem seria a posse dos dados oriundos de sensores e como se daria o tratamento desses dados[112].

Ou então, existe a questão de ter uma política, mas há o risco de abrir mão de certos recursos que se preconiza com a privacidade. Por exemplo, as Smart TV's da Samsung possuem uma política de privacidade em que há um trecho em que ressalta o risco de captura e transmissão de dados sensíveis se a função de reconhecimento de voz estiver ligada: “Para fornecer a função de reconhecimento de voz, alguns comandos de voz poderão ser transmitidos para um serviço de terceiros, que converte fala para texto ou para a extensão necessária para a função”, e "Por favor, esteja ciente que se suas palavras incluírem dados pessoais ou outras informações sensíveis, essa informação estará entre os dados capturados e transmitidos para terceiros pelo uso do reconhecimento de voz”[113].

Essa função permite que ao invés de utilizar o controle remoto, o espectador possa controlar o aparelho apenas pela voz, bastando ligar a função e conectar a televisão à internet. Dessa forma, se o usuário abrir mão desse recurso em prol da privacidade (não ter informações sensíveis coletadas e transmitidas para terceiros) ele não terá acesso a uma funcionalidade que lhe garante mais praticidade e que é de certa forma um diferencial desse televisor para outro.

É crucial que o indivíduo seja claramente informado e consciente de como seus dados serão processados, e por quem. Se houver intenção de compartilhar os dados de um indivíduo com terceiros, mas o fabricante não for transparente sobre esse fato e o titular dos dados não for claramente informado, é provável que os dados pessoais tenham sido obtidos de forma injusta e o processo não será considerado transparente.

---

[111] Ibid.
[112] Ibid
[113] https://www.samsung.com/hk_en/info/privacy/smarttv/

4.3.1.2 Garantindo transparência e limitando finalidade no ambiente de smart houses

Diante das questões acima mencionadas, é interessante discutir como a transparência pode ser mais garantida dentro do contexto de uma casa inteligente. Deve ser possível fornecer informações claras e compreensíveis ao titular dos dados sobre o propósito do processamento de dados pessoais, a base legal e os destinatários das informações. Isso pode ser alcançado por meio do design de interfaces de usuário amigáveis à privacidade, que evitam padrões obscuros e reduzem a usabilidade[114].

A transparência ainda pode ser aprimorada com a introdução de um painel de configurações de proteção de dados e privacidade facilmente acessível, que daria aos usuários finais a possibilidade de exercer facilmente seus direitos[115].

> Uma configuração padrão forte de proteção de dados deve ser estabelecida, juntamente com configurações de proteção de dados que permitiriam ao usuário final controlar efetivamente, sem qualquer ônus, suas preferências.
> [...]
> O processamento de dados pessoais deve ser transparente, o que significa que o sistema e seus componentes devem ser projetados de maneira que aspectos relevantes do processamento de dados pessoais sejam conhecidos pelos titulares dos dados, permitindo-lhes tomar decisões informadas e exercer seus direitos. Além disso, a ferramenta deve garantir que outros direitos, como privacidade, liberdade de expressão e ausência de discriminação, também sejam salvaguardados[116].

Ainda existe a questão de a linguagem dessas políticas devem ser acessíveis, pois geralmente escrita de uma maneira que é difícil para a pessoa comum entender, e é ideal que o aceite da política seja granular, pois a prática comum é que tenha uma decisão única que retira o poder do usuário de modificar/personalizar o que será coletado[117].

Tudo isso deve ser estabelecido de forma em que deixe claro para o usuário a legalidade do tratamento, o propósito claro de tal, e garanta segurança, confiabilidade e transparência. E, o mais importante, seguir o que é dito na política, ou seja, como no exemplo trazido da política da Smart Tv da Samsung, é

---

[114] GKOTSOPOULOU, Olga et al. Data protection by design for cybersecurity systems in a smart home environment. **IEEE conference on network softwarization**. Paris, p. 101-109, 2019. Disponível em: https://ieeexplore.ieee.org/abstract/document/8806694
[115] Ibid
[116] Ibid.
[117] ALVES, Davis; PEIXOTO, Mário; ROSA, Thiago. op cit

dito que os dados de voz serão compartilhados com terceiros para converter a voz em texto: "Para fornecer a função de reconhecimento de voz, alguns comandos de voz poderão ser transmitidos para um serviço de terceiros, que converte fala para texto ou para a extensão necessária para a função". Logo, se esses dados são compartilhados para outra empresa e para outra finalidade que não essa, o tratamento desvia do propósito informado, e não seguindo os princípios abordados neste tópico.

Todavia, é uma prática frequente das empresas, principalmente das maiores utilizarem os dados que coletam para outras finalidades:

> Em abril de 2019, a Amazon admitiu que as gravações de voz dos seus consumidores são ouvidas regularmente com o objetivo de melhorar o seu serviço. A gigante de tecnologia Google também afirmou em julho de 2019, que os contratantes escutam regularmente as gravações de voz obtidas pelo Google Home.[118]

Ou seja, as empresas estariam utilizando os dados sigilosos dos seus consumidores para outro propósito que não foi informado e que não tem permissão, com fim de interesse e benefício próprio.

[118] CANDIDO, Enzo Raian Teixeira; MOURA, José Antão Beltrão. op cit.

5 CONCLUSÕES FINAIS

Ao longo da presente monografia foi possível se situar em um desafio da atual sociedade conectada, em que a medida que a tecnologia vai se desenvolvendo, novas problemáticas vão surgindo. Uma delas está relacionada à Internet das Coisas, que possui aplicação em diversos setores, incluindo as residências, que se tornam casas inteligentes.

Com o crescente aumento de casas inteligentes, surgem mais problemas que podem afetar diversas esferas de seus usuários, a ressaltar a proteção de dados pessoais. Foi apresentado que um guia para realização de um tratamento de dados são os princípios de proteção de dados, mas apesar de promoverem uma base de um tratamento de dados seguro o que acontece na prática é que muitas vezes eles não são seguidos seja por uma não preocupação com a privacidade desde o início do desenvolvimento do produto, seja pelo desafio de limitação da própria tecnologia. O que se observa na prática é o desenvolvimento de ferramentas da forma mais conveniente para as empresas, sem pensar nos direitos dos usuários.

Foram analisados principalmente quatro princípios: minimização, segurança, transparência e limitação de propósito, observando alguns riscos aos usuários de esses princípios não estarem sendo aplicados, como vazamento de dados, falta de informação e controle do titular sobre o uso dos seus dados, juntamente com exemplos ilustrativos.

Foi ressaltada também a questão da inerência da tecnologia não permitir essa aplicação, pois há uma tendência de coleta massiva de dados em um ambiente smart house, sendo coletados dados para além de dados diretamente fornecidos pelo titular, pois através do machine learning é possível gerar outras inferências, o que torna mais difícil acontecer uma minimização na coleta em um ambiente de uma casa inteligente.

Os princípios de proteção de dados, apesar de promoverem uma base de um tratamento de dados seguro, muitas vezes não são seguidos por parte dos fabricantes, e o que se observa na prática é o desenvolvimento de ferramentas da forma mais conveniente para as empresas, sem pensar nos direitos dos usuários.

Todavia, apesar dessas limitações, deve existir um equilíbrio entre inovação e defesa dos direitos, não sendo um limitado pelo outro. Por isso, a solução que se mostra mais concreta para criar um ambiente seguro e com respeito ao usuário é aplicar o *privacy-by-design*, ou seja, pensar em privacidade desde a concepção de uma ferramenta, para que o produto seja construído já se preocupando com tal questão, e não haja a necessidade de ser reativo se alguma violação a dados acontecer, pois já terá sido preventivo desde antes.

Além disso, como mencionado ao longo da tese, seria interessante existir alguma espécie de fiscalização dos produtos antes de entrarem no mercado, a fim de conferir se aquela solução segue os princípios de proteção de dados.

Sem contar que deve haver uma gestão de privacidade na prática das empresas e desenvolvedores de produtos, de tudo aquilo que envolva de maneira direta ou indireta a privacidade e proteção dos dados do usuário, e que esteja sempre atenta e atualizada

O fato é que a realidade atual é de as pessoas terem a sua volta uma maior integração, interação e inteligência de recursos e serviços, utilizando-os no ambiente doméstico, de estudo e de trabalho, e para tudo isso ser realizado é necessária uma coleta de dados. Mas um descuido em relação ao tratamento de dados pessoais rende reais consequências, sobretudo pela sensibilidade de os dados poderem estar e ficar expostos sem o conhecimento ou aprovação do usuário. É preciso que a pessoa se sinta segura dentro de sua residência, e o fato de estar usando tecnologias que vendem um maior conforto e modernidade não devem ser uma barreira para tal.

REFERÊNCIAS

AIRES, Regina Wundrack do Amaral; MOREIRA, Fernanda Kempner Moreira; Freire Patrícia de Sá. Indústria 4.0: competências requeridas aos profissionais da quarta revolução industrial. **VII Congresso Internacional de Conhecimento e Inovação**, Foz do Iguaçu/PR, set. 2017. Disponível em: https://proceeding.ciki.ufsc.br/index.php/ciki/article/view/314/153.

ALBANY, Mada et al. A review: Secure Internet of thing System for Smart Houses. **Procedia computer science,** v. 201, p. 437-444, 2022. Disponível em: https://www.sciencedirect.com/science/article/pii/S1877050922004707

AL-FUQAHA, A et al. Internet of Things: A Survey on Enabling Technologies, Protocols and Applications. **IEEE Communications Surveys & Tutorials**, v. 17, ed. 4, p. 2347-2376, 15 jun. 2015. DOI 10.1109/COMST.2015.2444095. Disponível em: https://ieeexplore.ieee.org/document/7123563.

ALVES, Davi; PEIXOTO, Mário; ROSA, Thiago. **Internet das coisas (iot)**: segurança e privacidade de dados pessoais. Rio de Janeiro: Alta books, 2021.

ALVES, Paulo. Estudo aponta falhas na Alexa que podem revelar informações importantes. **Techtudo**. Disponível em: https://www.techtudo.com.br/noticias/2021/03/estudo-aponta-falhas-na-alexa-que-podem-revelar-informacoes-importantes.ghtml. Acesso em 30 jan. 2024

ASHTON, Kevin. That “Internet of Things” thing. **RFiD journal**, v. 22, p. 97-114, 2009.

ÁUDIOS da Alexa vazam para 30 mil funcionários da Amazon de forma indevida. **Invest news**, 3 jun. 2023. Disponível em: https://investnews.com.br/geral/audios-da-alexa-vazam-para-30-mil-funcionarios-da-amazon-de-forma-indevida/. Acesso em 30 jan. 2024

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: funções e limites do consentimento. Rio de Janeiro: Forense, 2 ed. 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

BRUNO, Fernanda et al. **Tecnopolíticas da vigilância**. São Paulo: Boitempo, 2018.

CANDIDO, Enzo Raian Teixeira; MOURA, José Antão Beltrão. **Segurança e privacidade em assistentes pessoais**. Tese (bacharelado em ciência da computação) - centro de engenharia e informática, Universidade Federal de Campina Grande. Campina Grande, 2023. Disponivel em: http://dspace.sti.ufcg.edu.br:8080/xmlui/bitstream/handle/riufcg/29302/ENZO%20

RAIAN%20TEIXEIRA%20CANDIDO%20-%20TCC%20ARTIGO%20CI%c3%8aNCIA%20DA%20COMPUTA%c3%87%c3%83O%20CEEI%202023.pdf?sequence=1&isAllowed=y

CARMEN, Gabriela Del. Smart Home: 10 tecnologias essenciais para deixar a sua casa mais inteligente. **Forbes Tech**, ago. 2021. Disponível em: https://forbes.com.br/forbes-tech/2021/08/smart-home-10-tecnologias-essenciais-para-deixar-a-sua-casa-mais-inteligente/#foto9. Acesso em 19 jan. 2024

CAVOUKIAN, Ann. Privacy by design: the 7 foundational principles. **Information and Privacy Commissioner of Ontario**. Toronto, 2009. Disponível em: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf

Convenção 108 do Conselho da Europa. **Convenção para a Proteção das Pessoas em Relação ao Tratamento Automatizado de Dados de Caráter Pessoal**. Número da Convenção: 108. Data de Assinatura: 28 de janeiro de 1981. Local de Assinatura: Estrasburgo. Ratificação pelo Brasil: 10 de setembro de 2003. Promulgação pelo Brasil: Decreto nº 4.509, de 10 de dezembro de 2002. Publicação: Diário Oficial da União, Seção 1, de 11 de dezembro de 2002.

CRUZ, Sylvio Augusto de Mattos.Big data e o fim do livre arbítrio: a democracia manipulada. **Pensar acadêmico**, Manhuaçu, v.19, n.3, p.1083-1102, set.-dez., 2021. Disponível em: https://www.pensaracademico.unifacig.edu.br/index.php/pensaracademico/article/view/2536/2091.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. São Paulo: Thomson Reuters, 2 ed. 2019.

DOS SANTOS, Ranieri Alves; SCANDOLARA, Daniel Henrique; MOHR, Eduarda Talita Bramorski. Desafios da lgpd na governança de dados pessoais em cenários de big data. in: DALMARCO Eduardo Monguilhott; FANTONELLI Miliane; WAZLAWICK Raul (coord.) **Mostra Científica da Proteção de Dados na Saúde, Tecnologia e Poder Público**.Florianópolis: UFSC, 2023. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/251199/ebook2023_final.pdf?sequence=1#page=9

EXISTE diferença entre casa conectada e casa inteligente?. **Desktop blog**, 25 abr. 2023. Disponível em: https://www.desktop.com.br/blog/casa-conectada-e-casa-inteligente/. Acesso em: 20 nov. 2023

GERBER, Ben. **OECD Privacy Principle**s. OECD, 2020. Disponível em: http://oecdprivacy.org/

GHIGLIERI, Marco; VOLKAMER, Melanie; RENAUD, Karen. Exploring consumers' attitudes of smart TV related privacy risks. *In*: TRYFONAS, Theo. (Ed.) **Human Aspects of Information Security, Privacy and Trust**. Vancouver: Springer, 2017, p. 656-674.

GKOTSOPOULOU, Olga et al. Data protection by design for cybersecurity systems in a smart home environment. **IEEE conference on network softwarization**. Paris, p. 101-109, 2019. Disponível em: https://ieeexplore.ieee.org/abstract/document/8806694

HAIGH, Karen Zita; YANCO, Holly A. Automation as caregiver: a survey of issues and Technologies. **AAAI Technical Report** WS-02-02. Disponível em: https://www.aaai.org/Papers/Workshops/2002/WS-02-02/WS02-02-007.pdf.

HÄRDLING, Emma. **Data protection in the smart home**: do data subjects have control over the AI-generated inferences drawn about them from the smart devices in their homes?. Tese (mestrado em direito da União Europeia) - Departamento de direito, Universidade de Uppsala. Uppsala, 2022. Disponível em: https://www.diva-portal.org/smash/get/diva2:1716359/FULLTEXT01.pdf

HEEJUNG, Yu; HOWON, Lee; HONGBEOM, Jeon. What is 5G? Emerging 5G Mobile Services and Network Requirements. **Sustainability**, [S.l.], v. 9, n. 10, p. 1848, 2017. DOI: 10.3390/su9101848. Disponível em: https://www.mdpi.com/2071-1050/9/10/1848.

ICO (Information Commissioner 's Office). **A guide to data protection principles**. Londres: ICO, [s.d.]. Disponível em: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

ICO (Information Commissioner 's Office). **Personal data breaches: a guide**. Londres: ICO, [s.d.]. Disponível em: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/

CISA (Cybersecurity and Infrastructure Security Agency). **Shifting the balance of cybersecurity risk**: principles and approaches for secure by design software. [s.l.] abr. 2023. Disponível em: https://www.cisa.gov/resources-tools/resources/secure-by-design

LI, Shancang; XU, Li Da; ZHAO, Shanshan Zhao. 5G Internet of Things: A survey. **Journal of Industrial Information Integration**, v. 10, p. 1-9, jun. 2018. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S2452414X18300037

LORENZO, Alessandro Di. Amazon pagará multa milionária após Alexa violar privacidade de crianças. Olhar Digital. 21 jul. 2023. Disponível em: https://olhardigital.com.br/2023/07/21/pro/amazon-pagara-multa-milionaria-apos-alexa-violar-privacidade-de-criancas/. Acesso em: 08 set. 2023

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV editora, 2018.

MARTINEZ-VILLALBA, Juan Carlos Riofrío. La Cuarta Ola De Derechos Humanos: Los Derechos Digitales. **Revista Latinoamericana de Derechos**

Humanos, [S.l.], v. 25, n. 1, p. 107-126, 2014. ISSN 1659-4304. Disponível em: https://ssrn.com/abstract=2515038.

MORAES, Alexandre de; HAYASHI Victor Takashi. **Segurança em IoT**: entendendo os riscos e ameaças em internet das coisas. Rio de Janeiro: Alta books, 2021.

MORGAN, Jacob. A Simple Explanation Of 'The Internet Of Things'. **Forbes**, 13 mai. 2014. Disponível em: https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/?sh=4db41a221d09. Acesso em: 20 nov. 2023.

NASCIMENTO, Rodrigo. O que, de fato, é internet das coisas e que revolução ela pode trazer? **IT forum**, 12 mar. 2015. Disponível em: https://itforum.com.br/noticias/o-que-de-fato-e-internet-das-coisas-e-que-revolucao-ela-pode-trazer/. Acesso em 12 dez. 2023

OLIVEIRA, Manuel Maria Marques Pinto da Costa. **Privacidade no ciclo de vida do desenvolvimento seguro**. Tese (mestrado em engenharia informática) - Faculdade de ciências, Universidade de Lisboa. Lisboa, 2019. Disponível em: https://repositorio.ul.pt/handle/10451/40204

OLIVEIRA, Nairobi Spiecker de et al. Segurança da informação para internet das coisas (IoT): uma abordagem sobre a lei geral de proteção de dados (LGPD). **Revista Eletrônica de Iniciação Científica em Computação**, v. 17, n. 4, 2019. Disponível em: https://seer.ufrgs.br/reic/article/view/88790.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). Manual de Oslo: Diretrizes para a coleta e interpretação de dados sobre inovação. 3 edição. Paris: OCDE, 2005.

PANDEY, Sakshi et al. IOT based Home automation and analysis using machine learning. **SSRN**, mar 2019. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3353476

PATEL, Keyur K.; PATEL, Sunil M.; SCHOLAR, P. Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. I**nternational journal of engineering science and computing**, v. 6, n. 5, 2016. Disponível em: http://www.opjstamnar.com/download/Worksheet/Day-110/IP-XI.pdf

PINISETTY, Srinivas et al. Monitoring data minimisation. **arXiv**, v. 1, jan. 2018. Disponível em: https://arxiv.org/abs/1801.02484

PRIVACY INTERNATIONAL. **A guide for policy engagement on data protection**. Londres, set. 2018. Disponível em: https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf

RAAB, Charles D. Regulating surveillance: The importance of principles. In: BALL, Kirstie; HAGGERTY, Kevin D.; LYON, David. **Routledge handbook of surveillance studies**. Nova Iorque: Routledge, 2012.

Report Linker. **Global Smart Home Services Market Size, Share & Industry Trends Analysis Report By Type**. KBV Research, fev. 2024. Disponível em: https://www.reportlinker.com/p06364748/Global-Smart-Home-Services-Market-Size-Share-Industry-Trends-Analysis-Report-By-Type-By-Regional-Outlook-and-Forecast.html?utm_source=GNW

SCARAMUZZA, Lara Vitória Silva; GODOY, Henri Alves de. Segurança da informação aplicada em big data. **FatecSeg-Congresso de segurança da informação**. 2022. Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/70

SHAFIQUE Kinza et al. Internet of things (IoT) for next-generation smart systems: a review of current challenges, future trends and prospects for emerging 5G-IoT scenarios. **IEEE Access**, vol. 8, p. 23022-23040, 2020. Disponível em: https://ieeexplore.ieee.org/abstract/document/8972389

SINHA, Satyajit. **State of IoT 2023**. Iot analytics, 24 mai. 2023. Disponível em: https://iot-analytics.com/number-connected-iot-devices/. Acesso em 30 nov. 2023

SUKINO, Letícia Sayuri Uemura; IMAMURA, Mayara Saory. Direito à privacidade e intimidade frente aos direitos fundamentais de quarta dimensão. **ETIC - Encontro de iniciação científica**, v. 13, n. 13, 2017. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/6159.

UNIÃO EUROPEIA. Regulação 2016/679, de 27 de abril de 2016. Regulamento Geral de Proteção de Dados. Jornal Oficial da União Europeia, 04 mai. 2016.

United Nations Conference on Trade and Development. **Data Protection and Privacy Legislation Worldwide**, dez. 2021. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

WEISER, Mark. The Computer for the 21st Century. **Scientific American**, v. 265, n. 3, p. 94-104, 1991. Disponível em: https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf