Capacitando os utilizadores para os seus direitos de privacidade na *Internet of Things*

Nelson Vieira
Faculdade de Ciências Exatas e da Engenharia
Universidade da Madeira
Funchal, Portugal
2080511@student.uma.pt

Mary Barreto (Orientadora)
Faculdade de Ciências Exatas e da Engenharia
Universidade da Madeira
Funchal, Portugal
mary.barreto@staff.uma.pt

***Abstract*—Os dispositivos da *Internet of Things* (IoT) estão em toda parte, desde o nascimento da computação ubíqua que a vida quotidiana humana é imaginada contendo milhões de dispositivos que controlam todos os aspetos de nossas vidas. Hoje em dia temos carros inteligentes, casas inteligentes, cidades inteligentes, *wearables* entre outras coisas que usam vários tipos de dispositivos e vários tipos de redes para comunicarem. Estes dispositivos criam novas formas de recolher e processar dados pessoais de utilizadores e não utilizadores. A maioria dos utilizadores finais nem sabem ou têm pouco controlo sobre as informações que estão a ser recolhidas por estes sistemas. Este trabalho faz uma abordagem holística deste problema, fazendo primeiro uma revisão da literatura, depois realizando um questionário para saber mais sobre o conhecimento geral do público e, finalmente, com base nas informações recolhidas, é proposto um sistema que fornece aos utilizadores informações sobre o dispositivos que estão próximos e como proteger os dados que não desejam compartilhar com estes dispositivos, este sistema é capaz de detetar que tipo de dispositivos estão próximos, que tipo de dados são recolhidos por estes dispositivos, mostrar opções de privacidade ao utilizador quando é possível fazê-lo e o que pode ser feito para evitar que dados indesejados sejam recolhidos.**

***Index Terms*—privacidade, Internet of Things, computação ubíqua, assistente de privacidade**

I. Introdução

A privacidade como a conhecemos é um conceito relativamente recente [1], [2], antes da era digital quase não havia a noção de privacidade para a maioria das pessoas. Durante muitos séculos, a maioria das pessoas residia em pequenas comunidades onde estavam continuamente envolvidas na vida umas das outras. Ainda mais recente é a ideia de que a privacidade é um componente crucial da segurança pessoal, em contraste com a inegável necessidade da segurança pública, incluindo a exigência de muros vigiados e portas fechadas. Há muito vista como um luxo, a privacidade ainda costuma ser vista como um bem de se ter e não como um requisito essencial, embora seja reconhecida como um direito humano, conforme consta no artigo 12 da Declaração Universal dos Direitos Humanos [3]: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei". A privacidade pode ser definida [4], [5] como o direito de governar como as informações e dados pessoais são recolhidos, armazenados e usados, frequentemente envolve o uso de informações confidenciais com cuidado e, como tal, as organizações devem ser abertas e honestas sobre o tipo de dados que planeiam recolher, por que precisam deles e onde e com quem planeiam partilhá-los. Os utilizadores devem ter o direito de controlar como as suas informações são partilhadas.

Esta definição pode causar alguma confusão com a ideia de segurança [6] e embora a privacidade e a segurança estejam interligadas, a segurança envolve medidas tomadas para salvaguardar os dados de risco, ameaça ou perigo, frequentemente alude à proteção. É a prática de manter a informação pessoal dos utilizadores e dados seguros e prevenindo o acesso não autorizado aos mesmos. O principal contraste entre privacidade e segurança é que o primeiro trata de informações pessoais dos indivíduos e como estes querem que os seus dados sejam utilizados e mantidos, enquanto este último trata da sua proteção contra possíveis ameaças. A segurança pode existem sem privacidade, mas o oposto não é verdade. Para a gestão de dados sensíveis e pessoais, privacidade e segurança informática são igualmente cruciais. Os utilizadores devem estar cientes dos procedimentos internos relativos à recolha, processamento, retenção, e partilha de informação pessoal.

As preocupações com a privacidade digital têm vindo a crescer [7]–[9] nos últimos anos, especialmente depois dos ataques informáticos do grupo descentralizado de hackers *Anonymous*, *WikiLeaks* e da divulgação de documentos ultra secretos da Agência de Segurança Nacional dos Estados Unidos por Snowden. Estas preocupações podem ser notadas com o aumento da literatura escrita sobre o assunto, ao procurar termos como "privacy", "online privacy", "digital privacy" no Google Scholar, ACM Digital Library ou Science Direct, pode ser visto que, nos últimos 5 anos, retornam cerca de 5 000 000, 650 000 e 8 0000 documentos, respetivamente, incluindo artigos, livros, artigos de conferência, etc.

A maioria da investigação tem-se concentrado na *web*, enquanto a privacidade nos sistemas IoT não tem sido tão explorada. Uma vez que os dispositivos IoT estão a tornar-se mais predominantes, surgem novos métodos de comunicação, recolha, e análise de dados. Porque já existe uma quantidade substancial de investigação centrada em privacidade na *web* em vez de privacidade na IoT, é um terreno muito mais fértil para explorar a questão da privacidade no contexto da IoT.

Internet of Things é um termo que surgiu pela primeira vez nos anos 90, e pode estar ligado ao artigo de Mark Weiser sobre a computação ubíqua [10] e o crescimento de dispositivos de todos os tamanhos que comunicam entre si para realizar várias tarefas, tornando o sonho de Weiser uma realidade. A primeira utilização do termo *Internet of Things* foi em 1999 pelo pioneiro da tecnologia britânica Kevin Ashton [11], director executivo do Centro de Auto-ID no Instituto de Tecnologia de Massachusetts, para descrever um sistema em que os itens podem ser ligados à internet por sensores. Ele inventou a frase enquanto fazia uma apresentação para a Procter & Gamble para realçar o valor de ligar etiquetas de Identificação por Radiofrequência (RFID) utilizadas em cadeias de fornecimento corporativas ligadas à internet, a fim de contar e rastrear bens sem a necessidade de assistência humana. Estes dispositivos são utilizados em várias aplicações, começando em casa [12] com termostatos, frigoríficos, micro-ondas, etc., passando para carros inteligentes [13], o sistema educacional [14], as nossas roupas e os nossos relógios [15] e mesmo para o espaço exterior [16]. Os recursos da IoT podem incluir equipamento IoT (como assistentes domésticos inteligentes e veículos autónomos), serviços IoT (como serviços de análise de vídeo ligados a câmaras inteligentes e sistemas de localização de posição interior), ou aplicações IoT (como aplicações remotas de televisão inteligente) que localizam e utilizam informação sobre nós. A *Internet of Things* é agora amplamente utilizada para descrever situações em que uma gama de objetos, dispositivos, sensores, e itens comuns estão ligados à internet e têm capacidades computacionais.

A ideia de utilizar computadores e redes para monitorizar e gerir dispositivos não é nova, apesar do termo *Internet of Things* ser relativamente recente. As melhorias da tecnologia sem fios nos anos 90 permitiram a adoção generalizada de soluções máquina-a-máquina (M2M) corporativas e industriais para monitorização e operação de equipamentos. Muitas das primeiras soluções M2M, por outro lado, baseavam-se em redes proprietárias ou em normas específicas da indústria, em vez de normas da internet. Ligar outros dispositivos que não um computador à internet não é um conceito novo. Uma máquina de Coca-Cola no Departamento de Informática da Universidade de Carnegie Mellon [17] foi o primeiro dispositivo ubíquo a ser ligado à internet. O sistema, criado em 1982, observou remotamente as luzes de esgotamento de stock nos botões de pressão da máquina de venda automática e difundiu o estado de cada fila da máquina de venda automática na rede para que pudesse ser acedido utilizando o protocolo Name/Finger através de um terminal. Em 1990, uma torradeira que podia ser ligada e desligada através da internet, criada por John Romkey [18], foi demonstrada no evento Interop Internet Networking.

A *Internet of Things* pode ser definida como: "Uma rede aberta e abrangente de objetos inteligentes que têm a capacidade de se auto-organizarem, partilhar informação, dados e recursos, reagindo e agindo face a situações e mudanças no ambiente" [19].

IoT é uma das tecnologias de crescimento mais rápido [20], prevê-se que cresça para os triliões de dispositivos até 2030 [21], e com esta expansão surgem novas vulnerabilidades de segurança e perigos de recolha de dados, a falta de segurança nestes dispositivos torna-os alvos ideais para violações da privacidade e divulgação inadequada aos clientes das capacidades dos dispositivos e práticas de dados agrava as questões de privacidade e segurança.

A privacidade nos sistemas IoT não é vista como um factor crucial no desenvolvimento de aplicações ou sistemas [22]. Normas específicas para opções de privacidade foram impostas por normas de privacidade dos dados incluindo o Regulamento Geral de Proteção de Dados (RGPD) e a Lei de Privacidade do Consumidor da Califórnia, mas mesmo estes regulamentos têm sido criticados [23]–[27].

II. Estado da Arte

Esta secção fornece uma visão geral da literatura recente com os temas que foram consideradas mais relevantes para este trabalho.

A. Paradoxo da Privacidade

A utilização de uma variedade de dispositivos digitais tem inúmeras vantagens, mas eles trazem também consigo a ubiquidade do equipamento de captura de dados, é compreensível que a maioria dos utilizadores em rede tenha sérias preocupações sobre a privacidade dos seus dados pessoais. No entanto, as opiniões expressas estão em total desacordo com a realidade, segundo o relatório sobre o estado da privacidade de Thomson et al. [28], de apenas um em cada quatro utilizadores europeus lê os termos e condições na sua totalidade antes de efetuar uma compra *on-line* ou subscrever a um serviço, 59% admitiram apenas a digitalização rápida do termos e condições antes de concluir uma compra, enquanto 14% admitiu que nunca os leu de todo, 30% dos inquiridos até trocariam os seus endereço de *e-mail* para ganhar uma recompensa, ou entrada numa rifa, enquanto 17% faria por isso, para obter uma aplicação e 30% fá-lo-ia por dinheiro.

Isto é o que se chama um paradoxo de privacidade, tem havido múltiplos artigos escritos sobre este assunto [29]–[33], alguns artigos tentam uma explicação teórica enquanto outros tentam uma explicação empírica. Tem havido interpretações ou explicações muito diferentes deste paradoxo, alguns artigos [34]–[36] aplicam o conceito teórico do *homo economicus* [37], que é a representação de pessoas como seres que atuam constantemente de uma forma lógica e interessada em si próprios, sem se preocuparem com a moralidade ou a ética, e que o fazem o melhor que podem, no contexto da privacidade. Diferentes preconceitos cognitivos e heurísticos podem influenciar a forma como os consumidores tomam decisões, de acordo com vários estudos sobre o comportamento de escolha do consumidor [38]–[41]. De acordo com vários artigos [42], [43], este paradoxo pode ser explicado pelo facto de algumas pessoas terem genuinamente violações de privacidade online e que a maioria das opiniões sobre privacidade são, portanto com base na heurística ou em contas de segunda mão. O estudo de Taddicken [44] argumenta que a pressão de grupo é a razão

pela qual as pessoas têm este comportamento contraditório, Norberg et al. [45] explica este paradoxo ao sugerir que embora a perceção do risco afete as atitudes e intenções comportamentais relatadas, a confiança tem um impacto direto no comportamento de privacidade, enquanto outros [41], [46] confiam na teoria quântica. Brandimarte et al. [47] exploraram a ideia de que quando se trata da sua privacidade de dados, os utilizadores têm uma *ilusão de controlo*.

Este paradoxo foi comprovado por uma série de estudos empíricos [42], [48]–[50], as práticas de privacidade online são baseadas em mentalidades de privacidade separadas e assim não são intrinsecamente paradoxais.

B. Privacidade em IoT: Abordagens

Houve uma série de revisões sistemáticas da literatura (SLR) [51]–[54] e *systematic mapping reviews* [55], [56] feitas para estudar as questões de privacidade e segurança na IoT.

No SLR de Gupta e Ghanavati [51], os autores revêm os artigos com metodologias e técnicas que identificam riscos de privacidade ou que notificam os utilizadores sobre estes riscos. Eles dividem a literatura nas seguintes categorias: 'Modelação Ontológica e Abordagens Semânticas', 'Abordagens de Dados', 'Abordagens Baseadas na Análise do Código Fonte', 'Estudos do Utilizador e Abordagens Baseadas em Inquéritos', 'Abordagens Baseadas em *Blockchain*' e 'Abordagens Baseadas em Estruturas e Arquiteturas'. Em seguida, examinam a literatura actual sobre estes três pré-requisitos. Os resultados mostram que: a maioria das obras concentra-se em dispositivos IoT únicos quando se trata de ameaças à privacidade; ao analisar as questões de privacidade, fatores-chave de privacidade tais como redução e agregação de dados são ignorados; os estudos existentes ignoraram a sensibilidade das informações obtidas; os estudos mais úteis não incluíram um leque diversificado de utilizadores ao avaliar os problemas de privacidade; não foi feito nenhum trabalho para descobrir as dificuldades de conformidade entre uma aplicação IoT e diferentes regras de privacidade; e de acordo com os dados atuais, fornecer aos clientes notificações de privacidade em tempo real não é uma prioridade elevada. No entanto, este SLR tem as seguintes limitações: os autores apenas escolheram artigos e não teses ou livros e a partir dos trabalhos selecionados, só foram considerados os escritos em inglês.

Kühtreiber et al. [52] avaliam as *frameworks* e ferramentas estabelecidas para programadores, especificamente no caso da IoT, e acham que as soluções atuais são difíceis de utilizar, apenas com sucesso em cenários limitados e insuficiente para lidar com os problemas de privacidade inerentes ao desenvolvimento de IoT. Este estudo carece de uma revisão exaustiva das lacunas escolhidas literatura, juntamente com questões de investigação que estabeleçam o significado dos artigos escolhidos.

Sicari et al. [53] examinam a investigação em curso e atividades em curso que se concentram em soluções de privacidade e segurança da IoT. Os autores começar por descrever os requisitos de privacidade e segurança da IoT, tais como controlo de acesso, confidencialidade, e autenticação. Os autores então realizaram um estudo de literatura relacionado com estas três necessidades. Os autores chegaram à conclusão de que as questões de privacidade da IoT foram apenas parcialmente examinadas e que é necessária mais atenção. O estudo, no entanto, tem falhas: a análise prévia da investigação centra-se principalmente nas necessidades de segurança, enquanto ignorando considerações de privacidade; os autores não realizam uma análise exaustiva das lacunas nas publicações examinadas; e não fornecem um resumo abrangente de futuros tópicos de investigação no domínio da privacidade na IoT que requerem mais atenção.

Lin et al. [54] realizam uma revisão da literatura para identificar vulnerabilidades de segurança e privacidade nas três camadas da arquitetura da IoT: rede, perceção, e aplicação. Os autores descrevem as seis primeiras propriedades fundamentais de segurança para estes níveis como confidencialidade, integridade, disponibilidade, identificação e autenticação, privacidade, e confiança. Em seguida, os autores analisam uma variedade de ameaças à segurança para cada uma das três fases. Os autores concluem dando um resumo sucinto de muitas técnicas de preservação da privacidade dos dados, incluindo as fases de recolha de dados, agregação e análise dos dados. Os autores concentram-se, contudo, em grande medida nas componentes de segurança da IoT e, como já foi dito, consideram a privacidade como um dos aspetos de segurança mais cruciais, em vez de encararem a privacidade como uma preocupação distinta. Além disso, a investigação não realiza uma análise exaustiva de lacunas para descobrir os pontos fracos dos esforços anteriores.

Com base na análise da literatura de Ziegeldorf [57], seguem-se as preocupações mais proeminentes em matéria de privacidade na IoT:

1) A preocupação mais proeminente é a *identificação*, que liga um identificador, tal como um nome e localização, com a identidade de um indivíduo, isto também permite e agrava outras ameaças;
2) *Localização e rastreio* é a ameaça de detetar a localização de um indivíduo através de numerosas técnicas, tais como GPS, tráfego na internet, ou localização do smartphone. Esta ameaça requer *identificação* de algum tipo;
3) No comércio eletrónico, o *profiling* é frequentemente utilizado para personalização. As organizações recolhem informação sobre indivíduos a fim de deduzir os seus interesses através da associação com outros perfis e fontes de dados.
4) *Interação e apresentação* faz alusão à partilha de informação privada com um público não intencional enquanto o faz através de um meio público. As aplicações IoT necessitam frequentemente de uma interação extensa com o utilizador, espera-se que os utilizadores destes sistemas obtenham informações através de dispositivos inteligentes no seu ambiente imediato e que os utilizadores interagem com sistemas de formas criativas e naturais. No entanto, muitos desses modos de comunicação e apresentação já estão disponíveis para o público em

geral, tornando-os aparentes a qualquer pessoa por perto. Quando a informação pessoal é transferida entre um sistema e o seu utilizador, a privacidade é violada.

5) *Transições do ciclo de vida* ocorrem quando um dispositivo IoT é vendido, utilizado pelo seu proprietário e eventualmente eliminado. Pode haver uma expectativa que o objeto apaga todas as informações, mas dispositivos inteligentes frequentemente mantêm grandes volumes de dados sobre o seu próprio passado ao longo de toda a sua existência. Isto pode conter imagens e vídeos pessoais, que nem sempre são apagados após a transferência de propriedade.
6) *Ataques ao inventário* envolvem a entrada não autorizada e a aquisição de informação sobre a presença e as características das coisas pessoais. Os utilizadores maliciosos podem utilizar dados de inventário para traçar o perfil da propriedade e assaltar.
7) A *interligação* é o processo de ligar sistemas díspares, quando os sistemas estão a ligar diferentes fontes de dados, existe um maior perigo de acesso não autorizado e de fuga de dados.

Outro conceito que vale a pena analisar é a privacidade diferencial que se relaciona mais com o inquérito que será conduzido, mas também com a recolha geral e análise de dados dos utilizadores por aplicações e sistemas.

C. Privacidade Diferencial

A noção de privacidade diferencial, de acordo com Michael Kearns [58], baseia-se em três princípios importantes. O primeiro é que "a privacidade diferencial exige que a adição ou remoção do registo de dados de um único indivíduo não alterar a probabilidade de qualquer resultado por muito". O segundo princípio sendo que "nenhum observador exterior pode aprender muito sobre qualquer indivíduo por causa dos dados específicos dessa pessoa". O terceiro princípio importante sendo que "para cada indivíduo no conjunto de dados, e para qualquer observador não independentemente das suas crenças iniciais sobre o mundo, depois de observarem o resultado de um cálculo diferencialmente privado, a sua crença posterior sobre qualquer coisa está perto do que teria sido se tivessem observado a saída do mesmo cálculo executado sem os dados do indivíduo".

A privacidade diferencial tem o potencial de aumentar significativamente a proteção da privacidade individual, ao adicionar propositadamente ruído a um conjunto de dados, dá negabilidade plausível a qualquer indivíduo que possa ter tido os seus dados explorados enquanto ainda é capaz de calcular estatísticas com uma precisão relativamente elevada. Embora os algoritmos que lidam com noções de justiça, ética e privacidade são difíceis de implementar devido à subjetividade destes conceitos, e os algoritmos de privacidade diferencial não são diferentes, ainda podem ajudar em no que diz respeito à abordagem dos dilemas morais inerentes à tecnologia.

Existem outros algoritmos que visam preservar a privacidade da mesma forma que a privacidade diferencial, tais como o algoritmo de *box blurring* da Google [59] que é utilizado na vista de rua do Google Maps, o Visor da Microsoft [60] que é uma ferramenta de análise de vídeo como serviço e o sistema de aprendizagem profunda colaborativa de Shokri e Shmatikov [61], no entanto, em geral, estes algoritmos lutam com elevados custos computacionais, ataques internos, ou privacidade não comprovável.

Zhao et al. [62] conduzem um SLR sobre a privacidade diferencial para dados não estruturados. Os autores apresentam métodos de privacidade diferencial para conteúdos sensíveis em dados de imagem, áudio, vídeo, e texto. Comparam os vários métodos e efetuam análises de utilidade para cada método, destacando os benefícios e desvantagens de cada um, a perda de utilidade é medida em avaliações experimentais entre os dados reais e a sua variante ofuscada. Chegam à conclusão de que a privacidade diferencial, bem como as suas variações, dão proteção rigorosa à privacidade de dados não estruturados contra atacantes com conhecimentos de base imprevisíveis. Sugerem também potenciais temas de estudo futuros que ainda têm de ser investigados.

D. Soluções Propostas

Esta secção enumera sete soluções que emergiram da revisão de literatura estruturada para melhorar o fosso entre os conceitos de privacidade e segurança entre sistemas e utilizadores.

1) Criando Novas Formas de Conscienlização para o Utilizador: Tem sido feito algum trabalho para determinar o conhecimento dos utilizadores sobre as suas ações online relativamente à sua privacidade. Skirpan et al. [63] construíram uma experiência de teatro interativo, esta foi criada para tentar provar que uma experiência simulada com um problema de privacidade credível pode encorajar as pessoas a tomar medidas antes de se depararem realmente com uma catástrofe. O enredo da peça consiste numa companhia tecnológica inexperiente que revelou a sua revolucionária tecnologia de IA enquanto lidava com um denunciante da empresa e um hack inoportuno de dia zero no seu sistema. O público é capaz de interagir com os atores e influenciar a forma como a história se desenrola. O público e os atores tiveram a oportunidade de experimentar papéis, comportamentos e opiniões a que normalmente não teriam acesso na vida quotidiana. Os autores tiveram entrevistas e inquéritos feitos após as peças com membros do público, no entanto, apenas fizeram entrevistas a meio da produção e apenas a uma pequena fração do público participou efetivamente nesta recolha de dados, observaram também que, após contactarem as pessoas meses após as entrevistas, não mudaram realmente o seu comportamento relativamente aos seus direitos de privacidade.

2) Legislação: Alguns documentos procuram melhorar a legislação [64], [65] porque, caso contrário, nas suas opiniões, os direitos de privacidade não serão respeitados se não forem legalmente exigíveis, defendem que, sem o acordo expresso do indivíduo em causa, as informações privadas obtidas por dispositivos IoT não devem ser retidas ou processadas sob qualquer forma, e devem ser adotados os procedimentos necessários para garantir que os dados recolhidos não sejam

os de um indivíduo não relacionado. Mas melhores leis de proteção para o utilizador também criariam oposição da maioria das empresas que pretendem extrair o máximo de dados privados dos seus utilizadores sem quaisquer restrições, a fim de aumentar as suas margens de lucro.

3) Privacidade Através da Segurança: Sun et al. [66] concebem uma estratégia de comunicação leve para um sistema de controlo remoto, utilizando dois tipos de espaços virtuais para alcançar o objetivo de anúncio de identidade e troca de dados. Construíram um sistema protótipo do esquema e testaram-no na Freenet, demonstrando que o método pode resistir eficazmente à influência da análise de fluxo no anonimato da comunicação, preservando ao mesmo tempo a segurança dos dados de comunicação.

4) Propostas de Arquiteturas / Frameworks: Antunes et al. [67] fazem um SLR sobre aprendizagem federada na área dos cuidados de saúde e fazem uma proposta de arquitetura. A técnica conhecida como aprendizagem federada permite a formação distribuída de modelos de aprendizagem de máquinas utilizando conjuntos de dados hospedados remotamente sem a necessidade de amplificação de dados. O objetivo fundamental da arquitetura proposta é permitir que as instituições de saúde que têm acesso a informação médica sensível a utilizem na análise de dados distribuídos e na investigação da aprendizagem automática, assegurando ao mesmo tempo a confidencialidade dos pacientes. Uma vez que a informação transmitida entre instituições necessita de garantias de confidencialidade para os parâmetros do modelo de aprendizagem e resultados de análise, a arquitetura pode adotar uma série de formas baseadas num paradigma de segurança de confiança zero [68]. Além disso, as instituições desenvolvem um sistema de verificação de algoritmos de aprendizagem que pode armazenar e disseminar manifestos, bem como envolver-se em procedimentos analíticos distribuídos que necessitam do acordo unânime de todos os participantes. Este estudo demonstra também que a literatura anterior implica que a encriptação homomórfica e a privacidade diferencial são abordagens eficazes para prevenir violações de dados sem incorrer em custos de computação proibitivamente elevados.

Opara et al. [69] apresentam um sistema para detetar possíveis problemas com regulamentos de privacidade ou segurança nas fases iniciais de desenvolvimento, esta abordagem destina-se aos programadores. O documento propõe uma ontologia de domínio específico para a modelagem de políticas de segurança e privacidade da IoT, uma notação para representar e validar políticas de segurança e privacidade da IoT, um conjunto de diretrizes e regras para detetar erros de políticas da IoT, e uma ferramenta para modelar e capturar visualmente políticas de segurança da IoT e descobrir problemas de políticas. Embora a framework apresentada seja teoricamente promissora, ainda não foi testada num ambiente real, pelo que a sua eficácia ainda não pode ser medida. Os autores também não comparam a sua proposta com outras já disponíveis.

5) Blockchain: Blockchain é uma opção para garantir a privacidade em IoT devido a provas de conhecimento zero, assinaturas de anéis e *mixing* [70].

Yu et al. [71] mostra várias implementações de blockchain que proporcionam privacidade através da segurança, com base em diferentes categorias como integridade de dados, partilha de dados e autenticação e controlo de acesso. Os autores utilizam a privacidade como um proxy para a segurança, também não discutem os pontos fracos e fortes de cada implementação ou fazem qualquer comparação, também não proporcionam quaisquer outras questões de investigação.

Ali et al. [72] sugerem um stack de software que combina a partilha de ficheiros *peer-to-peer* com contratos inteligentes de blockchain para oferecer aos utilizadores de IoT o controlo sobre os seus dados e eliminar a necessidade de uma gestão centralizada de dados de IoT. Os contratos inteligentes de blockchain são utilizados na arquitetura proposta do 'consórcio modular' para regular o acesso, estabelecendo simultaneamente a responsabilidade tanto dos proprietários dos dados como de outras partes a que os utilizadores concedem acesso.

6) Outras Propostas: Zhu et al. [73] apresentam um sistema de sensor híbrido que salvaguarda a privacidade, ao mesmo tempo que monitoriza a disponibilidade de estacionamento. Os autores fundiram a deteção IoT com *crowdsensing* e melhoraram-na com métodos de preservação da privacidade. Os autores empregaram filtros físicos nebulosos para mascarar os sensores IoT na deteção de IoT, e uma técnica criptográfica baseada em compromissos criptográficos, provas de conhecimento zero, e credenciais anónimas em *crowdsensing*. Além disso, utilizaram o *crowdsourcing* para criar um modelo de aprendizagem de máquinas para reconhecimento de estacionamento na presença de filtros de nevoeiro. O seu papel incluía protótipos de prova de conceito como um sistema Raspberry Pi e uma aplicação móvel, bem como um estudo de avaliação do modelo de aprendizagem de máquinas e os efeitos do *crowdsourcing*.

7) Assistentes de Privacidade: Existe uma série de assistentes de privacidade no mercado. Os assistentes de privacidade têm o objetivo de dar ao utilizador flexibilidade na escolha das opções de privacidade preferidas nas aplicações disponíveis, a maioria é utilizada em smartphones, muito poucos são feitos para dispositivos na IoT.

O CyLab da Carnegie Mellon University, que é o instituto de investigação de segurança e privacidade da universidade, começou a desenvolver em 2019 uma infra-estrutura IoT que pretendia estar livre de fugas de privacidade e de software coberto pela sua iniciativa "Secure and Private IoT 2019", este projeto enquadrar-se-ia no seu principal tema de investigação, a Confiança. Neste projeto, iniciaram a conceção de um Assistente de Privacidade Personalizado (PPA) [74], que envolveria o uso de entrevistas semi-estruturadas com 17 participantes para examinar a perceção dos utilizadores de três hipotéticas implementações PPA, cada uma das quais potencialmente mais autónoma, ao mesmo tempo que delineavam as vantagens e desvantagens de cada implementação. As entrevistas foram divididas em três secções: exploratória, ancoragem e PPA; enquanto o objetivo da fase exploratória era aprender sobre as atitudes dos participantes e a compreensão da IoT, a

fase de ancoragem visava normalizar a compreensão básica dos participantes sobre como a IoT funciona. A fim de levar as pessoas a pensar sobre potenciais preocupações de privacidade no final da secção de ancoragem, os autores perguntaram aos participantes sobre as suas opiniões sobre privacidade de dados. Na secção PPA, foi proposta a ideia de uma PPA para a IoT como um potencial projeto futuro. Os autores esclareceram que o PPA poderia distinguir entre pedidos de dados ativos, tais como um dispositivo que pedia informações biométricas do rastreador de saúde do utilizador, e recolha de dados passivos, tais como um dispositivo inteligente com um microfone que poderia gravar as afirmações das pessoas enquanto estas estivessem por perto. A Notificação, Recomendação, e Implementação automática de uma PPA IoT foram as três que os autores e participantes discutiram. Os PPA de Notificação podem determinar que dispositivos adjacentes estão a solicitar dados e alertar os utilizadores para a presença e pedidos desses dispositivos, para que os utilizadores possam aprovar ou rejeitar cada pedido. Com base nos PPA de notificação, os PPA de recomendação oferecem aos consumidores conselhos sobre como partilhar os seus dados com base nas suas preferências. As decisões de partilha de dados dos utilizadores seriam tomadas pelos PPA automáticos. Isto diminuiria a carga cognitiva dos consumidores, mas também retiraria a sua capacidade de influenciar o processo. Verificaram que as atitudes dos participantes em relação às várias implementações eram geralmente favoráveis, embora também manifestassem preocupações, que variavam consoante o grau de automatização. Dadas as motivações divergentes dos participantes, alguns desejavam um maior controlo, enquanto outros desejavam evitar ser ultrapassados por notificações e pela falta de acordo relativamente à implementação ótima dos PPA.

Após a fase de conceção, o instituto implementou um assistente de privacidade (PA) [75], os autores chamaram-lhe IoT Assistant. Devido à abordagem predominante de "aviso e escolha" para a proteção da privacidade dos dados, decidiram que o PA também cairia nesta abordagem, mas como muitos sistemas implementam o aviso como forma de consentimento, sem por vezes oferecerem escolhas ao utilizador final, queriam também que este trabalho fornecesse um quadro conceptual que visse uma escolha de privacidade centrada no utilizador, bem como uma taxonomia para os profissionais a utilizar na conceção de escolhas de privacidade significativas para os seus sistemas. Os autores definem escolhas de privacidade significativas como "as capacidades fornecidas pelos sistemas digitais para os utilizadores controlarem diferentes práticas de dados sobre os seus dados pessoais", alargam a noção de escolhas de privacidade com cinco facetas: eficácia (a oportunidade de estabelecer preferências de privacidade que correspondam precisa e completamente à recolha de dados e métodos de utilização que um utilizador está de acordo), eficiência (a capacidade de especificar estas opções com o mínimo esforço e tempo), consciência do utilizador (em que as opções de privacidade significativas devem ser comunicadas de forma proeminente e clara aos utilizadores), abrangência (os utilizadores devem compreender as suas opções, como afetam a recolha e a potencial utilização dos seus dados, bem como que conclusões se podem tirar destes dados e as repercussões potenciais das mesmas) e neutralidade (as decisões de privacidade significativas não devem ser sujeitas a manipulação ou parcialidade). O IoT Assistant oferece quatro configurações de privacidade, dando aos utilizadores finais uma variedade de alternativas para melhor se adequarem às suas variadas preferências de privacidade e, como resultado, as opções de privacidade são mais eficazes no ambiente IoT. O IoT Assistant funciona como uma plataforma centralizada de escolha de privacidade, implementando várias opções de privacidade, permitindo aos consumidores governar mais eficazmente a sua privacidade de dados em IoT. Os três modos de descoberta do sistema IoT que o IoT Assistant suporta são códigos QR, notificações push, e interfaces de mapa baseadas em localização. Estas ferramentas de descoberta vão provavelmente tornar os utilizadores mais conscientes dos dispositivos IoT instalados e das opções de privacidade que têm. Além disso, o ponto de vista unido da notificação integrada e da opção no IoT Assistant dá informações sucintas mas completas sobre as práticas de dados IoT para ajudar os utilizadores a compreender melhor as implicações das suas escolhas de privacidade. Além disso, os autores trabalham para implementar a notificação integrada e a opção no IoT Assistant sem preconceitos ou enquadramentos, tentando oferecer aos consumidores um espaço neutro para executar as suas escolhas de privacidade. Embora os autores encarem o IoT Assistant como um passo significativo no sentido de "opções de privacidade significativas" na IoT, este assistente ainda tem muitos problemas, tais como o facto de ainda se encontrar nas suas fases iniciais de desenvolvimento e de não ter havido muito crescimento dado que foi criado em 2020 e nós estamos em 2023. Talvez a principal razão pela qual esta aplicação não foi capaz de ser desenvolvida mais é que a própria aplicação serve para mostrar ao utilizador os dados que já se encontram na infra-estrutura da IoT que foi criada anteriormente, e como tal não é capaz de identificar novos dispositivos IoT sem que os próprios utilizadores finais criem na página web principal [76] da infra-estrutura uma nova entrada para o dispositivo em questão com o qual o utilizador quer interagir. Outra razão que paralisa esta aplicação, bem como outras que procuram proporcionar melhor privacidade nos sistemas de IoT é que muitos sistemas não oferecem qualquer tipo de escolhas de privacidade ao utilizador final ou a outros utilizadores que não são os utilizadores finais pretendidos, mas sobre os quais os dispositivos ainda estão a recolher dados.

A infra-estrutura da IoT que foi desenvolvida [76] é construída sobre um design aberto e distribuído que permite a implementação e gestão de recursos da IoT a ser realizada por qualquer número de atores. Parte desta infra-estrutura é a Internet of Things Resource Registry, é uma plataforma web que permite aos proprietários de recursos declarar não só o local onde um recurso é implantado, mas também práticas de dados como o(s) motivo(s) para um determinado processo de recolha de dados, o nível de detalhe nos dados a serem

recolhidos, a retenção, os destinatários dos dados, e muito mais. Além disso, revela quaisquer definições de privacidade configuráveis pelo utilizador que possam estar ligadas a um determinado recurso.

E. Principais Levantamentos

Existem duas formas principais de proporcionar privacidade nos sistemas de IoT, através da segurança ou da utilização de avisos de privacidade, outras formas como através de legislação ou com a criação/utilização de uma estrutura que proporcione privacidade enquadram-se nestas duas categorias. A maior parte da literatura assume que segurança e privacidade são sinónimos, por exemplo [65], [66], [69], pelo que a maior parte das soluções propostas são abrangidas pela privacidade através da segurança. As soluções propostas que utilizam avisos de privacidade, como [75], são implementadas de uma forma que utiliza outros dispositivos como smartphones que fornecem os próprios avisos, é difícil fornecer avisos de privacidade nos próprios dispositivos IoT porque muitos destes dispositivos não têm ecrã ou o ecrã é demasiado pequeno para fornecer as informações necessárias ao utilizador. Como ainda não existem normas para a implementação de avisos de privacidade, e as melhores práticas estão dispersas por toda a literatura, são na sua maioria implementadas de forma aleatória, pouca orientação é dada aos designers e programadores sobre como fazer um desenho de aviso de privacidade que seja suficiente e aceitável para o seu sistema particular e as suas características. Os designers podem desconhecer as numerosas possibilidades de criar notificações de privacidade aceitáveis e, como resultado, não as exploram sistematicamente.

Aleisa e Renaud [77] também identificam a segurança e a consciencialização da privacidade como potenciais soluções para as questões de privacidade na IoT, mas também identificam a minimização dos dados, o método de boleia e a introspeção. A minimização de dados implica limitar a recolha de informações pessoais ao que é absolutamente central e reter os dados apenas pelo tempo necessário para satisfazer o objetivo dos serviços da tecnologia [78]. A boleia [79] é um método de proteção da privacidade dos utilizadores que divulgam a sua localização, as aplicações consideram a localização como o objeto da sua atenção. A troca de fidelidade é eliminada, pois não é importante saber quem se encontra num determinado local. O método de introspeção [80] examina as ações de VM para salvaguardar adequadamente a informação privada dos utilizadores. O estado do CPU de cada VM, conteúdos de memória, informação de rede fornecida pelo hipervisor, e qualquer software malicioso que possa estar presente na VM são todos recolhidos e analisados. A privacidade dos consumidores é posta em risco se um dispositivo IoT perder integridade devido a uma agressão hostil.

III. Desafios de Privacidade

IoT é uma teia complexa de arquiteturas, aplicações e tecnologias. Em termos de arquiteturas, pode ser decomposta em três camadas: a camada de perceção, a camada de rede e a camada de aplicação.

A camada de perceção, também conhecida como camada de sensores, interage com objetos e componentes físicos através de dispositivos inteligentes (RFID, sensores, atuadores, e assim por diante). Os seus principais objetivos são a ligação de objetos à rede IoT e a monitorização, recolha e análise de informação de estado sobre estas coisas utilizando dispositivos inteligentes implantados. Esta camada pode muitas vezes não ser fiável, por exemplo com veículos autónomos onde é difícil ler sinais rodoviários ou prever se certos objetos são inanimados ou não, mas esta falta de fiabilidade também traz privacidade mesmo que alguns dos dados possam ser inutilizáveis. O ruído também pode ser acrescentado a esta camada para proporcionar privacidade extra.

Na camada de rede existem muitas redes concorrentes como ZigBee, Z-Wave, Bluetooth Low Energy, LoRa, Wi-fi, etc., esta camada está fragmentada especialmente no que diz respeito a redes sem fios e isso torna muito difícil criar uma arquitetura IoT que possa utilizar várias redes e ter os vários dispositivos a comunicar entre si, apesar de a interoperabilidade ser vista como um factor muito importante na IoT. Algumas destas redes são protocolos padrão abertos enquanto outras são proprietárias e utilizam diferentes protocolos de comunicação, utilizam diferentes frequências, diferentes gamas e diferentes taxas de dados. Ao criar uma arquitetura IoT, os designers pensam frequentemente em como resolver problemas específicos e utilizar o que é melhor para as necessidades atuais, e a forma como a IoT é fragmentada não ajuda a proporcionar progresso.

A camada de aplicação recebe dados da camada de rede e utiliza-os para executar serviços ou operações essenciais. Esta camada, por exemplo, pode fornecer o serviço de armazenamento para fazer o backup dos dados recebidos numa base de dados ou o serviço de análise para analisar os dados recebidos, a fim de prever o estado futuro dos dispositivos físicos. Esta camada engloba uma vasta gama de aplicações, cada uma com o seu próprio conjunto de requisitos. Alguns exemplos são redes inteligentes, transporte inteligente, e cidades inteligentes.

De acordo com Qu et al. [81], permanecem várias barreiras significativas, incluindo a falta de uma base teórica, a otimização do trade-off entre privacidade e valor dos dados, e a sobre-complexidade de isomerismo do sistema. Uma vez que não existem fundamentos matemáticos para a conceção da estrutura da IoT, os projetos do sistema IoT são planeados e executados utilizando abordagens empíricas, que têm limitações no desenvolvimento da IoT. A teoria científica e a análise quantitativa devem permitir uma otimização trade-off, no entanto, existem múltiplas partes com características e requisitos diversos, tornando esta otimização altamente desafiante. Uma pletora de normas e protocolos aumenta a complexidade desnecessária do isomerismo do sistema. Assegurar aplicações IoT eficazes enquanto desperdiça tão poucos recursos quanto possível implica menos recursos disponíveis para a proteção da privacidade, contudo, a proteção da privacidade leve não pode preencher todos os critérios, e os atacantes podem explorar

informação estrutural para lançar vários ataques simultâneos.

IV. Metodologia

O trabalho global será composto por duas fases que serão descritas nos parágrafos seguintes. A primeira fase, descrita principalmente ao longo deste trabalho, centra-se na recolha do estado da arte em termos dos tópicos mais relevantes, dos quais foram selecionados os principais conceitos de privacidade a serem explorados na fase 1 da fase 2, com a preparação de um questionário para recolher as perceções dos utilizadores relativamente à privacidade e aos tópicos recolhidos na revisão sistemática da literatura. A segunda fase da Fase 2 consiste em desenvolver uma aplicação, parcialmente baseada na informação gerada pelo inquérito, que possa identificar que tipo de dispositivos existem, que tipo de dados são recolhidos por esses dispositivos, apresentar opções de privacidade ao utilizador quando disponíveis, e o que pode ser feito para evitar que dados indesejáveis sejam recolhidos.

The Phase 1 Systematic Literature Review gathered the most relevant papers discussing methodologies and techniques for the protection of users' privacy data with special focus on IoT systems. For this SLR, this paper considered focusing only on papers from the last 12 years, from 2010 until 2022, since papers before then become out of date with the evolution of technology. In this SLR, it was reviewed 54 papers published in top computer science, security, privacy and software engineering outlets.

This paper followed Keshav's three-pass approach [82] when choosing which papers to read fully and which ones to ignore, first the title would be read, then the abstract, the introduction and conclusion and briefly skim the rest of the paper and then decide if it was worth reading any further, the focal point in this phase was answering the following question: does the paper present a new methodology or interesting angle to tackle users' privacy concerns? Only then the document would be read in its entirety while ignoring any tables, figures, images or graphs. If the paper failed to present any interesting idea, approach, or technique it would be discarded, but if not, it would be read carefully from the beginning again in order to fully understand what it presents. Having collected the major findings, this work then aims to conduct a throughout study split in several stages and around the specific research questions which will be explored in each phase. For that matter, the research questions listed are:

Phase 1:

RQ1: What approaches are being considered for privacy issues in IoT in the currently available literature?

RQ2: What are user perceptions on online privacy?

Phase 2:

RQ3: How to empower users to protect their privacy rights?

RQ4: What issues are prevalent in IoT that make it difficult to address privacy and security problems?

The second phase will be evaluated on two stages, the first one consists on doing a study on people's general privacy concerns, while using and interacting with IoT devices. This study will abide on preparing a questionnaire to assess general user's knowledge on privacy concepts, their habits and concerns, their understanding of privacy rights, and what they do to safeguard those rights. The goal of this study is to both understand the privacy paradox and collect data on their proposal to address privacy issues with regard to IoT devices.

A. Estágio 1: Perceções do Utilizador

This study aims to understand people's perception of IoT and their privacy practices online. It also serves to demystify the privacy paradox and also to help provide a solution to the privacy issue in IoT. The questionnaire consists of 92 questions divided into 7 sections to access users' knowledge, it follows a kind of narrative, the first section being general privacy questions then about the predisposition to data sharing, to concerns with privacy then about daily digital routines, then about profile identification, and then about IoT general knowledge before a section about non-identifiable demographic data. The scale that is used in the questionnaire is based on the work of Philip K. Masur [83]. Great care is taken when it comes to this survey's data collection, in order to not identify any individual or group of individuals, for instance, when it comes to differential privacy, any data that might identify someone will not be disclosed, even though the data might suffer from some inaccuracy because of this.

This survey was partially based in a study done in the Philippines by the government in the context of their privacy act of 2012 [84], this was the second survey done on the country's population. It was also inspired by Alves's master's thesis [85], which was about citizen's perception about privacy in the wake of GDPR.

This survey was done through the internet, it was created in Google Forms, this way it is guaranteed to reach the most people possible, besides Google Forms itself, it will be used other online venues for distribution and even printing.

B. Estágio 2: Estudo no Contexto, uma Aplicação

This work proposes an application that gives users information about IoT devices in their surroundings like the type of information these devices collect and what privacy options are available. This application will be developed for mobile phones because it is the most used device that people take everywhere they go, and because the application will use georeferencing to show the location of the IoT devices. The main objective of this application is to give users another option in order to protect their private data. The application will show the geolocation of the IoT devices, what type of device it is, what type of data is being collect by the device. The application will not detect the devices by itself, this will be done by the users themselves, in the first few iterations of this application it was proposed that the application itself would detect the devices and would categorize what type of device it was and what type of data it was collecting but it

was discovered that this approach was too complex and so it was not feasible to do with the constraints of this paper. The application will be developed with Flutter, other options could be React Native or a progressive web application, but Flutter uses ahead of time and just in time compilation with Dart as it is programming language while React Native uses the Javascript programming language that was never created for mobile programming so it uses a bridge to convert Javascript to native components for Android or iOS. Flutter has better performance and as such it is the chosen framework for this application.

V. Estado Atual do Projeto

The preliminary results of the study, based on 10 responses, show that everyone agrees that privacy is important to them and some people know that they should not share their personal information with anyone they do not trust (like clicking on random urls or using unprotected websites/software), but most of them think that privacy and security are the same concept, most respondents also do not read privacy notices but accept them to access the information they want to get to, most respondents use their devices mostly to access social networks and for work, when it comes to IoT, there is a dissonance between knowing the term and using devices like smart watches or RFID enabled devices, from the respondents that answered yes to using IoT devices most use because of work. It is also noted that most respondent have a background in engineering, so the responses are skewed. As a result, the survey will remain open to gather a larger number of responses and participants for more significant results and generalizations.

Work plan	January				February				March				April				May			
Week	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Discovery and planning																				
Research enquiry																				
State of the art																				
Project requirements																				
Wireframes and user stories																				
Prototyping and refinement																				
Development																				
Tests and iterations																				
Release and documentation																				

TABLE I
Work plan timeline

As can be seen in Table I, the first months will involve the design of the application and the enquiry of the study followed by the development of the application and the synthesis of the study, and finally testing and refinement of the application. Because of the exploratory nature of this work the application might suffer alterations to the design, specially in the testing stage, and also depending on the results of the study.

VI. Trabalho Futuro

Although there are existing hardware solutions that can detect some devices on particular networks, like ZigBee or Bluetooth LE, namely IoT sniffers and there exist some georeferencing applications that try to pinpoint certain IoT devices, there is still a need for some kind of device or framework that is network agnostic and can detect where the devices are located and what kind of data the IoT devices that are around it are collecting. This gadget should also be capable of informing users about the privacy notices of the devices and what can the users do to safeguard their personal data. The IoT sniffers that are available are primarily used in the detection of problems in the communication of devices in the network or to solve problems of interoperability between different IoT networks. There are many obstacles that impede the creation of such a device and the fact that it still does not exist anything like it may be related ton either there iss not enough interest from users or researchers to focus on such an endeavour or the complexity of such a task is greater than the rewards.

VII. Conclusão

This project aims to do an exploratory analysis of privacy in IoT systems. It proposes a survey to better understand user's knowledge on this subject and an application that aims to create more users awareness and better inform about their environment, as well as the IoT devices that inhabit it and how they can respond accordingly.

Hopefully the work conducted on this project will be useful to further support researchers and the application that will be developed will be able to provide greater visibility, thus allowing users to acquire knowledge about the data being collected and how they can adjust their behaviour or respond more effectively to protect their privacy rights.

References

[1] D. Vincent, *Privacy: A short history*. John Wiley & Sons, 2016.

[2] B. Moore, *Privacy: Studies in social and cultural history*. Routledge, 2017.

[3] E. Roosevelt, P. C. Chang, C. Malik, W. R. Hodgson, H. S. Cruz, R. Cassin, A. E. Bogomolov, C. D. 1st Baron Dukeston, and J. P. Humphrey. (1948) Universal declaration of human rights. Accessed: 2022-11-05. [Online]. Available: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[4] I. A. for Privacy Professionals. (2021) What does privacy mean? Accessed: 2022-11-04. [Online]. Available: https://iapp.org/about/what-is-privacy/

[5] S. Spiekermann and L. F. Cranor, "Engineering privacy," *IEEE Transactions on Software Engineering*, vol. 35, no. 1, pp. 67–82, 2009.

[6] HIV.gov. (2018) The difference between security and privacy and why it matters to your program. Accessed: 2022-11-04. [Online]. Available: https://www.hiv.gov/blog/difference-between-security-and-privacy-and-why-it-matters-your-program

[7] P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into iot device purchase behavior," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–12.

[8] Y. J. Park, "Personal data concern, behavioral puzzle and uncertainty in the age of digital surveillance," *Telematics and Informatics*, vol. 66, p. 101748, 2022.

[9] N. A. Zhang, C. A. Wang, E. Karahanna, and Y. Xu, "Peer privacy concern: Conceptualization and measurement." *MIS Quarterly*, vol. 46, no. 1, 2022.

[10] M. Weiser, "The computer for the 21 st century," *Scientific american*, vol. 265, no. 3, pp. 94–105, 1991.

[11] K. Ashton. (2009) That "internet of things" thing. Accessed: 2022-11-05. [Online]. Available: https://www.rfidjournal.com/that-internet-of-things-thing

[12] D. Marikyan, S. Papagiannidis, and E. Alamanos, "A systematic review of the smart home literature: A user perspective," *Technological Forecasting and Social Change*, vol. 138, pp. 139–154, 2019.

[13] F. Arena, G. Pau, and A. Severino, "An overview on the current status and future perspectives of smart cars," *Infrastructures*, vol. 5, no. 7, p. 53, 2020.

[14] M. Al-Emran, S. I. Malik, and M. N. Al-Kabi, "A survey of internet of things (iot) in education: Opportunities and challenges," *Toward social internet of things (SIoT): enabling technologies, architectures and applications*, pp. 197–209, 2020.

[15] N. Niknejad, W. B. Ismail, A. Mardani, H. Liao, and I. Ghani, "A comprehensive overview of smart wearables: The state of the art literature, recent advances, and future challenges," *Engineering Applications of Artificial Intelligence*, vol. 90, p. 103529, 2020.

[16] I. F. Akyildiz and A. Kak, "The internet of space things/cubesats," *IEEE Network*, vol. 33, no. 5, pp. 212–218, 2019.

[17] C. Everhart, E. Caplan, and D. Nichols, "Re: Interesting uses of networking," https://cseweb.ucsd.edu/~bsy/coke.history.txt, 1990, accessed: 2022-12-14.

[18] J. Romkey, "Toast of the iot: The 1990 interop internet toaster," *IEEE Consumer Electronics Magazine*, vol. 6, no. 1, pp. 116–119, 2017.

[19] S. Madakam, V. Lake, V. Lake, V. Lake *et al.*, "Internet of things (iot): A literature review," *Journal of Computer and Communications*, vol. 3, no. 05, p. 164, 2015.

[20] M. Hasan. (2022) State of iot 2022: Number of connected iot devices growing 18% to 14.4 billion globally. Accessed: 2022-11-04. [Online]. Available: https://iot-analytics.com/number-connected-iot-devices/

[21] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of things market analysis forecasts, 2020-2030," in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2020, pp. 449–453.

[22] N. Alhirabi, O. Rana, and C. Perera, "Security and privacy requirements for the internet of things: A survey," *ACM Transactions on Internet of Things*, vol. 2, no. 1, pp. 1–37, 2021.

[23] D. Peloquin, M. DiMaio, B. Bierer, and M. Barnes, "Disruptive and avoidable: Gdpr challenges to secondary research uses of data," *European Journal of Human Genetics*, vol. 28, no. 6, pp. 697–705, 2020.

[24] A. Gladis, N. J. Hartwich, and O. Salge, "Weaponizing the gdpr: How flawed implementations turn the gold standard for privacy laws into fool's gold," 2022.

[25] G. Gentile and O. Lynskey, "Deficient by design? the transnational enforcement of the gdpr," *International & Comparative Law Quarterly*, vol. 71, no. 4, pp. 799–830, 2022.

[26] B. Green, "The flaws of policies requiring human oversight of government algorithms," *Computer Law & Security Review*, vol. 45, p. 105681, 2022.

[27] D. Y. Byun, "Privacy or protection: The catch-22 of the ccpa," *Loy. Consumer L. Rev.*, vol. 32, p. 246, 2019.

[28] D. Thomson, D. P. Cochrane, I. Chantzos, P. Carter, S. John, P. U. Helmbrecht, and S. Room, "State of privacy report 2015," Symantec, Tech. Rep., 2015.

[29] D. J. Solove, "The myth of the privacy paradox," *Geo. Wash. L. Rev.*, vol. 89, p. 1, 2021.

[30] M. Williams, J. R. C. Nurse, and S. Creese, "Privacy is the boring bit: User perceptions and behaviour in the internet-of-things," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, 2017, pp. 181–18 109.

[31] A.-R. Lee, "Investigating the personalization–privacy paradox in internet of things (iot) based on dual-factor theory: Moderating effects of type of iot service and user value," *Sustainability*, vol. 13, no. 19, p. 10679, 2021.

[32] D. Goad, A. T. Collins, and U. Gal, "Privacy and the internet of things-an experiment in discrete choice," *Information & Management*, vol. 58, no. 2, p. 103292, 2021.

[33] N. Gerber, P. Gerber, and M. Volkamer, "Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior," *Computers & security*, vol. 77, pp. 226–261, 2018.

[34] D. Wilson and J. S. Valacich, "Unpacking the privacy paradox: Irrational decision-making within the privacy calculus," 2012.

[35] J. Warshaw, T. Matthews, S. Whittaker, C. Kau, M. Bengualid, and B. A. Smith, "Can an algorithm know the" real you"? understanding people's reactions to hyper-personal analytics systems," in *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, 2015, pp. 797–806.

[36] N. Lee and O. Kwon, "A privacy-aware feature selection method for solving the personalization–privacy paradox in mobile wellness healthcare services," *Expert systems with applications*, vol. 42, no. 5, pp. 2764–2771, 2015.

[37] P. J. Zak, *Moral markets: The critical role of values in the economy*. Princeton University Press, 2008.

[38] A. Acquisti, S. Gritzalis, C. Lambrinoudakis, and S. di Vimercati, "What can behavioral economics teach us about privacy?" in *Digital privacy*. Auerbach Publications, 2007, pp. 385–400.

[39] B. P. Knijnenburg, A. Kobsa, and H. Jin, "Dimensionality of information disclosure behavior," *International Journal of Human-Computer Studies*, vol. 71, no. 12, pp. 1144–1162, 2013.

[40] R. Wakefield, "The influence of user affect in online information disclosure," *The Journal of Strategic Information Systems*, vol. 22, no. 2, pp. 157–174, 2013.

[41] C. Flender and G. Müller, "Type indeterminacy in privacy decisions: the privacy paradox revisited," in *International Symposium on Quantum Interaction*. Springer, 2012, pp. 148–159.

[42] T. Dienlin and S. Trepte, "Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors," *European journal of social psychology*, vol. 45, no. 3, pp. 285–297, 2015.

[43] Y. M. Baek, "Solving the privacy paradox: A counter-argument experimental approach," *Computers in human behavior*, vol. 38, pp. 33–42, 2014.

[44] M. Taddicken, "The "privacy paradox" in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure," *Journal of computer-mediated communication*, vol. 19, no. 2, pp. 248–273, 2014.

[45] P. A. Norberg, D. R. Horne, and D. A. Horne, "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of consumer affairs*, vol. 41, no. 1, pp. 100–126, 2007.

[46] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & security*, vol. 64, pp. 122–134, 2017.

[47] L. Brandimarte, A. Acquisti, and G. Loewenstein, "Misplaced confidences: Privacy and the control paradox," *Social psychological and personality science*, vol. 4, no. 3, pp. 340–347, 2013.

[48] W. Xie and K. Karan, "Consumers' privacy concern and privacy protection on social network sites in the era of big data: empirical evidence from college students," *Journal of Interactive Advertising*, vol. 19, no. 3, pp. 187–201, 2019.

[49] K. S. Schwaig, A. H. Segars, V. Grover, and K. D. Fiedler, "A model of consumers' perceptions of the invasion of information privacy," *Information & Management*, vol. 50, no. 1, pp. 1–12, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378720612000754

[50] S. Sannon, N. N. Bazarova, and D. Cosley, "Privacy lies: Understanding how, when, and why people lie to protect their privacy in multiple online contexts," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–13.

[51] S. Gupta and S. Ghanavati, "Privacy in the internet of things: Where do we stand? a systematic literature review," 5 2022. [Online]. Available: https://www.techrxiv.org/articles/preprint/Privacy_in_the_Internet_of_Things_Where_do_We_Stand_A_Systematic_Literature_Review/19874329

[52] P. Kühtreiber, V. Pak, and D. Reinhardt, "A survey on solutions to support developers in privacy-preserving iot development," *Pervasive and Mobile Computing*, vol. 85, p. 101656, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574119222000785

[53] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer networks*, vol. 76, pp. 146–164, 2015.

[54] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[55] J. Porras, J. Pänkäläinen, A. Knutas, and J. Khakurel, "Security in the internet of things-a systematic mapping study," 2018.

[56] B. S. Ahmed, M. Bures, K. Frajtak, and T. Cerny, "Aspects of quality in internet of things (iot) solutions: A systematic mapping study," *IEEE Access*, vol. 7, pp. 13 758–13 780, 2019.

[57] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the internet of things: threats and challenges," *Security and Communication Networks*, vol. 7, no. 12, pp. 2728–2742, 2014.

[58] M. Kearns and A. Roth, *The ethical algorithm: The science of socially aware algorithm design*. Oxford University Press, 2019.

[59] A. Frome, G. Cheung, A. Abdulkader, M. Zennaro, B. Wu, A. Bissacco, H. Adam, H. Neven, and L. Vincent, "Large-scale privacy protection in google street view," in *IEEE International Conference on Computer Vision*, 2009. [Online]. Available: https://research.google.com/archive/papers/cbprivacy_iccv09.pdf

[60] R. Poddar, G. Ananthanarayanan, S. Setty, S. Volos, and R. A. Popa, "Visor: Privacy-preserving video analytics as a cloud service," in *USENIX Security Symposium*, August 2020. [Online]. Available: https://www.microsoft.com/en-us/research/publication/visor-privacy-preserving-video-analytics-as-a-cloud-service/

[61] R. Shokri and V. Shmatikov, "Privacy-preserving deep learning," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2015, pp. 909–910.

[62] Y. Zhao and J. Chen, "A survey on differential privacy for unstructured data content," *ACM Comput. Surv.*, vol. 54, no. 10s, sep 2022. [Online]. Available: https://doi.org/10.1145/3490237

[63] M. Skirpan, M. Oates, D. Byrne, R. Cunningham, and L. F. Cranor, "Is a privacy crisis experienced, a privacy crisis avoided?" *Commun. ACM*, vol. 65, no. 3, pp. 26–29, feb 2022. [Online]. Available: https://doi.org/10.1145/3512325

[64] R. H. Weber, "Internet of things: Privacy issues revisited," *Computer Law & Security Review*, vol. 31, no. 5, pp. 618–627, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0267364915001156

[65] N. Fabiano, "Internet of things and blockchain: Legal issues and privacy. the challenge for a privacy standard," in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2017, pp. 727–734.

[66] Q. Sun, K. Lin, C. Si, Y. Xu, S. Li, and P. Gope, "A secure and anonymous communicate scheme over the internet of things," *ACM Trans. Sen. Netw.*, vol. 18, no. 3, apr 2022. [Online]. Available: https://doi.org/10.1145/3508392

[67] R. S. Antunes, C. André da Costa, A. Küderle, I. A. Yari, and B. Eskofier, "Federated learning for healthcare: Systematic review and architecture proposal," *ACM Trans. Intell. Syst. Technol.*, vol. 13, no. 4, may 2022. [Online]. Available: https://doi.org/10.1145/3501813

[68] B. Chen, S. Qiao, J. Zhao, D. Liu, X. Shi, M. Lyu, H. Chen, H. Lu, and Y. Zhai, "A security awareness and protection system for 5g smart healthcare based on zero-trust architecture," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10 248–10 263, 2021.

[69] A. Opara, H. Johng, T. Hill, and L. Chung, "A framework for representing internet of things security and privacy policies and detecting potential problems," in *Proceedings of the 37th ACM/SIGAPP Symposium on Applied Computing*, 2022, pp. 198–201.

[70] W. contributors. (2022) Privacy and blockchain. Accessed: 2023-01-02. [Online]. Available: https://en.wikipedia.org/wiki/Privacy_and_blockchain

[71] Y. Yu, Y. Li, J. Tian, and J. Liu, "Blockchain-based solutions to security and privacy issues in the internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 12–18, 2018.

[72] M. S. Ali, K. Dolui, and F. Antonelli, "Iot data privacy via blockchains and ipfs," in *Proceedings of the Seventh International Conference on the Internet of Things*, ser. IoT '17. New York, NY, USA: Association for Computing Machinery, 2017. [Online]. Available: https://doi.org/10.1145/3131542.3131563

[73] H. Zhu, S. C.-K. Chau, G. Guarddin, and W. Liang, "Integrating iot-sensing and crowdsensing with privacy: Privacy-preserving hybrid sensing for smart cities," *ACM Trans. Internet Things*, vol. 3, no. 4, sep 2022. [Online]. Available: https://doi.org/10.1145/3549550

[74] J. Colnago, Y. Feng, T. Palanivel, S. Pearman, M. Ung, A. Acquisti, L. F. Cranor, and N. Sadeh, "Informing the design of a personalized privacy assistant for the internet of things," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI '20. New York, NY, USA: Association for Computing Machinery, 2020, pp. 1–13. [Online]. Available: https://doi.org/10.1145/3313831.3376389

[75] Y. Feng, Y. Yao, and N. Sadeh, "A design space for privacy choices: Towards meaningful privacy control in the internet of things," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI '21. New York, NY, USA: Association for Computing Machinery, 2021. [Online]. Available: https://doi.org/10.1145/3411764.3445148

[76] A. Das, M. Degeling, D. Smullen, and N. Sadeh, "Personalized privacy assistants for the internet of things: Providing users with notice and choice," *IEEE Pervasive Computing*, vol. 17, pp. 35–46, 07 2018.

[77] N. Aleisa and K. Renaud, "Privacy of the internet of things: a systematic literature review (extended discussion)," *arXiv preprint arXiv:1611.03340*, 2016.

[78] E. D. P. Supervisor, "Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," Official Journal of the European Union, 1995.

[79] K. P. Tang, P. Keyani, J. Fogarty, and J. I. Hong, "Putting people in their place: an anonymous and privacy-sensitive approach to collecting sensed data in location-based applications," in *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, 2006, pp. 93–102.

[80] C. Kang, F. Abbas, and H. Oh, "Protection scheme for iot devices using introspection," in *2015 6th International Conference on the Network of the Future (NOF)*. IEEE, 2015, pp. 1–5.

[81] Y. Qu, S. Yu, W. Zhou, S. Peng, G. Wang, and K. Xiao, "Privacy of things: Emerging challenges and opportunities in wireless internet of things," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 91–97, 2018.

[82] S. Keshav, "How to read a paper," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 3, pp. 83–84, jul 2007. [Online]. Available: https://doi.org/10.1145/1273445.1273458

[83] P. K. Masur, *Situational privacy and self-disclosure: Communication processes in online environments*. Springer, 2018.

[84] P. Survey and R. Center. (2022) Conduct of privacy survey. Accessed: 2022-12-19. [Online]. Available: https://www.privacy.gov.ph/wp-content/uploads/2022/01/CONDUCT-OF-PRIVACY-SURVEY-Final-Report-v3.pdf

[85] M. H. d. S. Alves, "Gdpr in portugal: Analysis of citizens' perception about privacy," 2021.