

2023

**MARIANA ALVES
CARVALHO**

**VIOLÊNCIA DOMÉSTICA E TECNOLOGIA:
ANÁLISE DE EXPERIÊNCIAS E POSSÍVEIS
CENÁRIOS EM RELAÇÃO A *SMART PRODUCTS***

2023

**MARIANA ALVES
CARVALHO**

**VIOLÊNCIA DOMÉSTICA E TECNOLOGIA:
ANÁLISE DE EXPERIÊNCIAS E POSSÍVEIS
CENÁRIOS EM RELAÇÃO A *SMART PRODUCTS***

Dissertação apresentada ao IADE - Faculdade de Design, Tecnologia e Comunicação da Universidade Europeia, para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Design de Produto e do Espaço realizada sob a orientação científica da Doutora Hande Ayanoglu, professorAra auxiliar no IADE - Faculdade de Design, Tecnologia e Comunicação da Universidade Europeia e Doutor Rodrigo Hernández Ramírez, professor auxiliar no IADE - Faculdade de Design, Tecnologia e Comunicação da Universidade Europeia.

Aos meus pais,
Elsa e José.

Aos meus avós,
Elisa e Domingos.

E a todas as vítimas.

agradecimentos

Começo por agradecer profundamente à minha orientadora, a professora Doutora Hande Ayanoglu, pelo privilégio que foi contar com a sua orientação e acima de tudo por exigir sempre mais de mim. Foi essencial durante esse último ano para a conclusão desta dissertação. Ao meu orientador, o professor Doutor Rodrigo Hernández Ramírez, pela sinceridade e rigor na orientação da investigação. Ao professor Davide Parrilli pela ajuda prestada e disponibilidade.

Especialmente aos meus pais, avós e irmãs pelas palavras de apoio perante as minhas escolhas e pelas palavras de conforto e força. Sem eles nunca teria sido possível alcançar esta formação.

Sem dúvida aos meus amigos, sou grata pelo apoio incondicional. Indiscutivelmente, em especial um agradecimento ao Ricardo, à Rita e ao Boris, que foram uma força para mim, nos momentos de maior tensão.

Por fim, um agradecimento especial aos participantes dos questionários, às técnicas da APAV e ILGA pela simpatia e a todos que de forma direta, ou indiretamente, contribuíram para a conclusão desta dissertação.

Palavras-chave

Violência Doméstica; Consciencialização; Tecnologia; *Smart products*; Privacidade.

resumo

Nos últimos anos, o aumento da popularidade e modernização da tecnologia tem dado oportunidade a perpetradores para o surgimento de novas formas de violência. Este abuso emergente, facilitado pela tecnologia, é uma forma insidiosa de violência praticada pelo parceiro íntimo que abrange uma série de comportamentos propícios online e, cada vez mais, através do uso indevido de *smart products*. No entanto, estatísticas locais e a nível nacional indicam que este é um problema grave na sociedade e, enquanto não existir consciencialização global deste problema, o mercado continuará a oferecer uma variedade de soluções na forma de dispositivos que estão muitas das vezes a facilitar o abuso e não a oferecer segurança. Diante deste cenário, o objetivo é identificar como os *smart products* podem viabilizar novas formas de perseguição e abuso. Para isso, a estruturação do documento compreendeu-se em cinco partes: a primeira consiste numa introdução ao problema estudado, num enquadramento global e a relevância deste estudo, contendo ainda a estruturação da pesquisa com definição das componentes específicas, desenvolvimento de hipóteses e metodologia. Na segunda parte, foi realizada uma revisão sistémica de artigos da literatura para identificar o quadro atual da violência e a sua associação com a tecnologia. Para complementar a pesquisa, na terceira parte foi incluída uma análise de *benchmarking* de *smart products*. Na quarta parte, para examinar as novas formas de violência, iniciou-se um plano de recolha e análise de dados por meio de questionário. Finalmente, na parte cinco desenvolveu-se cenários futuros, de forma a otimizar a parte anterior de natureza prática. Este estudo comprovou que, de facto, as próprias vítimas podem não ter noção clara dos limites, nos quais os comportamentos de controlo se tornam abusivos, reforçando a importância que precisa de ser dada a este problema.

Keywords

Domestic Violence; Awareness; Technology; *Smart products*; Privacy.

Abstract

In recent years, the increasing popularity and modernization of technology has given perpetrators the opportunity for new forms of violence to emerge. This emerging abuse, facilitated by technology, is an insidious form of intimate partner violence that encompasses a range of enabling behaviors online and, increasingly, through the misuse of smart products. However, local and national statistics indicate that this is a serious problem in society and until there is global awareness of this problem, the market will continue to offer a variety of solutions in the form of devices that are often facilitating abuse rather than offering safety. Against this backdrop, the goal is to identify how smart products can enable new forms of stalking and abuse. To this end, the document was structured in five parts: the first consists of an introduction to the problem under study, an overall framework and the relevance of this study, and also contains the structuring of the research with the definition of the specific components, hypothesis development, and methodology. In the second part, a systemic review of literature articles was conducted to identify the current picture of violence and its association with technology. To complement the research, in the third part a benchmarking analysis of smart products was included. In part four, to examine the new forms of violence, a questionnaire-based data collection and analysis plan was initiated. Finally in part five future scenarios were developed in order to optimize the previous practical part. This study has proven that, in fact, the victims themselves may not have a clear sense of the limits at which controlling behaviors become abusive, reinforcing the importance that needs to be given to this problem.

Palavras-chave.....	i
Resumo.....	i
Keywords.....	iii
Abstract	iii
Palavras-chave.....	ii
Índice Geral	vi
Índice de Figuras	ix
Índice de Tabelas.....	xii
Listas de Abreviaturas, Siglas e Acrónimos.....	xv
CAPÍTULO 1 Introdução	1
1.1 Contextualização da Investigação	1
1.2 Problema de Investigação.....	2
1.3 Motivação.....	3
1.4 Questão de Investigação e Objetivos.....	4
1.5 Hipóteses de investigação	5
1.6 Benefícios de Investigação.....	8
1.7 Diagrama de Estudo	9
1.8 Metodologia e Planificação da Investigação.....	10
1.9 Estruturação e Desenvolvimento da Investigação.....	11
CAPÍTULO 2 Enquadramento Teórico	13
2.1 Introdução.....	13
2.2 Design contra o Crime.....	13
2.3 Violência	15
2.3.1 Violência Doméstica	16
2.3.2 Tipos de Violência.....	25
1. Violência financeira/econômica.....	25
2. Violência psicológica	25

3. Violência Emocional	26
4. Violência física.....	27
5. Violência Sexual.....	27
2.3.3 Prevenção da Violência Doméstica.....	29
2.4 Enquadramento Legal Atual em Portugal	30
2.5 Associações de Apoio às Vítimas em Portugal.....	31
1. APAV- Associação Portuguesa de Apoio à Vítima	31
2. ILGA	31
3. CETA.....	32
4. <i>UN Women</i>	33
2.6 Tecnologia e a Violência Doméstica.....	34
2.6.1 <i>Smart Homes</i>	36
2.6.2 Violência doméstica na era das <i>smart homes</i>	39
2.6.3 IoT e <i>Smart Products</i>	40
2.7 Conclusão.....	43
CAPÍTULO 3 Benchmarking de <i>Smart Products</i> Existentes.....	44
3.1 Introdução.....	44
3.2 Análise de Produtos.....	44
3.3 Rastreadores GPS	58
CAPÍTULO 4 Perceção das Vítimas.....	63
4.1 Introdução.....	63
4.2 Inquérito por Questionário	63
4.2.1 Participantes	63
4.2.2 Material e Procedimentos de Recolha de Dados.....	65
4.3 Análise e Discussão dos Resultados.....	71
4.4 Conclusão.....	88
CAPÍTULO 5 Design Especulativo e Cenários Possíveis.....	91

5.1 Introdução.....	91
5.2 Os Princípios de Design Especulativo na Investigação de Design.....	91
5.3 Design Especulativo nas Preocupações de Privacidade	92
5.4 Cenários Possíveis	94
Cenário 1: Aplicações <i>Stalkerware</i>	95
Cenário 2- iRobot	97
Cenário 3- Luzes inteligentes	99
Cenário 4: Rastreador de localização	101
5.5 Conclusão	103
CAPÍTULO 6 Conclusão e Trabalhos Futuros.....	105
6.1 Conclusões e Implicações da investigação.....	105
6.2 Limitações e Futuras Investigações.....	109
REFERÊNCIAS BIBLIOGRÁFICAS	110
ANEXOS	124
Anexo I - Guião de abordagem em questionário presencial.....	125
Anexo II - Guião de abordagem em questionário para associações.....	126
Anexo III - Guião de abordagem em questionário para publicação em redes sociais e mensagens diretas.....	128
Anexo IV- Questionário	129
Anexo V- Tratamento dos Dados	142
Anexo VI- Resultados do questionário no SPSS.....	156

Índice de Figuras

Figura 1: Diagrama de estudo.	9
Figura 2: Ciclo da violência doméstica.	17
Figura 3: História da tecnologia da casa inteligente. (Fonte: Baseado em Harbour Research, 2021).....	37
Figura 4: A evolução das <i>Smart homes</i>	38
Figura 5: Diagrama de Abuso. (Fonte: Baseado em Tanczer, 2018)	40
Figura 6: Primeiro produto IoT. (Fonte: Montagem baseada em Romkey, 2017)	41
Figura 7: Amazon Echo (Fonte: Google images).....	45
Figura 8: Apple AirTag. (Fonte: Google images)	47
Figura 9: iRobot Roomba j7+ com esvaziamento automático e ligação Wi-Fi (Fonte: Raff et al. 2020).....	48
Figura 10: Ecobee Smart Thermostat Premium (Fonte: Delaney, 2022)	49
Figura 11: Apple watch series 8. (Fonte: Apple, 2021)	50
Figura 12: Yale Assure Lock 2, fechadura inteligente. (Fonte: Yale, 2022).....	51
Figura 13: Ring Cam on Mount, câmara de vigilância. (Fonte: Delaney, 2019)	52
Figura 14: Phillips Hue <i>Smart Light</i> Starter Kit, luzes inteligentes. (Fonte: Staff, 2019).....	53
Figura 15: Computador e Ipad. (Fonte: Google images).....	55
Figura 16: Tomada inteligente Xiaomi Mi Smart Power Plug. (Fonte: You Get)	56
Figura 17: Imagens do espaço de recolha presencial.	70
Figura 18: Estatísticas de confiabilidade.....	72
Figura 19: Perfil Demográfico.	73

Figura 20: Diferenças de conhecimento sobre sistemas inteligentes.	77
Figura 21: Resultados da frequência de utilização da internet.	78
Figura 22: Resultados da frequência de utilização de sistemas e <i>smart devices</i>	80
Figura 23: Resultados da questão 15, sobre conforto com a monitorização.	82
Figura 24: Resultados à pergunta 16, quantidade de <i>smart products</i>	83
Figura 25: Resultados da média de <i>smart products</i> por género.	84
Figura 26: Resultados de género sobre o tipo de vítima.	85
Figura 27: Resultados questão 17, privacidade pessoal.	86
Figura 28: Resultados do questionário em SPSS, rastrear é intrusivo.	87
Figura 29: Preocupação de que seja rastreada a localização ao fazer uma publicação.	88
Figura 30: Diagrama PPPP de futuros potenciais (Dunne & Raby, 2013).	92
Figura 31: Cenário dedicado a aplicações <i>salkerware</i>	96
Figura 32: Cenário dedicado a iRobot.	98
Figura 33: Cenário dedicado às luzes inteligentes.	100
Figura 34: Cenário dedicado a rastreadores de localização.	102
Figura 35: Resultados do questionário em SPSS Residente em Portugal.	156
Figura 36: Resultados do questionário em SPSS Região.	156
Figura 37: Resultados do questionário em SPSS Idade.	157
Figura 38 Resultados do questionário em SPSS género.	157
Figura 39: Resultados do questionário em SPSS Habitação.	158
Figura 40: Resultados do questionário em SPSS Escolaridade.	159

Figura 41: Resultados do questionário em SPSS Emprego.....	159
Figura 42: Resultados do questionário em SPSS Descrição do Relacionamento.	160
Figura 43: Resultados do questionário frequência de utilização da Internet.....	162
Figura 44: Diferença da quantidade de <i>smart products</i> entre género.....	164
Figura 45: Medição do risco de produtos de rastreamento sejam intrusivos.	168
Figura 46: Medo de rastrear a localização em publicações, questão 23.....	169

Índice de Tabelas

Tabela 1: Hipóteses de investigação.	7
Tabela 2: Perfil geral das vítimas (Fonte: Apav, 2021).....	20
Tabela 3: Tipo de contacto efetuado para a APAV (Fonte: APAV, 2021)	20
Tabela 4: Idade da vítima. (Fonte: Apav, 2021).....	21
Tabela 5: Comparação do número de vítimas entre concelhos (Fonte: APAV, 2019; APAV, 2021).....	22
Tabela 6: Idade do/a autor/a do crime. (Fonte: Apav, 2021).....	23
Tabela 7: Escolaridade do/a autor/a do crime. (APAV, 2021).....	24
Tabela 8: Identificação das características dos smart products.....	57
Tabela 9: Aplicações, websites e dispositivos que rastreiam a localização.	60
Tabela 10: Produto físico, rastreador de localização.....	61
Tabela 11: Frequência para toda a amostra.....	65
Tabela 12: Descrição das perguntas e secções do questionário.	69
Tabela 13: Características sociodemográficas global.....	75
Tabela 14: Identificação da seção um do questionário.....	142
Tabela 15: Variáveis presentes nos dados demográficos	143
Tabela 16: Identificação da seção dois do questionário.....	144
Tabela 17: Variáveis presentes na secção de experiência tecnológica.....	148
Tabela 18: Identificação da seção três do questionário.....	150
Tabela 19: Variáveis presentes na secção de privacidade pessoal.	151

Tabela 20: Identificação da seção quatro do questionário.....	152
Tabela 21: Identificação da seção quatro do questionário.....	152
Tabela 22: Identificação da seção cinco do questionário.....	153
Tabela 23: Identificação da seção cinco do questionário.....	154
Tabela 24: Resultado do questionário em SPSS Região.....	156
Tabela 25: Resultados do questionário em SPSS Idade.....	157
Tabela 26: Resultados do questionário em SPSS género.....	158
Tabela 27: Resultados do questionário em SPSS Habitação.....	158
Tabela 28: Resultados do questionário em SPSS Escolaridade.....	159
Tabela 29: Resultados do questionário em SPSS Emprego.....	159
Tabela 30: Resultados do questionário em SPSS Descrição relacionamento.....	160
Tabela 31: Resultados do questionário em SPSS Sistemas inteligentes.....	160
Tabela 32: Resultados do questionário em SPSS Rastreadores GPS.....	161
Tabela 33: Resultados do questionário frequência de utilização da Internet.....	162
Tabela 34: Resultados do questionário frequência de utilização.....	163
Tabela 35: Diferença da quantidade de <i>smart products</i> entre vítimas e não vítimas.....	164
Tabela 36: Comparação de dados da questão 17.....	165
Tabela 37: Comparação de dados de género, questão 18.....	166
Tabela 38: Comparação de dados de género, questão 19.....	167
Tabela 39: Comparação de dados de género, questão 20.....	167
Tabela 40: Medidas de proteção do assédio ou abuso online.....	168

Tabela 41: Género e tipo de vítima..... 169

Listas de Abreviaturas, Siglas e Acrónimos

AMCV | Associação de mulheres Contra Violência

AMBraga | Associação Mulheres de Braga

IADE | Instituto de Artes Visuais, Design e Marketing

APAV | Associação Portuguesa de Apoio à Vítima

BLE | *Bluetooth Low Energy*

CETA | *Clinic to End Tech Abuse*

EMAV | Equipa Multidisciplinar de apoio à vítima de Violência Doméstica

ILGA | Intervenção Lésbica, Gay, Bissexual, Trans e Intersexo

IOT | *Internet of things*

ODS | Objetivos de Desenvolvimento Sustentável

ONG | Organização não governamental

ONU | Organização das Nações Unidas

PSP | Polícia de segurança pública

TCP/IP | Protocolo de controle de transmissão/Protocolo da internet

TIC | Tecnologias de informação e comunicação

WHO | *World health organization*

CAPÍTULO 1 | Introdução

1.1 Contextualização da Investigação

Este estudo pretende ser um resumo de ideias, conceitos, estudos e investigação previamente desenvolvidos e publicados, considerando as áreas do conhecimento e períodos cronológicos. Até à data, no que diz respeito à parte empírica, existe todo um passado literário que perpetua a violência doméstica “tradicional”, interligando-a com a tecnologia. Muitas vezes, essa distinção é feita porque as tecnologias facilitam aos perpetradores de violência doméstica meios que expandem o controle e abuso. Este problema de ordem grave a nível mundial, causa mortes diariamente devido à violência de género. Existem muitas soluções que visam promover o bem-estar e, conseqüentemente, reduzir este problema, mas com o crescente avanço tecnológico nenhuma se mostrou eficaz.

Para responder à proposta de análise desta dissertação, o termo “*smart product*” foi adotado, tendo em consideração os vários fatores limitadores. O termo frequentemente é usado como um termo genérico e não há consenso sobre o que realmente é um produto inteligente (Raff et al. 2020). Percebeu-se também que existe uma maior confusão com os termos na pesquisa em português pois este pode ser aplicado noutros contextos. Segundo Raff et al. (2020), esses conflitos com terminologias limitam o avanço sistemático do campo de análise e impedem a integração do conceito de produto inteligente em conceitos relacionados, como a Internet das Coisas (IoT). Desta forma, numa tentativa de não haver tanta dispersividade ou confusão, optou-se pela abordagem do termo em inglês, “*smart product*”. De acordo ainda com Raff et al. (2020), este termo têm ganho importância nas últimas décadas, entre os especialistas em tecnologia, académicos e políticos, impulsionada pelos avanços tecnológicos. Com essa importância, os *smart products* tornaram-se uma realidade tangível, e cada vez mais acessível, o que contribuiu para a rotura de alguns mercados tradicionais (Brock, 2019).

Os dispositivos tecnológicos foram ganhando espaço considerável, integrando-se no quotidiano das pessoas, tal como as *smart homes*. Em geral, uma casa inteligente, tradução direta de “*smart homes*”, difere de uma casa tradicional, através da adição de *smart products* domésticos, que se referem a vários componentes de *hardware* e *software* que, através da sua conexão online, permitem a autonomia bem como controle localizado ou remoto do ambiente em que estão inseridos (Hargreaves & Wilson, 2017). Esta definição reconhece que as casas inteligentes têm configurações e podem variar de alguns dispositivos a uma casa totalmente autónoma, além de que a interface de software que controla a casa e que a torna inteligente é

normalmente uma aplicação. Já o hardware é um monitor montado na parede. Os dois diferem entre si pela sua mobilidade, um sendo transportável e o outro fixo num ponto da casa. Caso exista a possibilidade de ativação por voz, esta mobilidade deixa de ser um fator relevante.

A violência doméstica facilitada pelas tecnologias é um tema relativamente novo. Não existe muita literatura sobre esta questão emergente, especialmente em Portugal. Por esse motivo, neste capítulo procurou-se perceber os fundamentos teóricos básicos iniciais do problema da violência, tal como a motivação, a questão de investigação, os benefícios e ainda estruturação do documento.

1.2 Problema de Investigação

Em 1948, a violência de género foi reconhecida como uma violação dos direitos humanos pela assembleia geral da Organização das Nações Unidas (ONU, 2022) na sua “Declaração Universal dos Direitos Humanos”. Esse documento reconhece que a violência ocorre em diversos setores da sociedade e é um indicativo da desigualdade de género na história da humanidade.

Logo após, em 1995, também as Nações Unidas publicaram uma declaração de Beijing e a sua plataforma para ação, que ainda na atualidade é usada para guiar as nações a atingirem a igualdade de género (UN WOMEN, 2020). Apesar destas iniciativas internacionais, a violência e a discriminação de género permanecem e sofrem alterações que muitas vezes tornam os casos difíceis de comprovar, de tal forma que, infelizmente não se conhece bem o alcance dos problemas, embora as investigações deste carácter tenham aumentado acentuadamente nos últimos anos (Taylor & Xia, 2018).

Este interesse prende-se com o facto de cada vez mais ser necessário perceber e tentar minimizar os efeitos da violência por parceiros íntimos facilitada pela tecnologia. Existem fatores que dificultam a compreensão profunda deste problema por utilizarem diferentes termos para descrever fenómenos semelhantes ou idênticos, incluindo a perseguição de parceiros íntimos facilitada pela tecnologia (Woodlock, 2017), agressão de encontros eletrónica (Smith-Darden et al., 2017), abuso de encontros virtuais (Peskin et al., 2017), violência digital (Hellevik & Øverlien, 2016) e outros. Vários termos para analisar a mesma coisa criam uma grande confusão e conclusões aparentemente contraditórias entre os investigadores (Henry et al., 2020).

Parceiros íntimos são aqueles que compartilham um relacionamento pessoal, que pode ser visto como uma conexão emocional, contacto regular, contacto físico contínuo, comportamento sexual ou identificarem-se como casal, podendo ser casados ou apenas

namorados (Breiding et al. 2015). Nesses casos, os desenvolvimentos tecnológicos são considerados um contributo fulcral para a proximidade e facilidade de comunicação mesmo com a distância física, mas também para a consolidação de novas relações (Mosley & Lancaster, 2019; Reed et al. 2017). Apesar desses benefícios, notou-se que esses desenvolvimentos contínuos podem ter contribuído para uma mudança do paradigma tradicional da violência. Esta preocupação comum a todos, prendeu-se em perceber e promover mudanças de comportamento com pensamento nas gerações futuras, na certeza de que o designer, é também responsável por suscitar essas mudanças na comunidade.

1.3 Motivação

Esta dissertação provém de um primeiro projeto e pesquisa, executado no primeiro ano de mestrado, entre setembro de 2020 a janeiro de 2021. Este projeto focou-se na violência doméstica durante a pandemia e resultou num protótipo de um produto inteligente para ser usado apenas por mulheres, para que pudessem pedir ajuda em caso de agressão.

No decorrer desse projeto, percebeu-se que a tecnologia é uma preocupação cada vez maior para as vítimas. Um reflexo dessa preocupante situação da violência ligada à tecnologia é o resultado obtido ao se procurar artigos com as palavras “*domestic violence with technology*”, (tradução de “violência doméstica com tecnologia” em inglês) no *website* Google Scholar (2022), onde são encontradas 1160 notícias a nível global entre 1 de janeiro e 10 de agosto de 2022, o que equivale uma média de 5,22 notícias por dia. Entre os resultados encontrados nessa busca, verificam-se artigos que falam da tecnologia de forma negativa onde é abordado o *stalking*, violência doméstica digital nas universidades, a saúde mental e como esta afeta as vítimas de violência doméstica através da tecnologia, violência sexual facilitada pela tecnologia, entre outros vários assuntos. Por outro lado, a tecnologia também é abordada de forma positiva, como para apoiar vítimas, entre elas crianças e jovens, durante e após a pandemia, formas online de fornecer esse apoio, práticas de segurança digital dos defensores do abuso de tecnologia, entre outros. Este resultado somente reporta crimes notificados e estudos científicos. Verifica-se, no entanto, uma potencial subnotificação deste tipo de ocorrências, o que indica um número ainda maior de casos de violência doméstica com tecnologia. Além disso, a maior parte dessas investigações baseiam-se no contacto interpessoal entre os abusadores e as vítimas no mundo real.

Com a internet e outras tecnologias, como telemóveis e produtos inteligentes, que se tornaram mais amplamente disponíveis em todo o mundo, a ocorrência de crimes utilizando essas tecnologias aumentou ao mesmo tempo (Poushter, 2016, Vogels, 2021). Isto leva a que

muitos abusadores procurem esses produtos inteligentes com o intuito de monitorizar a vítima e não para sua proteção ou utilização devida. Um dos casos mais recentes, diz respeito ao *smart device* AirTag, lançado em 2021, criado com o principal objetivo de rastrear coisas, facilitando assim, em casos de furto ou perda (Mace & Caxemira, 2021), que as vítimas localizem os seus pertences através da aplicação ‘Find My’, trazendo aos seus utilizadores mais segurança ao manterem o controle sobre as suas coisas. Estes rastreadores GPS têm sido utilizados para controle e perseguição de pessoas. Muitos desses casos foram notificados pela The New York Times ainda no ano em que foram lançados. Segundo Mace and Caxemira (2021), Ashley com 24 anos recebeu uma notificação no seu telemóvel em que dizia que um AirTag havia sido visto pela primeira vez quatro horas antes, e um mapa do AirTag onde mostrava os caminhos em ziguezague que esta havia percorrido nesse dia. Várias notícias foram igualmente postadas, com assuntos similares no TikTok, Reddit e Twitter acerca de AirTag’s encontrados em carros e em pertences pessoais. Ainda Mace and Caxemira (2021) relataram que, mesmo após a vítima ligar para a polícia, estes indicaram que a sua situação não era uma emergência e, caso quisesse apresentar denúncia, teria que levar o dispositivo com a mesma, o que não aconteceu pois a vítima desfez-se dele com o medo.

Outro caso de denúncia foi novamente de uma mulher que recebeu uma notificação a informar que estava sendo rastreada. Mais uma vez foi informada pela polícia que apenas poderia ser registada a queixa se alguém aparecesse em sua casa e que as notificações de rastreamento não são provas suficientes (Mace & Caxemira, 2021). Mesmo que este *smart product* alerte em caso de estar perto de dispositivos móveis, no caso do AirTag, o mesmo só acontece se estes forem do mesmo sistema operativo. Mesmo quando avisa, muitas das vezes apenas ocorre várias horas e até dias depois (Mace & Caxemira, 2021). Estes acontecimentos levantam questões sobre privacidade pessoal que suscitam interesse sobre a análise de *smart products* no mercado, com intuito de se criar alternativas a estes problemas.

1.4 Questão de Investigação e Objetivos

Num primeiro momento, a questão que deu início à presente investigação e que marca o início da investigação sobre violência doméstica era: “Como impedir que os dispositivos IoT sejam utilizados como ferramentas para abusos domésticos?”. Em seguida, após o levantamento da revisão de literatura, percebeu-se a escassez de pesquisas sobre a intersecção da violência do parceiro íntimo, perseguição e abuso com base na tecnologia em Portugal. Portanto, o principal objetivo é descrever e fornecer uma visão geral da perseguição e abuso sob influência crescente da tecnologia, praticada e relacionada com espaços e dispositivos

inteligentes, de forma a responder à questão de investigação **“*Smart products* podem viabilizar novas formas de perseguição e abuso na violência sobre o parceiro íntimo?”**

Para cumprir os requisitos previamente abordados inerentes à definição e delimitação do problema emergentes na especificação do estudo, os objetivos são estabelecidos com base na operacionalidade e no alcance da investigação. Foram examinados sistematicamente os artigos e pesquisas publicados nos últimos anos, de modo a preencher a lacuna na atual compreensão da violência doméstica facilitada pela tecnologia, particularmente pelos *Smart products* e assim reforçar o rigor do campo e orientar investigações e projetos futuros. Ao obter respostas para este objetivo principal, os seguintes objetivos secundários da presente dissertação são:

- Investigar a revisão da literatura sobre o atual quadro teórico examinado em estudos e as características da violência doméstica, os tipos de violência e fatores influenciadores envolvidos no processo de utilização de produtos/dispositivos e casas inteligentes.
- Navegar nas áreas de *smart products* e de *IOT*, bem como compreensão do que são produtos inteligentes e como são inteligentes. Mostrar como os produtos podem ser conceptualizados de formas distintas.
- Identificar as perceções e experiência dos usuários em sistemas inteligentes e rastreadores GPS em relação à confiança, monitorização, rastreamento e vigilância.
- Especular o efeito da utilização indevida das tecnologias domésticas inteligentes através das lentes de género e como as pessoas percebem as oportunidades e desvantagens.

1.5 Hipóteses de investigação

Como a violência doméstica facilitada pela tecnologia é um fenómeno relativamente novo, não há muita literatura sobre a questão emergente, especialmente em Portugal. O quadro teórico incluiu elementos de pesquisas anteriores de vários autores, nomeadamente alguns dos quais referenciados na Tabela 1. Esta dissertação procurou validar 6 hipóteses de investigação. O critério de validação utilizou o método indutivo.

Na primeira hipótese, foi desenvolvido um quadro de análise, com uma avaliação qualitativa e interpretativa, uma listagem e análise de produtos que partilham a localização, com objetivo de identificar semelhanças, conjugados com a literatura.

Para segunda hipótese, foi igualmente utilizada uma avaliação qualitativa e interpretativa através da criação de possíveis cenários.

A terceira, quarta, quinta e sexta hipóteses foram comprovadas pela análise dos questionários. Este método colocou em evidência o abuso facilitado pela tecnologia desenvolvido também numa análise teórica descritiva inicial. O método quantitativo foi o mais indicado para a análise, pois traz uma abordagem visual para a validação das hipóteses.

Tabela 1: Hipóteses de investigação.

Hipóteses	Referência
H1 A violência doméstica pode aumentar devido à falta de privacidade. Há muitos produtos e serviços que violam a privacidade ao partilhar a localização.	Mace and Caxemira (2021); Faria and Lauriault (2021); YWCA (2017).
H2 Design especulativo pode ajudar a mostrar potenciais resultados e possibilidades de design que devem surgir no futuro.	Dunne and Raby (2013); Malpass (2016); O'Regan (2020).
H3 Os <i>smart products</i> atuam como potenciais viabilizadores de controle e violência doméstica.	Bowles (2018); Sovacool et al. (2021); Faria (2020); Faria and Lauriault (2021); Freed et al. (2018); Open North (2021); Dunn (2020); YWCA (2017); Harry (2020); Dragiewicz et al. (2018, 2019); Lenhart et al. (2016); (Harris & Woodlock, 2022)
H4 Existe uma maior taxa de prevalência em vítimas de <i>smart products</i> do género feminino do que masculino.	Joshi (2022); Ghebreslassie (2018); Snook et al. (2017); Silva (2022); Sovacool et al. (2021); Webermann, Brand e Chasson (2014); APAV (2020).
H5 Dada a omnipresença da tecnologia, algum grau de vigilância social como o de monitorar pode ser considerado uma parte aceitável dos relacionamentos íntimos.	Sovacool et al. (2021) ; Bugeja et al. (2018); Marwick (2012); Lenhart et al. (2016)
H6 O género influencia a tolerância e confiança ao risco de <i>smart homes</i> e tecnologias domésticas inteligentes.	Marganski et al. (2015); Rio et al. (2021); Bugeja et al. (2018); Harry (2020).

1.6 Benefícios de Investigação

A maior parte dos estudos foram publicados recentemente, nos últimos 5 anos, com foco nos EUA, revelando um interesse emergente na violência doméstica facilitada pela tecnologia. No entanto, o maior foco dessas pesquisas é baseado na gravidade do impacto na saúde mental das vítimas, concluindo que o desenvolvimento dessas tecnologias mais avançadas traz problemas para pessoas vulneráveis. Como mostram estatísticas recentes do Pew Research Center, a percentagem de americanos que relataram experiências de assédio online aumentou de 14% para 20% entre 2016 e 2017, de maneira que, quantos mais indivíduos vivenciarem vitimação por meio tecnológico, mais urgentes são as pesquisas nesse campo (Vogels, 2021, Kim et al., 2022).

Neste contexto, mais conhecimento e formação sobre o problema do abuso tecnológico proveniente de produtos inteligentes gera mais consciência social nas gerações futuras e organizações, permitindo a criação de desenvolvimento de sistemas informáticos mais seguros e, conseqüentemente, produtos mais seguros também. Essa mudança de pensamento gera novos padrões de comportamentos que, por sua vez, obrigam os governos a tomar medidas na aplicação de leis para garantirem que o uso de IoT em residências inteligentes pelos seus utilizadores seja exclusivamente para conveniência dos próprios e não para facilitar o abuso (Joshi, 2022). Este estudo concebe uma oportunidade de combinar os dados que já existem sobre o tema no mundo em geral e comparar com uma amostra da população de Portugal.

1.7 Diagrama de Estudo

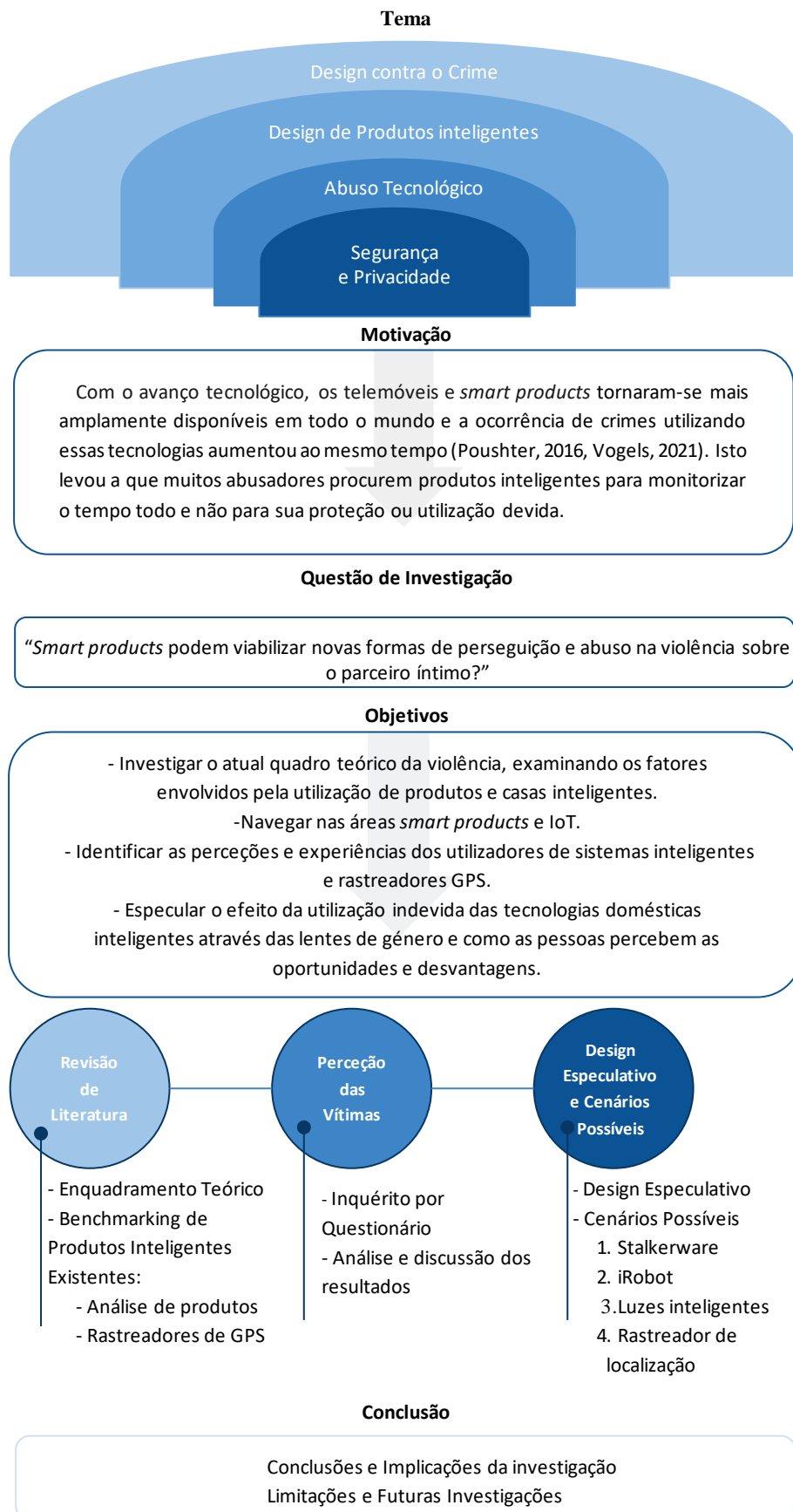


Figura 1: Diagrama de estudo.

1.8 Metodologia e Planificação da Investigação

Esta investigação tem carácter exploratório e é fundamentada em estudos qualitativos com dados secundários de pesquisa bibliográfica, para compreender o objeto de estudo e assim entender a dimensão do problema apresentado.

Mediante consultas de vários artigos, outras dissertações e organizações, foi realizado de um quadro teórico de acontecimentos fundamentais, a fim de contextualizar o ponto de vista dos serviços de apoio, a natureza e os impactos do abuso facilitado pela tecnologia e também com o intuito de observar o nível de conhecimento verificado nessas áreas de interesse inerentes.

Prosegue-se para um método de análise de *benchmarking*, que segundo Amirteimoori et al. (2022) trata-se de um procedimento de medição que permite identificar e comparar o desempenho de produtos e concorrentes que existem no mercado. O *benchmarking* é uma ferramenta de medição de desempenho de eficiência e produtividade, sendo estas características investigadas para cada produto, dispositivo, apresentado no capítulo três.

A fase seguinte teve em vista a compreensão das experiências vividas pelas vítimas de abuso facilitado pela tecnologia a cargo de um questionário. De acordo com Bell (1997), uma pesquisa quantitativa é utilizada quando o foco é obter informações que possam ser analisadas, extrair modelos de análise e fazer comparações. Por essa razão, o apuramento dos dados primários advém das técnicas de recolha de dados apurados através de um inquérito. A pesquisa descritiva teve a finalidade de demonstrar a delimitação do âmbito, universo e método de recolha de dados. A caracterização da amostra descreve as condições de realização e o seu procedimento ao apresentar e justificar variáveis, esclarecer sobre as técnicas e instrumentos de observação e, por último, referir os procedimentos utilizados nos instrumentos de recolha de dados.

Nesta fase, após selecionado o campo da amostragem para realização do questionário, a amostra selecionada foi do tipo não probabilístico e foi definida por acessibilidade. Não foi utilizado, portanto, nenhum procedimento estatístico, mas cuidadosamente verificada a sua representatividade, em parceria com várias associações portuguesas de apoio a vítimas, nomeadamente a APAV e a Cruz Vermelha Portuguesa. A princípio, o questionário foi respondido apenas por inquiridos residentes em Portugal, mas a provável dispersão na sua partilha, pode justificar a existência de respostas de não residentes em Portugal, potencializando uma comparação na recolha e diagnóstico dos dados.

A seguinte etapa tratou-se do ordenamento e análise de toda a informação recolhida, interligando os conceitos abordados anteriormente com os dados recolhidos, através das técnicas utilizadas. A integridade e objetividade ao identificar resultados válidos e precisos, foram suportadas por evidências constatadas. Isto leva a abordar o design especulativo para estruturação e fundamento na criação de possíveis cenários de abuso tecnológico no capítulo 5. Com base ainda, nas respostas dos questionários, e a possível solução de cada um.

1.9 Estruturação e Desenvolvimento da Investigação

Numa primeira fase, o capítulo 1 apresenta a introdução e a identificação da problemática, bem como a exposição da questão de investigação. Segue-se a revisão de literatura e *benchmarking*, dividida em dois capítulos, nomeadamente o 2 e 3, respetivamente.

Com um quadro teórico dos temas e trabalhos existentes relevantes para a investigação realizada, os critérios de seleção no desenvolvimento do estudo são: artigos, dissertações, livros e organizações que (1) incidiram o seu tema sobre violência facilitada pela tecnologia, (2) examinaram a violência em relações românticas atuais ou anteriores, (3) examinaram a violência que foi diretamente experimentada, (4) priorizando publicações feitas em 2019 ou após, podendo ainda assim existir algumas pesquisas de anos anteriores. Estes critérios foram selecionados com o fim de contextualizar o nível de conhecimento atual verificado nas áreas de interesse inerentes a este estudo, desde a violência de género, o impacto da tecnologia na violência doméstica.

O capítulo 3, trata-se de um levantamento com dados secundários de análise de mercado, composta pelas principais teorias relacionadas com produtos inteligentes e digitais que existem atualmente no mercado, através do *selection criteria*. Este dividiu-se em duas partes. A primeira aborda os produtos a nível geral, descrevendo individualmente a função de cada selecionado, assim como a avaliação dos consumidores. A segunda tem apenas enfoque naqueles que se destinam a rastrear a localização. É importante ressaltar que o foco da dissertação é a violência doméstica facilitada pela tecnologia, e não *hackers* em geral.

O capítulo 4, explica o método de análise escolhido: método de inquérito por questionário descrevendo todo o processo, desde a recolha dos dados mais focados em Portugal até ao tratamento dos mesmos.

O capítulo 5, por sua vez, é o resultado para o qual a investigação seguiu, tanto pelo nível de respostas alcançadas no questionário, como também resultante da pesquisa de design especulativo. Foi revelada assim a importância de incluir uma outra análise, desta vez, de

cenários relativos ao problema do abuso facilitado pela tecnologia, incluindo uma breve proposta de solução.

Por fim, o capítulo 6 demonstra como a violência doméstica facilitada pela tecnologia é uma questão abrangente e essencial. Este capítulo resumiu os resultados obtidos com uma análise geral ao abordado, incluindo algumas recomendações, uma discussão das limitações do estudo e apresentando propostas para pesquisas futuras.

CAPÍTULO 2 | Enquadramento Teórico

2.1 Introdução

Na atualidade, vivemos imersos em uma era digital, somos forçados a estar atualizados pelos avanços tecnológicos apresentados todos os dias em todo o mundo, originando assim uma mudança crescente na forma como nos relacionamos com os outros, com a cidade, com a casa e com os objetos. Estas relações têm-se alterado progressivamente diante de uma sociedade que cada vez mais procura respostas imediatas aos seus interesses.

Neste contexto, o foco da corrente análise detém-se sobre a atual era da tecnologia e pretendeu recolher informação de como esta evidencia novas formas de violência. Começando por analisar o seu conceito, os diferentes tipos de crime, formas de violência e a sua evolução. Entender de que forma pode afetar o sexo masculino e feminino, em que idades é mais frequente. Sobre uma análise de dados a nível local, nacional e internacional, por meio da realização de uma breve revisão literária sobre conceitos essenciais à pesquisa, de forma a perceber conforme o enfoque, como é possível prever comportamentos e mudar mentalidades. No mesmo capítulo, enquadra-se o balanço legal que atualmente limita o crime de violência doméstica, o seu ciclo e algumas das Instituições que lidam com este crime, de que formas estas agem dependendo das situações, percebendo ainda o impacto que a pandemia causou no aumento significativo de casos diários.

2.2 Design contra o Crime

Os espaços urbanos são os lugares onde historicamente o crime começou a ser abordado como um fenómeno (Mair & Mair, 2003), consequência da aglomeração humana que consequentemente impulsionou a sensação de insegurança nesses espaços (Jacobs & Lees 2013). Certamente, o cruzamento de dados históricos, com teorias como Newman (1972) provenientes de um passado de design, foram um contributo para a teoria e prática criminológica. O foco do corpo de investigadores que se resinificou há 50 anos, alterou a forma de execução deixando de ser a qualidade das coisas, passando a priorizar a abordagem das soluções aos problemas (Björklund, 2013). Um papel importante dos designers, é que estes usam os seus conhecimentos para entender as necessidades dos utilizadores e as tecnologias disponíveis para desenvolver melhorias, novos produtos, sistemas ou serviços que satisfaçam as conveniências e desejos dos consumidores (Press & Cooper, 2003).

Segundo os autores Rittel and Webber (1973) e Getzels (1975), a informação necessária para perceber o problema e a forma como este é entendido influencia a ideia de quem o decidiu resolver e quais soluções são consideradas relevantes. Portanto, encontrar uma solução significativa para o problema requer uma análise correta e inclusiva (Getzels, 1975). Considerando que os problemas podem ter vários pontos de vista, quantos investigadores envolvidos, parte a importância dos designers interpretarem primeiramente os dados recebidos ou coletados em relação a um projeto de design, a fim de criar uma primeira representação do problema em questão (Visser, 2006). O design tem então um papel de influência importante em suscitar a mudança de comportamento da sociedade, de tal forma que a abordagem “design contra o crime” utiliza na sua íntegra o design como processo de modificação da percepção do benefício do crime, atuando no desenvolvimento de produtos, serviços e ambientes como forma de proteção (Press & Cooper, 2003; Ekblom, 2011; Jacobs & Lees 2013). Portanto, o papel dos designers parece pertencer ao grupo de profissionais que estão melhor preparados para lidar com questões de crime. Onde também Pease (2001) acredita, que os designers são treinados para antecipar várias questões: tendo como foco as necessidades e os desejos dos utilizadores, tais como, os impactos ambientais, aspectos ergonômicos, entre outros.

Colocar designers na criação e desenvolvimento de produtos pode viabilizar ainda formas de antecipar consequências criminais dos produtos e serviços, facilitando o design contra o crime (Pereira, 2015). Ao funcionar como uma ferramenta para prevenção do crime, inicialmente necessita estudar os recursos potenciais dos produtos que potenciam a criminalidade, transformando-os em um ato menos chamativo para o perpetrador e assim quebrar o ciclo com uma possibilidade de variação de mecanismos diferentes para cada contexto, podendo ser reajustados durante a execução de cada projeto (Ekblom & Tilley, 2000).

Por outro lado, o design enquanto disciplina deve acompanhar também a emergência da tecnologia, mas não só a nível de produtos, também a nível digital e de serviços, como por exemplo, o design das redes sociais, que todos os dias alcança um elevado número de utilizadores e que contém campos que incentivam o compartilhamento de uma grande quantidade de informações pessoais. No entanto, não existem provas que garantam a total privacidade da identidade dos utilizadores, ou mesmo a estabilidade das informações divulgadas (Pereira, 2015). Como a partilha de informações pessoais (nome, morada ou fotografias) são um dos fatores de risco consequentes do rápido desenvolvimento de tecnologias, requer-se esforços para estabelecer mais investigações nesse campo a fim dos resultados poderem aumentar o sucesso das investigações e desencorajar a prática de crimes.

2.3 Violência

Segundo Braga et al, (2008), a palavra “violência” origina-se do latim e tem dois significados: violência, que significa veemência, ato apaixonado e sem controle, e infração ou violação. A violência é qualquer ato, omissão ou conduta que serve para infligir sofrimentos físicos, sexuais ou mentais, direta ou indiretamente num relacionamento, por uma das partes, sobretudo para controlar a outra. As pessoas envolvidas podem ser casadas ou não, ser do mesmo sexo ou não, viver juntas, separadas ou namorar. As vítimas podem ser ricas ou pobres, de qualquer idade, sexo, religião, cultura, grupo étnico, orientação sexual, formação ou estado civil, segundo APAV (2019).

“A palavra violência pode ter entendimentos diferentes, dependendo do que as pessoas consideram violência, mas tem uma definição e muitas leis relacionadas com a mesma. A violência é definida pela Organização Mundial de Saúde como "o uso intencional de força ou poder físico, ameaçado ou real, contra si próprio, outra pessoa, ou contra um grupo ou comunidade, que resulta ou tem uma elevada probabilidade de resultar em ferimentos, morte, danos psicológicos, mal desenvolvimento, ou privação".
(Who, 2020)

A definição desta palavra ainda tem algumas questões de interpretação por parte da sociedade, uma vez que nem sempre é fácil identificar um ato de violência, mas esta definição é a mais próxima da completa. As circunstâncias podem ser diferentes, mas um ato com estas características é considerado violência. No relatório mundial sobre violência e saúde da OMS (2020), é também apresentada em quatro tipologias diferentes, que distinguem as formas como a violência pode ser infligida.

Por conseguinte, a violência pode ser física; sexual; um ataque psicológico; e a privação. Está também dividida em três subtipos de violência relacionados com a relação entre a vítima e o perpetrador. Estes subtipos de violência são: "A violência autodirigida refere-se à violência em que o perpetrador e a vítima são o mesmo indivíduo e é subdividida em auto-abuso e suicídio"; "A violência interpessoal refere-se à violência entre indivíduos, e é subdividida em violência familiar e do parceiro íntimo e violência comunitária"; "A violência coletiva refere-se à violência cometida por grupos maiores de indivíduos e pode ser subdividida em violência social, política e económica" (Quem, 2020). Diferentes tipos de violência são apresentados nestes subtipos de violência e a violência doméstica faz parte do grupo de violência interpessoal, uma vez que se trata de um ato de violência entre indivíduos, mais especificamente, parceiros íntimos e família.

2.3.1 Violência Doméstica

Sabendo que violência é o resultado de um ato violento, impetuoso praticado por um indivíduo contra outro, impondo-lhe uma forma de conduta contrária à que ele pretende. A violência doméstica (VD) é também definida assim, mas com a diversidade de ser praticada dentro do mesmo espaço familiar. Não se pode dizer que é um fenómeno recente nem passageiro, mas segue sendo neutralizado na sociedade atual, pelo que, para além das Forças de Segurança, toda a sociedade deve estar envolvida na prevenção e combate deste crime.

Segundo ONU (2022), a violência doméstica é uma consequência que advém da necessidade e busca por poder que uma pessoa utiliza para ganhar ou manter controle sobre um parceiro íntimo. É uma ação física, sexual, emocional, econômica ou psicológica ou uma ameaça de ações que influenciam outra pessoa, incluindo qualquer comportamento que assuste, intimide, aterrorize, manipule, magoe, humilhe, culpe, magoe, ou ferir alguém. Por sua vez, o abuso doméstico pode acontecer a qualquer pessoa de qualquer raça, idade, orientação sexual, religião ou sexo. Pode afetar pessoas de todas as origens socioeconômicas e de todos os níveis de educação. A violência, ocorre dentro de uma série de relações, incluindo casais que são casados, que vivem juntos ou apenas que namoram. Por esta definição, é de realçar que a violência doméstica ou abuso, muitas vezes não são visíveis, e podem acontecer ou estar a acontecer com qualquer pessoa e em qualquer lugar.

De acordo com Dutton (2006), a violência doméstica não existe apenas entre casais ou ex casais, também é considerada violência doméstica quando envolve crianças ou pessoas idosas. Dutton (2006) afirma ainda que, este tipo de violência não se baseia apenas na agressão física, como as pessoas tendem a pensar. A agressão física é frequentemente acompanhada por abuso verbal, abuso psicológico e ameaças ou ações de destruição contra crianças, animais de estimação, e bens pessoais. Essa via de entendimento, sugere a ideia padrão da sociedade de que as pessoas tendem a associar a violência a algo físico, e muitas vezes situações de violência são desvalorizadas por não existirem agressões físicas (ONU, 2022). Na realidade, a violência pode ter muitas formas e estas não são fáceis de identificar. É importante haver mais debates, esses temas serem abordados sem tabus ou qualquer pejoração, porque conhecimento e informação é uma arma poderosa, para lidar com situações como estas. Quanto mais falado este tema for, mais as vítimas se conseguem aperceber e agir.

Uma das grandes lutas travadas desde o último século por grupos feministas, foi essa mesma, trazer o privado para público, segredos confinados do espaço doméstico ou na

conjugalidade, situações muitas vezes ocultas pelo agressor ou pela própria vítima, denotam crimes cuja amplitude é difícil de verificar na íntegra.

De acordo com o Domestic Violence Resource Center (2020), existem muitas formas de violência doméstica, incluindo a violência emocional, verbal e física, em que todos os tipos de violência funcionam como um sistema circular, podendo diferenciar alguns aspectos de acordo com o tipo de violência, sendo o ciclo sempre o mesmo. Regra geral dividido em três etapas segundo a APAV (2012) como demonstra a Figura 2, “o ciclo caracteriza-se pela sua continuidade no tempo, isto é, pela sua repetição sucessiva ao longo de meses ou anos” (APAV, 2012). Geralmente, existe um padrão de interação, quando termina onde antes começou podendo em situações de maior gravidade, quando a etapa 2 (ato de violência) passa a acontecer regularmente, o risco de resultar em homicídio torna-se elevado.

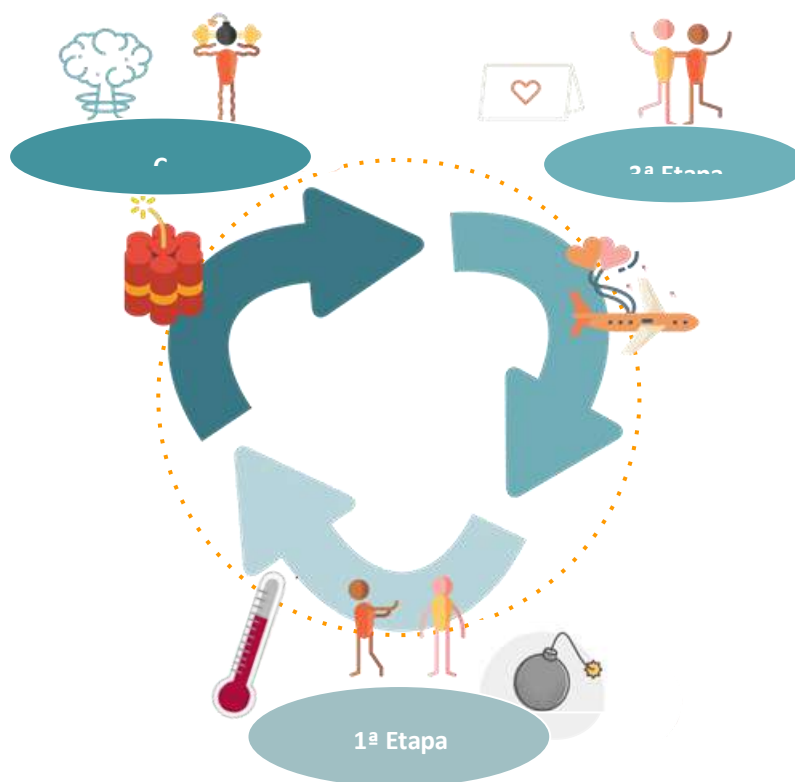


Figura 2: Ciclo da violência doméstica.

1ª Etapa Crescimento de Tensão: Nesta fase, os indivíduos sentem-se frequentemente como se estivessem "a caminhar sobre cascas de ovos" ou "à espera que o outro sapato caia". O parceiro pode estar nervoso, mal-humorado, facilmente irritado, ou imprevisível. Há uma sensação definitiva de ansiedade no ar.

2ª Etapa Aguda ou Abusiva: Esta é a fase mais violenta do ciclo, onde ocorrem abusos concentrados, intensos, emocionais e verbais, ou abusos físicos. Esta fase é a explosão da tensão da fase 1.

3ª Etapa Lua-de-mel: O parceiro pode pedir desculpa e prometer nunca mais magoar; ou pode culpar a vítima pela sua violência. Pode-se experimentar muitos sentimentos durante esta fase, tudo desde o amor à confusão. O mais importante a lembrar, porém, é que se não existir mudanças, o ciclo continuará.

Existem vários estudos e teorias sobre quais são as causas da violência para alguém ser violento com outro, especialmente com os seus íntimos. Um destes estudos é o de Margi Laird McCue's, defendendo que os homens são violentos com os seus íntimos porque "sentem ciúmes, possessividade e a necessidade de controle nas relações". (McCue, 2008) De facto, esta é uma das causas e não só gera abuso físico, mas também abuso psicológico, social e financeiro. McCue acrescenta que os agressores podem tomar controle das finanças, monitorizar a quilometragem do carro, as chamadas telefónicas, e sono, tudo devido ao seu extremo ciúme e à sua necessidade de controlo (McCue, 2008). Outros estudos, introduzem também a ideia de que o que causa violência doméstica é o ciclo de exposição à violência doméstica. "Um forte preditor da violência doméstica na idade adulta é a violência doméstica no lar em que a pessoa foi criada" (Benedictis et al, 2006). Este ciclo de violência doméstica, acontece porque as crianças aprendem que a violência pode ser usada na relação, e à medida que crescem, esta ideia permanece com elas. É aqui, que as soluções educacionais são importantes para prevenir a violência doméstica, além de desenvolverem formas de saber se as crianças são expostas à violência em casa.

Muitas causas podem ser consideradas como válidas para a prática da violência doméstica, mas é um problema quando indivíduos, pensam que só as pessoas com "perturbações ou problemas" podem agir violentamente com a sua intimidade. "Talvez a resposta mais comum que as pessoas dão é que os homens batem, matam, ou agredem sexualmente as mulheres intimidadas devem estar doentes ou mentalmente perturbadas" (Shoham, et al, 2010, p.571). Esta citação, parece ser uma crença muito comum entre as pessoas, mas como se viu anteriormente, a violência doméstica pode acontecer em qualquer lugar, por qualquer pessoa, por vezes de quem menos se espera.

Nesta seção, foram também apresentadas as primeiras estatísticas relacionadas com o género, cidade, idade e escolaridade, do perfil de vítimas e agressores, com base em duas referências que recolhem dados especificamente para a população portuguesa, a APAV e INE.

Quando comparados os dados, percebe-se que existe um aumento nos casos de violência registrados desde o ano 2016 até 2021, baseados no relatório anual da APAV, indicam um aumento de mais de 110% em atendimentos desde 2016, em que tinha um total de 35 411 atendimentos. Já em 2021, passou para um total de 75 mil 445 atendimentos, comparação com antes da pandemia em 2019 tinha um total de 54 403 atendimentos, o que sugere um aumento de 21 042 em apenas dois anos. Percebe-se então, que este aumento significativo ao longo dos anos, nunca foi inferior ao ano anterior, isso demonstra que tendencialmente os casos sobem de ano para ano e que a pandemia teve um grande papel nessa evolução. Além disso, os casos de abuso tecnológico são os que são menos notificados, pela sua natureza difícil de comprovar, fazendo com que os números apontados sejam muito maiores na realidade. Vale ressaltar também que em 2020, os dados relativos à pandemia, subiram significativamente. Foi um ano excepcional, devido à pandemia de Covid 19 e o isolamento social, o que pode ter levado a um aumento de casos de abuso tecnológico também.

Segundo a análise da APAV (2021), a média de vítimas por dia somou um total de 37 no ano de 2021, referente a, 25 mulheres, 5 homens, 5 crianças e 4 idosos, comprovando assim que os números são assustadores, como demonstrado na tabela 2, o perfil geral das vítimas. O problema não é existir a pandemia, mas sim, se a violência ganhou forma na pandemia, por todas as razões, de *stress* e isolamento forçado, então está longe de acabar.

Tabela 2: Perfil geral das vítimas (Fonte: Apav, 2021)

Perfil	Sexo	Nº de casos	Média de Idades	Relação com autor/a do crime
Geral da Vítima	Feminino (78%)	13 234	40 anos	15,5% cônjuge 8,5% companheiro/a 7,8% pai/mãe 7,5% ex-companheiro/a 6,4% filho
Crianças e jovens	Feminino (59%)	1 959	11 anos	26,3% filho
Vítima masculina	Masculino: Adulto (56,7%); Crianças e jovens (29,7%); Pessoa idosa (13,6%)	2 601	36 anos	13,7% pai/mãe 9,1% cônjuge 6,5% filho 4,7% companheiro/a 4,7% ex-companheiro/a
Pessoa Idosa	Feminino (70%)	1 594	76 anos	26,2% pai/mãe 16,5% cônjuge

Os dados revelam que é urgente tratar de combater a violência contra a mulher, sob essa conjuntura, percebe-se que as organizações não governamentais (ONG) e associações, prestam um trabalho essencial, pois é possível perceber pela Tabela 3, o tipo de contacto que mais se destacou (n=9.588) foi telefónico, seguido por (n=3.011) email/online e por último com menos destaque mas com um grande mérito (n=2.367) foi presencial nos gabinetes de apoio à vítima (APAV, 2021).

Tabela 3: Tipo de contacto efetuado para a APAV (Fonte: APAV, 2021)

Tipo de contacto efetuado para a APAV	Nº	%
Telefónico	9 588	61,8
Presencial	2 367	15,3
Email	3 011	19,4
Apoio Online (via zoom, redes sociais)	377	2,4
Outros (carta, notificação google forms)	167	1,1
Total	15 510	100

No que diz respeito às formas de como estas queixas chegam até à APAV, é possível perceber que maioritariamente estas acontecem por iniciativa própria (n=7,873). Seguida pelos Órgãos de Polícia Criminal que apresentaram 1.062 reportagens significando 7,8% do total

(APAV, 2021), uma esmagada maioria, são sexo feminino. No ano de 2021, de um total de 13.234 vítimas, segundo a APAV (2021), registou-se 13.413 autores/as de crime, além de se observar que existem mais abusadores do que vítimas, percebe-se também pelo gráfico 2 que o sexo masculino (n=8.167; 60,9%) mantém-se como tendência de anos anteriores, que os homens são os principais agressores (APAV, 2021). É importante destacar, o fato de que cada vez mais as vítimas tomam iniciativa própria, o que sugere que mesmo ao existir ameaças e manipulações, também existe consciência por parte das vítimas para entenderem que não está certo, e vontade de atuar e procurar ajuda.

Neste contexto específico, segundo a APAV (2021), e embora estudos mostrem que a violência doméstica existe em qualquer idade, é possível verificar que há faixas etárias onde é mais usual acontecer, (Tabela 4) fundamentalmente entre os 25 e os 54 anos (n=5.341). O que pode sugerir também que existem mais dados estatísticos para estas idades, logo, mais queixas porque trata-se das idades em que existe maior independência. Antes dos 25 anos, é possível depender-se mais de familiares, daí a falta de percepção do grau de criminalidade que estas vítimas vivem. Já a partir dos 55 anos, existe o chamado comodismo ou aceitação, em que a vítima pensa, que como já aguentou até ali, que não faz sentido mudar, podendo ter haver vários fatores como, a quantidade de anos juntos ou mesmo o facto do agressor se desculpar.

Tabela 4: Idade da vítima. (Fonte: Apav, 2021)

Idade da Vítima	Nº	%
0-3 anos	229	1,7
4-5 anos	142	1,1
6-10 anos	490	3,7
11-17 anos	1.098	8,3
18-24 anos	1.034	7,8
25-34 anos	1.586	12
35-44 anos	2.028	15,3
45-54 anos	1.727	13,1
55-64 anos	1.087	8,2
65 -74 anos	792	6
75-84 anos	547	4,1
85 ou + anos	255	1,9
ns/nr	2.219	16,8
Total	13.234	100

A nível de escolaridade, o número de vítimas que procuraram ajuda em 2021 foi mais ou menos uniforme. No entanto, foi possível perceber que existiu maior influência, destacando o ensino superior com a maior percentagem (n=898), seguindo-se pelo ensino secundário (n=763) e ensino básico- 3º ciclo (n= 715). “Desta forma, mantém-se a tendência crescente dos níveis de escolaridade das vítimas que procuram auxílio na APAV face aos anos anteriores.” (APAV, 2021).

Considerando todos os municípios de Portugal que a APAV registou de vítimas, existiram seis, que se destacaram com uma margem de casos gigantesca em relação com os demais. Analisando anos anteriores, observou-se um geral crescimento, contudo e equiparando com o ano de 2019, Lisboa capital de Portugal, localidade com maior densidade populacional que em 2019 segundo o Instituto Nacional de estatística (INE) tinha um total de 2.863.272 habitantes e o correspondente a 305 (2,61%) casos de violência (INE, 2020). No ano de 2021 Lisboa com um total de 2.871.133 habitantes, e 820 (6,2%) números de violência, desta forma, em comparação com ambos os anos a pequena subida de habitantes não se justifica para a subida das denúncias. Deveu-se sim, grande parte à pandemia e a toda a situação, por essa razão foi necessária a criação da Tabela 5, com a comparação do ano 2019 e 2021. Segundo APAV (2021), é de extrema relevância destacar, que o concelho de Braga, apesar de ser um concelho com menor densidade populacional que Lisboa, em 2019, este era o concelho com maior número de casos de violência doméstica. Contudo em 2021, passou para segundo, mas sempre com grandes números, e têm vindo sempre a aumentar ao longo dos anos, o que torna o concelho uma zona preocupante.

Tabela 5: Comparação do número de vítimas entre concelhos (Fonte: APAV, 2019; APAV, 2021)

2019 Concelho	Nº	%	2021 Concelho	Nº	%
Braga	463	3,97	Braga	546	4,1
Faro	212	1,82	Faro	465	3,5
Lisboa	305	2,61	Lisboa	820	6,2
Loulé	247	2,12	Loulé	418	3,2
Porto	379	3,25	Porto	405	3,1
Sintra	316	2,71	Sintra	429	3,2
Total	1.922 (11.676)	16,48 (100)	Total	3.083 (13.234)	23,3 (100)

Segundo a APAV (2021), do total de 13.413 autores/as de crime registados pela APAV em 2021, observa-se que a faixa etária dos agressores maioritariamente ronda os 25 e os 54 anos (n=3,182; 23,7%), (Tabela 6) muito semelhante a anos anteriores, já que em 2019 estas faixas etárias representavam 24,5% (n=2.886) dos casos e em 2020 28,3% (n=3.712).

É necessário abordar o facto que os menores (crianças/adolescentes até aos 18 anos) situam-se com 138 casos (1%), que relativo a anos anteriores sofreu uma pequena diminuição de casos já que em 2019 registou-se 155 casos (1,4%) e no ano de 2020, 150 casos (1,2%).

Tabela 6: Idade do/a autor/a do crime. (Fonte: Apav, 2021)

Idade do/a autor/a do crime	Nº	%
0-3 anos	---	---
4-5 anos	9	0,1
6-10 anos	5	0,03
11-17 anos	124	0,9
18-24 anos	392	2,9
25-34 anos	838	6,2
35-44 anos	1.215	9,1
45-54 anos	1.129	8,4
55-64 anos	679	5,1
65 -74 anos	352	2,6
75-84 anos	174	1,3
85 ou + anos	35	0,3
ns/nr	8.461	63,1
Total	13.413	100

A nível de escolaridade, o número de casos válidos no ano de 2021 de autores/as do crime foi apenas 1.719 dos 13.413 casos, desta forma não se consegue deter a informação na sua totalidade. No entanto, como demonstrado na Tabela 7, é possível perceber que existiu maior influência no ensino superior constatando a maior percentagem (n=406; 3%), seguindo-se pelo ensino básico- 3º ciclo com 2,9% (n=387) e no ensino secundário (n=384; 2,9%), (APAV, 2021).

Tabela 7: Escolaridade do/a autor/a do crime. (APAV, 2021)

Escolaridade do/a autor/a do crime	Nº	%
Nenhuma – não sabe ler/escrever	29	0,2
Nenhuma – sabe ler/escrever	20	0,1
Pré-escolar	8	0,1
Ensino básico - 1º ciclo	223	1,7
Ensino básico - 2º ciclo	208	1,6
Ensino básico - 3º ciclo	387	2,9
Ensino secundário	384	2,9
Pós-secundário	46	0,3
Ensino superior	406	3
Outro	8	0,1
Ñs/ñr	11.694	87,1
Total	13.413	100

Relativamente à relação do/a autor/a do crime com a vítima, destacam-se as relações de intimidade pois pertencem à maioria dos casos, como é o caso da conjugalidade (n=2.072; 15,5%), da relação entre companheiros (n=1.142; 8,5%), de ex-cônjuges (n=423; 3,2%), relações entre ex-companheiros/as (n=1.002; 7,5%), de ex-namorados/as (n=465; 3,5%) e de namorados/as (n=224; 1,7%). Ainda segundo APAV (2021), cerca de 40% das relações estabelecidas entre autor/a do crime e vítima, faziam parte deste tipo de relações de intimidade. Já em relações familiares, mostra exemplos em casos que a vítima é filho/a do/a autor/a do crime (n=1.051; 7,8%), seguindo-se os 6,4% (n=859) em que a vítima é pai/mãe do autor/a.

Segundo a APAV (2021), o tipo de vitimação em 13.234 vítimas que procuraram ajuda na APAV, 50% (n=6.644) foram alvo de vitimação continuada, com duração entre 2 e 3 anos (n=1.097;16,5%).

Cabe igualmente referir, que relativamente ao local do crime, representado na tabela 9, o mais mencionado com 49,4% dos casos (6.305) foi a residência comum, seguido pela residência da vítima (n=2.028; 15,9%) e do lugar/via pública (n=1.215; 9,5%), permanecendo a tendência dos anos anteriores como os locais mais referenciados pelas vítimas que procuram apoio da Instituição.

É de extrema relevância destacar que em 2021, locais como a internet e/ou telefone (n=847;6,6%) foram locais com grande número de casos, em que nestes não se referem a violência física, mas sim emocional, psicológica e muitas vezes *stalking*. Demonstrando assim,

que a tecnologia ao estar cada vez mais presente no cotidiano, os/as abusadores/as arranjam formas de manipular, manusear e controlar as vítimas, incluindo a utilização de vários tipos de violência.

2.3.2 Tipos de Violência

De acordo com o site oficial da Organização das Nações Unidas (UN, 2020), e outros dados da investigação (Benedictis et al. 2006), existem seis tipos de violência doméstica/abuso:

1. Violência financeira/econômica

Este tipo de violência não exige força física, mas sim manipulação com o intuito de apropriação ilícita do patrimônio de uma pessoa, o que acontece na maioria dos casos em pessoas com pessoas idosas, muitas vezes pelos seus familiares, profissionais e instituições (APAV, 2014). Dependendo dos casos, muitas dessas práticas são baseadas em:

- Forçar a pessoa a assinar um documento, sem lhe explicar para que fim se destina;
- Forçar a pessoa idosa a celebrar um contrato ou a alterar o seu testamento;
- Forçar a pessoa idosa a fazer uma procuração ou ultrapassar os poderes de mandato;
- Tomar decisões sobre o patrimônio de uma pessoa sem a sua autorização;
- Levantamentos significativos da conta da pessoa idosa;
- Mudanças suspeitas de beneficiários de testamentos, seguros ou de bens;
- Forçar a pessoa idosa a fazer uma doação, nomeadamente para reserva de vaga ou entrada em equipamento (APAV, 2014).

Estas ações são consequentes da ideia de que o matrimônio da pessoa idosa é da família e, a partir de certa idade, é cada vez mais comum existir um atropelamento da lei por essas pessoas que fazem de tudo para administrar os bens da pessoa idosa (APAV, 2014). Já segundo UN (2020), não necessariamente tem que existir uma faixa etária para as vítimas, mas sim a dependência da vítima ao agressor, envolvendo tornar ou tentar tornar uma pessoa financeiramente dependente, para o domínio total da vítima facilmente conseguido sobre os seus recursos financeiros e assim assumir o controle e negar o acesso ao dinheiro e/ou proibir.

2. Violência psicológica

Também conhecida por violência verbal, este tipo de abuso resulta da intenção que uma pessoa tem em provocar dor ou angústia, muitas vezes através de ameaças, humilhações ou intimidação de forma verbal ou não verbal, que resulta em insultos, intimidação, isolamento social mas também proibição de atividades. Ao que a UN (2020) aborda como violência psicológica a APAV (2012) chama de violência social, este tipo de abuso é o segundo mais comum, alguns dos comportamentos retratados colocam as vítimas em situação de submissão,

dos quais são naturalizados pela sociedade, como o micromachismo cultural. Para Bonino (2004), o micromachismo é um comportamento cotidiano e sutil, que na verdade estabelece uma estratégia de controle que ameaça a autonomia pessoal de uma ou mais mulheres. Contudo, este comportamento pode se tornar imperceptível e até mesmo justificado pela sociedade, em que o homem é visto muitas vezes como dominante, o "líder" nas relações. Assim, nota-se que há necessidade de tornar-se visível mais ações de violência se queremos elucidar e mudar comportamentos. Nestes casos, é possível haver sinais frequentes como a vítima encontrar-se emocionalmente perturbada, aparentar isolamento, insónias, medo de outras pessoas, depressão não habitual, revela uma inexplicável negação em participar em atividades normais e muitas vezes comuns (UN, 2020). Expondo o facto de que muitas mulheres se acostumam a viver sendo humilhadas, controladas e violentadas em seu psicológico, sofrendo ameaças a danos físicos pessoais ou sobre alguém bastante próximo, incluindo destruição de propriedade, podendo adicionar-se o mesmo a animais de estimação. O psicológico está muito ligado a “jogos mentais”, em que o abusador controla e muitas vezes força a vítima a isolar-se de tudo, impedindo até mesmo de ir escola e trabalho, ou que visite familiares ou amigos, muitas vezes também envolve o afastamento de redes sociais ou proibição de utilização de telefone (UN, 2020; APAV 2012).

3. Violência Emocional

Segundo a UN (2020), existe diferença entre violência psicológica e emocional. A violência emocional ocorre quando alguém tem um comportamento que “visa fazer o outro sentir com medo ou inútil” (APAV, 2012). Incluindo atormentar a autoestima da vítima por meio de críticas constantes ou menosprezar as habilidades, incluindo abusos verbais muitas vezes (UN, 2020). Segundo a UN (2020) existe uma lista de comportamentos comuns presentes quando um relacionamento é emocionalmente abusivo. Envolvendo o parceiro ter atitudes que põem em causa o emocional da vítima como:

- Chamar nomes, insultar ou criticar continuamente;
- Não confiar ou ter atitudes possessivas;
- Tentar isolar da família e dos amigos;
- Monitorizar a localização, as chamadas telefónicas e com quem está;
- Opor-se a que trabalhe;
- Controlar finanças ou se recusa a partilhar dinheiro;
- Punições negando dar afeto;
- Domina atitudes, espera que peça permissão;
- Ameaça fisicamente entes próximos ou animais de estimação;

- Humilha (UN, 2020)

4. Violência física

A violência física é o tipo de abuso mais frequente e reportado. A agenda de 2030 das Nações Unidas para os Objetivos de Desenvolvimento Sustentável (ODS) segundo Sardinha et al. (2022) exigem a sua eliminação na meta 5.2, apesar de existir este objetivo os governos não estão no caminho certo para cumprir as metas dos ODS para a eliminação da violência contra mulheres e meninas, apesar de fortes evidências de que a violência praticada pelo parceiro íntimo pode ser evitada. De acordo com Benedictis (2006), o uso de força física contra outra pessoa de forma intencional a ferir, ou colocar a pessoa em risco de ser ferida é considerado violência física. Esta ação pode ser traduzida em comportamentos como “esmurrar, pontapear, estrangular, queimar, induzir ou impedir” que a vítima obtenha medicação ou tratamentos (APAV, 2012). A agressão física é um crime, quer ocorra no meio familiar ou não, segundo Benedictis (2006) quando o assunto é violência doméstica é corrente associar-se logo ao abuso físico dentro relacionamento íntimo de duas pessoas, em que uma é agressiva com a outra. Estima-se que 38% a 50% dos assassinatos sejam cometidos por parceiros íntimos (Sardinha, 2022).

5. Violência Sexual

O crime de violência sexual é referente a qualquer comportamento em que um indivíduo força outro a atos sexuais que não deseja, reconhecido como problema de saúde pública e uma violação dos direitos humanos (Puri, 2012). Um estudo da UN (2020) acrescenta que este crime interfere forçar, tentar ou pressionar relações sexuais em que a outra pessoa não queira, podendo dizer respeito igualmente a relações desprotegidas ou mesmo “forçar o outro a ter relações com outras pessoas” UN (2020). A violência sexual recai maioritariamente sobre a mulher e é sempre uma demonstração extrema de poder e controle do abusador, que é predominantemente homem, sobre a vítima que se confira como uma forma de violência física e psicológica em simultâneo (Silva, 2022). Já as consequências de ser vítima de um crime sexual “são enormes, podendo ter sequelas durante anos ou para sempre”, devido ao facto da possibilidade ainda de gravidez indesejada e infeções sexualmente transmissíveis, causa danos a nível de bem-estar físico, sexual, reprodutivo, emocional, mental e social (Silva, 2022). Ademais, percebe-se que a exploração sexual foi um dos acontecimentos que culminou com a tecnologia, sendo utilizada como uma tática para humilhar a vítima em larga escala (Messing et al. 2020; Powell and Henry 2018).

6. Perseguição

O termo mais conhecido por “stalking” em inglês, as definições criminais de perseguição são baseadas conforme as leis locais e atuais, que variam conforme a sensação de medo das vítimas e da denúncia à polícia de que o perseguidor causará danos físicos (Storey and Hart, 2011; Cheyne & Guggisberg, 2018). Dada a evolução da tecnologia, algum grau de vigilância como a monitorização de um parceiro íntimo, pode ser considerado aceitável dentro da relação, o que torna o assédio e a perseguição mais difíceis de identificar e reconhecer como perigosos.

Segundo Bracewell, et al. (2020), perseguição envolve por vezes comunicação indesejada, assédio, comportamento intrusivo que a tecnologia ajudou a facilitar. Com o fácil acesso à localização próxima das vítimas, muitas vezes fornecida em redes sociais, tais como Facebook, Instagram, LinkedIn e Snapchat, ou apps de encontro (Kane, 2017). Além de fornecer ao abusador novas abordagens de controlar, humilhar, ameaçar e isolar as suas vítimas, oferece grandes oportunidades de comunicação. Estas plataformas existem principalmente para compartilhamento de informações sobre si mesmo, e se interessar por informações compartilhadas por outros. Isto gera uma motivação nos indivíduos de compartilhar informações do seu dia-a-dia sobre si mesmo e também buscar informações sobre outros impulsiona o uso destas redes sociais (Dhir et al., 2019).

Inevitavelmente o comportamento de perseguição não diminuiu com o resultado das restrições do COVID-19, nomeadamente o isolamento veio ajudar os abusadores a monitorarem mais facilmente o paradeiro (Bracewell, et al. 2020). Pesquisas anteriores à pandemia analisaram que, além das mulheres serem mais propensas do que os homens a sentir medo devido à perseguição, estimativas demonstram que uma em cada cinco mulheres e um em cada dez homens sofrem perseguição (desde os 16 anos) (Sheridan & Lyndon, 2010; ONS, 2021). Esse medo, das vítimas de não ser acreditado e o medo das consequências da denúncia advém da discrepância que este tema toma na realidade atual, que leva à não denuncia muitas vezes. O estudo dos tipos de violência doméstica ou abuso é importante para saber como preveni-la. Dividi-lo em categorias é mais fácil de se concentrar em aspetos específicos a desenvolver como objetivo de melhorar a prevenção do abuso doméstico.

O fato de a tecnologia se encontrar atrelada a todos no quotidiano, faz com que estejamos numa época na qual estarmos conectados à internet já não se trata de uma necessidade momentânea, e específica como procurar alguma informação online, mas sim uma necessidade contínua de estar online na rua, em casa, no trabalho, na escola. Isso impulsiona para mudanças comportamentais aceleradas, tudo passou a estar à distância de um aparelho

eletrônico com acesso à internet. Note-se que, mesmo com todas as aplicações criadas, todos os meios disponibilizados, com acesso digital, na maioria dos casos a vítima ainda necessitam de se deslocar até entidades competentes (Knoblauch, 2020).

2.3.3 Prevenção da Violência Doméstica

O estudo da violência doméstica, para compreender as causas e apoiar as vítimas da forma correta faz parte da viagem, mas outra parte também está a desenvolver formas de a prevenir no futuro, diminuindo os acontecimentos. Um documento especializado das Nações Unidas introduz o conceito de "Comunidades Mobilizadoras", que representa 6 fatores para prevenir a violência doméstica. Esses fatores são:

- **Prevenção:** A fim de afetar a mudança sustentável a longo prazo, as organizações precisam de adotar uma atitude pró-ativa em vez de uma atitude reativa;
- **Holística:** A prevenção da violência doméstica requer o empenho e o envolvimento de toda a comunidade;
- **Processo de Mudança Social:** Mudar as normas da comunidade é um processo, não um acontecimento único;
- **Exposição repetida a ideias:** Os membros da comunidade precisam de ser envolvidos com mensagens regulares e mutuamente reforçadas de uma variedade de fontes ao longo de um período de tempo sustentado;
- **Quadro dos Direitos Humanos:** Uma abordagem baseada nos direitos para prevenir a violência doméstica é o empoderamento das mulheres e a comunidade;
- **Propriedade da comunidade:** Projetos eficazes destinados a mudar crenças e práticas prejudiciais numa comunidade devem envolver e ser liderados por membros dessa comunidade (Michau et al, 2005).

Fazer trabalhar todos estes fatores em conjunto não é fácil, mas é o objetivo. É importante olhar para a prevenção a longo prazo, porque ela depende de todas as comunidades da humanidade. A existência de organizações, associações e produtos é uma boa evolução da prevenção da violência doméstica. É necessário que exista um enquadramento legal e todas as pessoas e comunidades trabalhem em conjunto para resolver problemas como a violência doméstica e outros.

2.4 Enquadramento Legal Atual em Portugal

A Violência Doméstica sofreu várias alterações significantes no que respeita ao regime jurídico-penal que a emoldura, sendo a presente lei mais completa no âmbito das consequências da prática da violência e ações adicionais à mesma.

Neste sentido, segundo o Decreto-Lei n.º 48/95, artigo 152.º (Artigo 152.º - Decreto-Lei n.º 48/95). São punidos por violência doméstica aqueles que “de modo reiterado ou não, infligir maus tratos físicos ou psíquicos, incluindo castigos corporais, privações da liberdade e ofensas sexuais” a todos os indivíduos destacados nas alíneas do artigo. Estas alíneas incluem o cônjuge e ex-cônjuge, namorados ou ex-namorados, filhos ou outro tipo de pessoa que seja ou esteja indefesa. De acordo com o presente artigo, a pena de prisão mínima para atos classificados como violência doméstica é de um a cinco anos. Podem também acrescer outras penas dependendo da situação em questão. A pena de prisão foi uma das partes da lei que se manteve ao longo dos anos e de todas as alterações do decreto-lei, porém, outras mudanças como o aumento de categorias de vítimas, visam melhorar o processo de identificação de violência deste tipo e a sua justiça.

Quanto à prevenção da violência doméstica e proteção e assistência às vítimas, a presente Lei n.º 112/2009 do Diário da República, 1.ª série — N.º 180 — 16 de setembro de 2009, apresenta todas as envolventes no processo, considerando-se:

“Vítima” é a pessoa singular que sofreu um dano, nomeadamente um atentado à sua integridade física ou psíquica, um dano emocional ou moral, ou uma perda material, diretamente causada por ação ou omissão, no âmbito do crime de violência doméstica;

“Técnico de apoio à vítima” é a pessoa devidamente habilitada que, no âmbito das suas funções, presta assistência direta às vítimas;

“Rede nacional de apoio às vítimas de violência doméstica” é o conjunto dos organismos vocacionados para o apoio às vítimas;

“Organizações de apoio à vítima” são as organizações da sociedade civil, não governamentais;

“Programa para autores de crimes no contexto da violência doméstica” é a intervenção junto dos autores de crimes no contexto da violência doméstica”.

Para garantir que este enquadramento legal atual, oriente na prevenção, proteção e assistência a estas vítimas, existem algumas associações dedicadas a esta causa.

2.5 Associações de Apoio às Vítimas em Portugal

Todos os países têm associações e organizações com vários objetivos e missões a nível nacional e as associações relacionadas com a igualdade de género e violência doméstica são cada vez mais comuns, para esta pesquisa foram analisadas quatro, a APAV, ILGA e CETA de Portugal e a UN Women internacional.

1. APAV- Associação Portuguesa de Apoio à Vítima

Em Portugal, uma das principais associações é a APAV, a Associação Portuguesa de Apoio à Vítima. "Uma instituição privada de solidariedade social, uma pessoa coletiva de utilidade pública, cujo objetivo estatutário é promover e contribuir para a informação, proteção e apoio dos cidadãos vítimas de delitos criminais." (APAV, 2023). A associação foi fundada em 25 de junho de 1990 e a sua principal missão é "apoiar as vítimas de crimes, as suas famílias e amigos, fornecendo-lhes serviços de qualidade gratuitos e confidenciais e contribuir para a melhoria das políticas públicas, sociais e privadas, centrada no estatuto da vítima" (APAV, 2023). O estatuto da vítima nem sempre tem sido o mesmo, mas tende a ser mais complexo e justo com o apoio de associações como esta. Como a violência doméstica é um crime, a APAV também fornece os seus serviços gratuitos às vítimas de violência doméstica.

A associação garante três tipos de apoio às vítimas: jurídico, social e psicológico (APAV, 2023). O "apoio é prestado por um conjunto de Técnicos de Apoio à Vítima, devidamente formados e preparados para poderem prestar um apoio de qualidade e que responda adequadamente às diferentes necessidades das vítimas de crime" (APAV, 2023). Uma vez que, todas as situações de violência doméstica e todas as vítimas são diferentes e requerem diferentes níveis de tratamento. Por conseguinte, é importante ter uma elevada qualidade de serviço e de entrega por parte dos técnicos associados.

2. ILGA

Fundada em Portugal 1995, segundo ILGA (2022) o nome significa Intervenção Lésbica, gay, bissexual, trans e intersexo. Trata-se de uma organização de âmbito nacional, com sede em Lisboa, a associação maior e mais antiga que luta pela igualdade e contra a discriminação das pessoas LGBT+ e das suas famílias em Portugal, tem como principal objetivo as ajudar na integração social através de um programa alargado de apoio no âmbito social que garante a melhoria e qualidade de vida, a partir de lutas contra a discriminação em função da orientação sexual, da expressão e identidade de género e das críticas sexuais, e além da promoção da cidadania, dos direitos humanos e da igualdade de género.

O serviço de apoio à vítima LGBTQ+ existe como resposta a pessoas lésbicas, gays, bissexuais, trans e intersexo. Segundo ILGA (2022), se encontrem em situação de: Vivências de discriminação e vitimização continuadas; Bullying no local de trabalho; Situações de violência doméstica, com risco aumentado de vitimação; Incapacidade de denunciar situações de vitimação e crimes de ódio ocorridos na comunidade, e nas instituições e serviços.

3. CETA

A *Clinic to End Tech Abuse* (CETA), tal como o nome indica, trabalha para acabar com o abuso tecnológico e melhorar a segurança tecnológica e a proteção para vítimas de violência por parceiro íntimo. Trata-se de um grupo de pesquisadores com o objetivo de desenvolver uma compreensão profunda do papel da tecnologia na violência por parceiro íntimo e criar ferramentas que ajudem sobreviventes e defensores a enfrentar os desafios tecnológicos da violência por parceiro íntimo (CETA, 2022). Esta organização que atua na cidade de Nova York, dedicada a ajudar sobreviventes de violência por parceiro íntimo nas ameaças complexas à sua segurança digital, em trabalhos anteriores estabeleceu protocolos de ajuda (Tseng et al. 2022). Ao atenderem a estas ameaças emergentes perceberam a necessidade da criação de sistemas flexíveis e plurais que possam atender às necessidades das vítimas a longo prazo. Têm como missão defender leis políticas que incluem melhorar a proteção contra o abuso de tecnologia e ainda publicar recursos para guiar outras pessoas que tenham a mesma visão de ajudar os sobreviventes.

Segundo CETA (2022), o status da emergente tecnologia tem capacitado os agressores e não os sobreviventes, e as ferramentas mais poderosas para eles são plataformas e-mail, redes sociais e outras que milhões de pessoas utilizam todos os dias. A invasão de contas pessoais de vítimas é o ato mais recorrente e poderoso dos agressores, ao terem acesso a informações privadas sobre a localização das vítimas e o que estão a fazer, podendo ainda muitas vezes instalarem “spyware” em dispositivos pessoais da vítima, como telemóvel e/ou computador, e desta forma conseguem observar todos os passos e recolher informações até de senhas (CETA, 2022).

Como a organização foi fundada por investigadores, a missão combina a pesquisa fundamental com o envolvimento da comunidade para garantir que a tecnologia capacita todos os que trabalham para acabar com o abuso tecnológico e os problemas relacionados, por meio de publicações académicas, onde fornecem recursos e outros documentos relacionados à defesa. Uma vasta lista de guias com instruções é facultada pela organização de forma gratuita, que conta com um explícito passo a passo de ações de proteção para Androids, Gmail e Google,

Icloud, redes sociais, e ainda uma lista de verificação de formas de como a vítima pode ainda estar conectada com o agressor *on-line* ou nos seus *smart devices* sem saber (CETA, 2022).

Estas ligações podem permitir aos abusadores continuar a obter informações sobre a vida da vítima, como também guias que apresentam informações sobre o "*Spyware*" ou "*stalkerware*" significa uma aplicação que foi concebida para permitir que uma pessoa possa obter informação sobre outra sem o seu conhecimento, com acesso total ao telemóvel consegue saber sempre a localização, ver fotografias, ou o que a vítima está a escrever ou a ver no seu telefone. Segundo CETA (2022), tipos de aplicações como Google Maps e Find My (para iPhone) não são aplicações de *spyware*, mas podem deixar que outra pessoa rastreie ou obtenha informações sobre a outra.

4. *UN Women*

Da mesma forma que as associações nacionais combatem a igualdade de género e a violência doméstica contra as mulheres, existem associações internacionais para combater estes problemas em maior escala. A *UN Women* é uma das associações que tenta combater temas como a violência doméstica, a par de muitas outras. De acordo com o seu site oficial, *UN Women* (2020) concentra-se em áreas prioritárias que são fundamentais para a igualdade de género e que podem desbloquear o progresso geral.

A organização afirma que, uma em cada três mulheres em todo o mundo sofre violência física ou sexual, principalmente por um parceiro íntimo. A violência contra mulheres e meninas é uma violação dos direitos humanos, e as consequências físicas, sexuais e mentais imediatas e de longo prazo podem ser devastadoras, incluindo a morte (UN Women, 2020). Com isso, é possível perceber que cada país e cultura têm abordagens diferentes à violência doméstica, e os dados relacionados com a violência doméstica podem variar de país para país, mas existem em todo o mundo. Para isso, é importante existir uma aliança entre países, e partilha de ideias para criar soluções para combater e prevenir a violência doméstica e ajudar as vítimas.

A *UN Women* introduz a seguinte solução para estes problemas: Ao existir parcerias com governos, ONU, organizações da sociedade civil, entre outras, passa a haver mais hipóteses de encontrar formas de prevenir a violência, centrando-se na educação precoce e relações respeitadas, por se presumir ser a prevenção mais rentável e a longo prazo de pôr fim à violência, segundo a *UN Women* (2020). Esta associação concentra-se, sobretudo, em ações e apoio a longo prazo para prevenir a violência doméstica. As soluções relacionadas com a educação podem realmente fazer a diferença na compreensão do que é a violência doméstica e como esta deve ser tratada.

Após a abordagem a estas instituições, reforçou-se que a influência da tecnologia na violência doméstica é um fenómeno pouco abordado ainda, contudo percebe-se cada vez mais a sua emergência.

2.6 Tecnologia e a Violência Doméstica

Os avanços tecnológicos trazem com eles coisas positivas em que permitem chegar a qualquer momento de qualquer lugar, por outro lado, isso suscita preocupações sobre o bem-estar pessoal e a isso agrega a violência por parceiro íntimo, a perseguição e o abuso baseado na tecnologia. Estes problemas estão cada vez mais interligados, à medida que a vigilância online se tornou facilmente alcançável (Messing, et al., 2020). Estatísticas mundiais relatam que todos os anos, mais de dois milhões de pessoas são vítimas de abuso incluindo psicológico, físico, sexual, financeiro, emocional, com controle e restrição. Segundo Snook et al. (2017), esses dados incluem mais de 100.000 pessoas em alto risco de homicídio e danos graves, dos quais indicam que 95.000 dessas pessoas são mulheres.

A tecnologia permitiu que os agressores domésticos "infringissem velhos danos de novas maneiras" (Yardley, 2020, p. 2). À medida que a acessibilidade, facilidade e o imediatismo das tecnologias digitais expandem a capacidade dos agressores de controlar além dos limites espaciais anteriores (Dragiewicz et al., 2018). As novas tecnologias conectam os dispositivos dos utilizadores com objetos do cotidiano, como as assistentes virtuais conectadas à internet (Alexa, Google home, Amazon echo, ou similares), relógios inteligentes (*Smartwatch*), fechaduras inteligentes, câmaras e muitos outros (Harris & Woodlock, 2022). Segundo Snook et al. (2019) estes impossibilitam as vítimas que sofrem de abusos reconhecer que estão a sofrer. Como resultado sofrem frequentemente de isolamento e afastam familiares e amigos, o que torna em muitos casos ainda mais complicado de perceber e comprovar.

A tecnologia por outro lado, segundo Snook et al. (2019), também garante poder ser a resposta ao problema pois permite resolvê-lo concedendo aos utilizadores a possibilidade de fazer ligações e garantir que têm a informação que necessitam para tomarem as suas próprias escolhas e reconstruir a sua independência.

É importante referir que, cada experiência de abuso doméstico de cada pessoa baseada em tecnologia é única, tal como a sua solução ao problema e o país onde a vive, possibilitando constatar que o desenvolvimento tecnológico é diferente em várias partes do mundo. No entanto, várias histórias podem assemelhar-se apelando aos pesquisadores e profissionais para analisarem o abuso não como um incidente isolado ou um comportamento, mas sim uma

combinação de comportamentos que demonstram um padrão e incluem ameaças implícitas ou explícitas de violência, segundo Dragiewicz et al. (2018).

Os tipos de abuso abordados relativos à tecnologia incluem, além de assédio nas redes sociais, rastrear utilizando tecnologias GPS, gravação de áudio e visual, comunicações ameaçadoras ou ofensivas por meio digital, monitorização, acesso a contas sem permissão, personificação de parceiros, publicação de identificação e informações privadas online (Dragiewicz et al. 2018). Os abusadores utilizam várias ferramentas, incluindo dispositivos físicos (rastreadores GPS, telemóveis, entre outros), contas virtuais, software e plataformas online (Harry, 2020). Vários investigadores indicaram nas suas pesquisas mais recentes, a manipulação de tecnologias pelos abusadores para facilitar o controle coercitivo. Este controle, consta com padrões de opressão e “danos à liberdade”, que impedem as vítimas de violência doméstica e em relacionamentos atuais ou anteriores de exercer a liberdade ou a personalidade independente (Stark, 2009, Dragiewicz et al., 2018; Harris, 2020; Woodlock, 2017; Yardley, 2020, Flynn, 2021). Termos conhecidos como “controle coercitivo digital” (Harris & Woodlock, 2022) ou “controle coercitivo facilitado pela tecnologia” (Dragiewicz et al., 2018, 2019) identificam e analisam o uso de comunicações, monitorização e tecnologias de vigilância pelos agressores para permitir ainda mais esse controle coercitivo.

Lenhart et al. (2016) dividiu o tipo de perpetuação de violência em três categorias dentro da vitimização (1) assédio direto; (2) invasão de privacidade e (3) acesso negado.

1. Assédio direto refere-se às atitudes tomadas de umas pessoas para as outras, incluindo exemplos: ser chamado nomes ofensivos, ser ameaçado fisicamente, e ser perseguido (Lenhart et al., 2016).
2. A invasão de privacidade ocorre da obtenção de acesso não autorizado, exposição ou divulgação de informação fora do controle do proprietário através do qual causa danos às vítimas, incluindo experiências como ser pirateado, ter informações ou imagens da pessoa exposta online sem a sua permissão, ser imitado, ser monitorizado, e ser rastreado online (Lenhart et al., 2016).
3. A recusa de acesso refere-se quando alguém utiliza características da tecnologia ou plataforma para prejudicar a vítima, esta ação tendencialmente impede o acesso a ferramentas ou plataformas digitais essenciais, resultando na sobrecarga de um dispositivo, sítio, servidor ou plataforma e impedindo o acesso ao mesmo (Lenhart et al., 2016).

A tecnologia é usada como uma ferramenta para controle coercitivo em relações abusivas (Dragiewicz et al. 2018). Relativamente a relacionamentos, quando este termina, segundo os investigadores Fox and Tokunaga (2015), aqueles que relatam sentimentos de angústia e de certa forma não queriam que terminasse são mais propensos a monitorar um ex parceiro e especular nas páginas das redes sociais dessa pessoa. As tecnologias que conectam os dispositivos dos utilizadores com os objetos do quotidiano, entre eles, sistemas de segurança doméstica, assistentes virtuais conectadas à internet como a Alexa e a Amazon echo, facilitam a capacidade de os abusadores arquivarem e compartilharem dados online, encorajando-os de certa forma a trocar a privacidade pela conveniência.

2.6.1 *Smart Homes*

Durante séculos, inovações mecânicas foram sendo inventadas e introduzidas em casa de forma a reduzir o fardo das mulheres. No entanto, falar dessa evolução durante todos esses séculos, como começaram e porquê está para lá do âmbito desta investigação, daí o foco seja um período histórico mais recente. Exemplo disso é a análise de Faria (2020), sobre a década de 1950, que relata o início da conscientização de muitas empresas de eletrodomésticos, favorecendo a ideia de como os dispositivos elétricos podiam tirar monotonia de tarefas domésticas tediosas. Lavar a roupa à mão, cozinhar e limpar, tarefas que na altura cabiam apenas às mulheres donas de casa, e dessa forma trazer mais tempo de lazer ou outras responsabilidades.

Nessa época, logicamente os eletrodomésticos eram pensados para as mulheres onde os papéis da sociedade forçaram a determinar papéis no lar e no trabalho, daí a publicidade ser dirigida para os homens, pois eram estes que detinham a maioritariamente o poder de compra. Segundo Faria (2020) historiadores traçam a evolução da casa inteligente desde o início dos anos 90 (Figura 3), quando os aparelhos elétricos revolucionaram a forma como se faziam as tarefas domésticas.



Figura 3: História da tecnologia da casa inteligente. (Fonte: Baseado em Harbour Research, 2021)

Tal como o nome indica *smart home*, significa casa inteligente, que consiste em um ou mais ambientes nos quais um ou mais dispositivos físicos (*devices*) conectados à internet e podem ser controlados a distância, por meio de telemóveis, tablet ou comando de voz. Segundo Nascimento and Esslin (2021), esta conexão entre dispositivos nas casas inteligentes permite atender aos pedidos dos seus moradores, de forma cada vez mais fácil e mais rápida, proporcionando assim melhor qualidade de vida e comodidade que casas tradicionais não são capazes. Ainda os autores, Nascimento and Esslin (2021), referem que com o sucessivo aumento do uso das tecnologias e consequente necessidade de inovação e evolução das mesmas, foram surgindo novas técnicas ao longo do tempo de forma a suprimir este carecimento.

Um exemplo deste avanço tecnológico para entender a evolução da automatização e o futuro das habitações, a evolução das *smart homes* na indústria (Figura 4), pode ser diferenciada em diferentes graus, desta forma, após a análise de vários autores (Coelho et al. 2021; Nascimento and Esslin 2021; Wilson et al. 2017; Pinheiro 2004; Silva et al. 2022) a divisão foi feita em quatro graus (1) casa tradicional, (2) sistemas de controle, (3) dispositivos inteligentes e (4) *smart home*.

1. O primeiro, retrata a casa tradicional com instalação elétrica convencional e tecnologia básica em que todos os dispositivos são desconectados, a iluminação, o aquecimento e ar condicionado são básicos.

2. Seguidamente sistemas de controle, que consiste na conexão de todos ou quase todos os dispositivos da casa, trabalhando em conjunto, aqui inclui o controle remoto de luzes.
3. Dispositivos inteligentes, aqui geralmente existe uma abundância de dispositivos inteligentes conectados à internet trabalhando de forma inteligente com um propósito, aqui já se incluem telemóveis com um aplicativo para cada dispositivo, termostatos inteligentes, luzes inteligentes, entre outros.
4. Por último, *Smart home*, a habitação pensa por si mesma, os dispositivos todos interligados comunicação e funcionam por conta própria de acordo com os padrões de configuração previamente selecionados, sendo que nesta casa já existem menos interruptores, dispositivos em zonas específicas, iluminação orientada para o bem-estar, controle de energia e todos os sistemas estão num único aplicativo.



Figura 4: A evolução das *Smart homes*.

Na literatura é recorrente o uso de termos como, “casa conectada” ou “casa automatizada”, para referir casas inteligentes, entretanto é preciso ressaltar que existem diferenças entre esses termos. Uma casa conectada é composta por um conjunto de sensores, dispositivos inteligentes, canais de comunicação, todos os possíveis para atender aos objetivos dos residentes, que muitas vezes implementam essas funções para atender as necessidades. Por exemplo, aprimoramento da segurança, melhoria do suporte à saúde, gerenciamento eficiente

de energia, como também coordenação de iluminação inteligente, tudo isto normalmente em uma rede baseada em IP, como a Internet (Bugeja et al. 2017).

A fácil acessibilidade de dispositivos domésticos conectados à internet, como lâmpadas, câmaras, Tv 's, termostatos, aspiradores, assistentes virtuais e fechaduras inteligentes está a estimular o crescimento das *smart homes*. Numa pesquisa mais recente, Bugeja et al. (2018) afirma que esse crescimento no adquirento dos aparelhos, beneficia os chefes de família, oferecendo a “capacidade aprimorada de controlar e automatizar aspectos relevantes de sua casa e tarefas domésticas diárias”. A maioria destes dispositivos tende a usar sensores embarcados e Internet para trocar e recolher dados entre si e com os utilizadores, incorporando o digital com o ambiente físico da casa (Bugeja et al. 2018).

2.6.2 Violência doméstica na era das *smart homes*

Os sistemas domésticos conectados inteligentes visam melhorar o conforto, conveniência, segurança, entretenimento e saúde dos moradores e seus convidados. Apesar das duas inúmeras vantagens, várias características tornam estes aparelhos das *smart homes* propensos a várias ameaças de segurança. O conceito de violência facilitada por tecnologia doméstica inteligente foi desenvolvido pela Dra. Leonie Tanczer, investigadora internacional em segurança e tecnologia e pela sua equipa (Tanczer et al, 2018).

Perante o exposto, deparamo-nos com a sua investigação no Reino Unido onde Tanczer et al. (2018), realizou entrevistas aprofundadas e workshops. O estudo constatou uma falta geral de sensibilização e de dados sobre abuso facilitado por tecnologia doméstica inteligente e criou um diagrama para demonstração de várias situações possíveis de abuso através dos aparelhos inteligentes na Figura 5.

Já Woodlock (2017), no seu artigo *SmartSafe* tinha o objetivo de “examinar como as tecnologias móveis oferecem oportunidades adicionais para a perpetração da perseguição e violência doméstica contra as mulheres”, com ênfase nos telemóveis e no género feminino. Este estudo constatou que as mulheres que não falam inglês são particularmente vulneráveis à perseguição facilitada pela tecnologia.



Figura 5: Diagrama de Abuso. (Fonte: Baseado em Tanczer, 2018)

A casa destina-se a ser um lugar que transmite proteção, amor, segurança, conforto, entre muitos adjetivos que são possíveis de encontrar para descrever a nossa habitação, que além de tudo isso é ainda o local mais íntimo de qualquer pessoa. Daí, de acordo com Snook et al. (2019), as casas se tornarem muitas vezes lugares do medo, devendo-se grande parte ao facto de como a tecnologia revolucionou a forma como nos comunicamos com os outros e com os objetos. Em muitas comunidades já quase deixou de existir a necessidade de uma pessoa ter que levantar para apagar as luzes, esse simples gesto passou a ser substituído por uma aplicação ligada aos dispositivos conectados com a casa que possibilita controlar várias coisas, desde câmaras, luzes, temperatura, tomadas, entre muitas outras. Ainda Snook et al. (2019), diz que a tecnologia pode ter um impacto poderoso na vida das pessoas, por facilitar em vários aspetos que podem ser positivos e negativos, dependendo de como é concebida e utilizada.

2.6.3 IoT e *Smart Products*

Em 1990, John Romkey desenvolveu o primeiro dispositivo IOT “*internet of things*” com tradução direta- internet das coisas, ao criar a primeira torradeira possível de ser ligada e desligada através da internet, uma torradeira automática Sunbeam Radiant Control (Figura 6),

tudo isto começou porque no ano de 1989 Dan Lynch, presidente do programa Interop, disse durante o programa que daria o prêmio de estrela no ano seguinte a Romkey. Segundo Mancini (2018), se este conseguisse conectar uma torradeira à internet, o aparelho seria colocado em exibição durante a conferência. O experimento aparentemente estranho na época, foi destinado a provar que a internet conseguia controlar fisicamente um objeto, foi conseguido através da conexão da torradeira com um computador com rede TCP/IP, que significa protocolo de controle de transmissão/protocolo da internet. Segundo Romkey (2017), tratava-se de um conjunto de regras padronizadas que permite utilizar em uma rede com a internet, que neste caso aconteceu com um objeto e foi bem-sucedido. Esse êxito foi a primeira instância do que acabaria se tornando uma tendência global.



Figura 6: Primeiro produto IoT. (Fonte: Montagem baseada em Romkey, 2017)

O termo conhecido por IoT, de acordo com Mascarenhas et al. (2021), refere-se à capacidade de dispositivos habilitados para internet se comunicarem de forma independente, a expressão “coisas” inserido na sigla IoT, provém devido aos diversos objetos e dispositivos que podem integrar a rede, como por exemplo os sensores, carros e também dispositivos residenciais. Sendo um dos benefícios centrais, a IoT autoriza tarefas independentes e não desperdiçam horas humanas. Ainda sobre Romkey (2017), o pioneiro em uma verdade duradoura sobre dispositivos inteligentes no qual observou um entusiasmo na reação dos visitantes da Interop de 1990. De acordo com Elder (2019), poucos compreenderam os problemas, durante a demonstração da torradeira, onde Romkey já pensava na privacidade e segurança, incluindo quem poderia ver a torradeira online e controlá-la. O que parecia não ter grande problema por ser um objeto insignificante, uma torradeira não necessita de controle de dados pessoais, passou a um sentimento contraditório ao constatar a possibilidade de alguém que não o próprio dono conseguir ligá-la enquanto este se encontra fora da sua habitação. Foi então aqui que tudo começou, e que se percebeu a inúmeras possibilidades maravilhosas para

a ciência, a medicina, o meio ambiente e a conveniência do dia a dia das pessoas, mas por outro lado a vulnerabilidade da privacidade e segurança que são cruciais na utilização dos aparelhos. À vista disso, foi assim que existiu todo um mundo novo de ameaças potenciais que exploram as fraquezas dos sistemas inteligentes.

Consequentemente, por essa falta de destreza das capacidades dos produtos que foram sendo criados ao longo dos anos, geraram o aumento de controle e abuso tecnológico, Riley (2020). Muitos desses problemas dos produtos inteligentes pensados para melhorar a qualidade de vida das pessoas, surgem quando existem tentativas deliberadas de sabotar o sistema através da introdução de vírus. Existem claro dispositivos mais vulneráveis do que outros, de acordo com a Npr (2016), além de ser uma rádio pública nacional, também é uma organização de comunicação social que constatou se uma torradeira estiver conectada ao *wi-fi* ou roteador doméstico, já estabelece uma camada de segurança, é essencialmente esse dispositivo que garante que as conexões aliadas aos dispositivos não são maliciosas. Apesar disso, essa camada de proteção também pode ser violada. Neste contexto, foi importante reconhecer a importância da compreensão mais profunda da proteção de dados e a segurança tecnológica, as suas causas e consequências no mundo, identificando os abusos e propondo melhorias para que não se repitam.

Por outro lado, a evolução da IOT, permitiu, segundo Pillan et al. (2017), o desenvolvimento de novas abordagens no design de produto e ambientes proporcionou soluções inovadoras e vantagens valiosas para os utilizadores, em termos de funcionalidade convenientes e de melhores modalidades de interação entre utilizadores humanos e os sistemas tecnológicos. Segundo Zheng et al. (2019), com essa evolução um mercado promissor de produtos inteligentes e conectados, com a capacidade de recolher, comunicar, processar e produzir informação, trouxe uma transformação digital predominante. Nessa perspectiva, o que se torna central é a contribuição do produto para um conjunto de serviços.

Produtos inteligentes, permitem a comunicação ou interação com o ambiente, outros produtos inteligentes ou humanos. Como Kees et al. (2015) enfatizam a existência de uma parte do produto inteligente que existe independentemente da tecnologia IoT, onde poderia, neste contexto, ser considerado um objeto habilitado para IoT. Os produtos, quando se tornam inteligentes, a aparência, o design e as funções dos produtos permanecem as originais. Desse ponto de vista, segundo os autores Pardo et al. (2020), o produto inteligente é, primeiramente, um produto físico, mas ao mesmo tempo é um objeto conectado, ou seja, o seu valor é acrescido com ferramentas adicionais, como a capacidade de comunicar com humanos, com outros produtos e fomentar um sistema de informação num produto sociável. Mitew (2014) introduz

esse ponto de vista, do objeto sociável como uma subcategoria de produtos inteligentes, ao mencionar que, os objetos se tornam sociáveis por terem a capacidade de um atuador. Conseguem agir ao trocar dados com outros, conseguindo possivelmente realizar ações de acordo com os dados recebidos. Os objetos sociáveis não necessitam de nenhum tipo de ação humana. Além de que, devido à enorme quantidade de dados que os produtos inteligentes podem armazenar, agregar e processar, os objetos podem assim adaptar-se e reagir, sendo capazes de compartilhar e analisar toda a informação de contexto que adquirem, segundo o autor Mitew (2014). Estes propõem-se à eficácia de um ambiente permanentemente atualizado, de uma forma que leva os humanos a se adaptarem.

2.7 Resultado

O objetivo deste capítulo foi explorar de entre vários artigos, livros e organizações, sobre a violência de gênero, as vítimas, os perpetradores e como a tecnologia está ligada à violência, desde a sua utilização em *smart homes* como em *smart products*. Os artigos foram avaliados ao nível de identificar as práticas existentes na violência e os vários tipos classificados, tais como, os resultados obtidos com a abordagem no desenvolvimento das *smart homes* e conseqüentemente os *smart products* que as integram estão sendo utilizados.

Mesmo com um universo grande de trabalhos explorados desde 2011 (aproximadamente 200 artigos), em vários desses artigos o pressuposto não foi encontrado, a generalidade do assunto divagava o contexto e conseqüentemente a solução não se mostrou precisa. Segundo Woodlock (2014), com o acesso fácil a tecnologias inteligentes, os abusadores têm acesso às vítimas 24 horas por dia, utilizando produtos inteligentes para abusar e assediar de forma fácil, instantânea e à distância. A lacuna de pesquisa mostra-se evidente, ao se perceber como os produtos e as suas funções podem ser repensadas. Portanto, uma análise *benchmarking* de *smart products* (capítulo 3) tornou-se um dos objetivos complementares para um resultado consistente, agregado a essa pesquisa teórica subsidiou-se a elaboração de um questionário online (capítulo 4). É importante destacar que o resultado desse questionário guiou para o desenvolvimento de possíveis cenários apresentados no capítulo 5, tal como a conclusão e solução encontrada.

CAPÍTULO 3| *Benchmarking de Smart Products* Existentes

3.1 Introdução

O termo "*smart product*" tornou-se cada vez mais popular nos últimos anos, à medida que cada vez mais fabricantes incorporam tecnologias avançadas nos seus produtos, tal como fez Romkey (2017) com a sua torradeira. *Benchmarking*, por sua vez, provém de "*benchmark*", que significa 'referência' e o seu processo compreende (a) a seleção de um produto, neste caso específico, a ser comparado, (b) a aquisição de dados de comparação com produtos concorrentes, (c) a análise de desempenho e a identificação de fontes de problemas, bem como (e) a identificação de avaliações de utilizadores (Pesando, 2022).

Percebe-se que cada vez se tornou mais fácil obter produtos inteligentes, tanto pelos preços como pela maior qualidade de vida que a grande maioria promete oferecer. Esta análise de *benchmarking*, tem como objetivo analisar mais de perto o conceito de produtos inteligentes, ao comparar alguns dos produtos inteligentes mais populares no mercado atual. Perceber quais as características de cada um e o porquê de serem inteligentes, com o princípio de que um produto inteligente é aquele que incorpora tecnologia avançada em objetos do dia-a-dia, tornando-os mais úteis e fáceis de utilizar. A maioria dos produtos inteligentes estão também ligados à Internet, ou a outras redes, que permitem receber atualizações e novas características ao longo do tempo (Silva, 2022; Bowles, 2018). Ainda dentro do mesmo capítulo pretendeu-se ainda diferenciar aqueles que possibilitam rastrear a localização e conseguir determinar quais as ameaças que cada um contribui. Para posteriormente, nos capítulos 4 e 5, os produtos analisados serem incluídos em perguntas chave e cenários, no desenvolvimento.

3.2 Análise de Produtos

Os produtos inteligentes proporcionam benefícios para os consumidores, de facto, a maioria dos consumidores concordaria que o melhor dos produtos inteligentes é a capacidade de receber novas características e atualizações ao longo do tempo (Pesando, 2022). Por outro lado, os produtos inteligentes também representam vários desafios tendo em consideração as suas características de 10 produtos foram analisadas.

Selection Criteria Segundo Pesando (2022), os produtos mais usados pela maioria, são sobretudo telemóveis e tablets, *smartwatches* (por exemplo, o Apple Watch), televisões inteligentes, eletrodomésticos inteligentes (por exemplo, um frigorífico inteligente), câmaras de segurança, aspiradores robóticos (iRobot) e carros. Nesse contexto, qualquer produto que

esteja ligado à Internet ou a alguma outra rede pode ser considerado um *smart product* (Bowles, 2018). Para um balanço mais realista dessa abordagem, foi elaborada uma listagem de *smart products*, abordados também no capítulo 1, majoritariamente integrantes assíduos numa *smart house*, ou dedicados ao uso quotidiano recorrente. Este capítulo dedicou-se apenas ao diagnóstico detalhado a partir do levantamento da análise de mercado, as compilações das funcionalidades correspondentes de cada produto referem-se a um mecanismo físico composto por vários elementos, que juntos trabalham para atingir uma ou mais funções, podendo muitas vezes ser autônomo.

Análise dos produtos selecionados

Amazon Echo Studio

A Amazon funciona como um alto-falante Echo, o Studio oferece os mesmos recursos de assistente de voz Alexa (Figura 7). Ao verbalizar-se "Alexa" (ou "Amazon", "Computador" ou "Echo") está ativa e de seguida, apenas necessita de se dar um comando ao alto-falante. Este aparelho ronda em volta dos 190€ (Greenwald, 2022). A Alexa responde a perguntas sobre informações gerais, como o clima, os resultados no desporto, conversões de unidades, reproduzir músicas, ler audiolivros, controlar dispositivos domésticos inteligentes e fazer chamadas telefônicas ou chamadas de voz Drop In para qualquer usuário que tenha esta tecnologia. É uma assistente de voz, mas pode ser um pouco difícil de trabalhar. Contudo, é esperado que se obtenha uma experiência bastante precisa, especialmente, quando se pode controlar uma casa inteligente (Greenwald, 2022).



Figura 7: Amazon Echo (Fonte: Google images)

Este aparelho permite usar o alto-falante para controlar dispositivos compatíveis com IOS/Android. Essa conexão das assistentes virtuais permite também destrancar portas, fazer chamadas telefônicas e compras, além de controlar outros aparelhos interligados. Segundo Esposito (2022), as echo exigem confirmação verbal quando solicitada uma ação sensível, mas pesquisadores da Royal Holloway University em Londres e da University of Catania, na Itália descobriram que é possível o invasor ter acesso a qualquer ação quando dito “sim” ao comando cerca de seis segundos após a solicitação. Isto permite-lhe desligar as luzes, ligar um forno de micro-ondas inteligente, definir o aquecimento para uma temperatura insegura ou destravar fechaduras inteligentes, ligar para qualquer número de telefone, incluindo um controlado pelo invasor, para que possa escutar o áudio próximo à assistente virtual (Esposito et al. 2022). Embora este Echo utilize uma luz para indicar a realização de chamadas, os dispositivos nem sempre ficam visíveis para os utilizadores, os menos experientes poderão não entender o significado e importância da luz. Com esse controle não autorizado é ainda possível fazer compras, apesar de ser enviado um email o invasor pode apagar esse email antes da vítima ter acesso (Goodin, 2022).

Avaliações dos utilizadores:

Segundo a PCMag, uma revista especializada em informática, o Amazon Echo Studio foi considerado uma escolha dos editores, em que numa escala de 5 foi avaliado com 4.5 como “excepcional” (Greenwald, 2022). Tal como foi possível ser observado na Amazon, que em 36,302 comentários, 76% disseram respeito a avaliações 5 estrelas.

Air Tag

Este dispositivo de 1,26 polegadas projetado para atuar como um localizador de objetos desenvolvido pela Apple (Figura 8), tem vindo a ser alvo de várias críticas sobretudo pelo facto de este acessório ser cada vez mais usado para a monitorização de pessoas sem permissão. Relevante realçar segundo Cole (2022), a Apple lançou o primeiro AirTag em Abril de 2021, ou seja, é um dispositivo ainda recente e desconhecido aos olhos de muitas pessoas. O design discreto pode torná-lo perigoso, além disso apenas funciona com a localização ativa e inclui auto-falantes. Este *smart device* possibilita a mesma pessoa ter vários ao mesmo tempo ativos, e ainda partilhar a localização com quem quiser (Apple, 2022). O AirTag não precisa de GPS para se localizar: ele usa a rede “Encontrar”, da Apple, para isso. Para funcionar a Apple exige a utilização de ID da Apple (Apple, 2022).



Figura 8: Apple AirTag. (Fonte: Google images)

Existem vários rastreadores GPS compatíveis já com Android, mas neste caso o analisado e mais conhecido entre os demais, é apenas compatível com Apple. Este pequeno disco com um valor apelativo de 39 euros, do tamanho equivalente a uma moeda de dois euros, tem dentro uma antena para *Bluetooth* e para a tecnologia *Ultra Wideband*, permite comunicar com outro dispositivo e até 100 metros como limite de conexão, neste caso um iPhone e essa comunicação permite saber onde se encontra exatamente o AirTag. Não precisa de carregador pois têm embutido uma pilha com duração de até um ano, e quando esta acaba permite mudar a pilha sem necessidade de assistência.

Além de prometer ser resistente à água à profundidade máxima de um metro, com duração máxima de 30 minutos, e apenas partilha a localização exata com iPhones do 11 até ao mais recente (Apple, 2022). Mesmo antes de existir o AirTag similares já eram confrontados com a facilidade dos abusadores que além de anexarem dispositivos GPS externos e embutidos usamos para perseguir e aterrorizar vítimas (Dimond et al. 2011; Southworth et al., 2007; Woodlock 2017). Dependendo do conhecimento tecnológico do abusador, um sobrevivente pode sentir que é impossível escapar (Dimond et al. 2011).

Avaliações dos utilizadores:

Do ponto de vista de abuso, as avaliações dos utilizadores é que temem este aparelho, pois não tinham conhecimento da posse do dispositivo até o encontrarem ou este ser emparelhado com um iPhone, que muitas vezes vítimas ao não os terem, não encontram. Na PCMag, apesar das várias notícias de 2022 sobre este aparelho, a que diz respeito à sua avaliação feita por Segan (2021) avaliou o rastreador como “excelente” com 4.0 e escolha dos editores.

iRobot Roomba j7+

Dentro dos robôs de limpeza inteligentes, que são máquinas criadas especificamente para realizar este serviço, projetado para espaços interiores, cada vez são mais autônomos e inovadores. Existe o iRobot Roomba j7+ (Figura 9) equipado com sensores embutidos que mapeiam o ambiente e atuadores embutidos que realizam o movimento e a limpeza, permitindo quase a sua total autonomia. Além disso, segundo Raff et al. (2020) estes utilizam conectores e softwares instalados para comunicação com o telemóvel do utilizador, em qualquer lugar, e a qualquer momento. No capítulo 2, constatou-se várias situações onde este aparelho está cada vez mais presente em *smart houses*.



Figura 9: iRobot Roomba j7+ com esvaziamento automático e ligação Wi-Fi (Fonte: Raff et al. 2020)

Este aspirador robô Roomba j7 + da iRobot com ligação Wi-fi, aprende e mapeia a planta de sua casa, usando o software de inteligência artificial para detetar obstáculos e redirecionar-se para evitar os mesmos, efetuando uma limpeza completa. Este, ao encontrar pela primeira vez os obstáculos envia fotografias, através da sua câmara embutida na parte da frente, para o aplicativo móvel associado (iRobot Home, compatível com Android e iOS), onde é possível controlá-lo. O j7+ é também conhecido por permitir limpezas de espaços programados num determinado horário e suportar comandos de voz como a Google Assistant e Amazon Alexa.

Avaliações dos utilizadores:

Segundo a PCMag, (Moscaritolo, 2021) o iRobot Roomba j7+ foi considerado (“*exceptional*”) com uma avaliação de 4.5 e com selo de escolha dos editores, apesar do seu preço ser bastante elevado este promete auto esvaziamento.

Ecobee Smart Thermostat Premium

O Termostato permite controlar a temperatura da habitação através do telemóvel, para além de suportar plataformas como Alexa, HomeKit, Google Assistant e SmartThings. Este dispositivo bastante elegante (Figura 10) tem incorporado um monitor de qualidade do ar, assim como um sensor de sala remoto. Pode funcionar como um dispositivo de segurança doméstica e um alto-falante inteligente autônomo alimentado pela Alexa ou os comandos de voz do Google Assistant/Siri com um alto-falante inteligente compatível, para alterar as configurações do termostato (Delaney, 2022). Além disso, possui notavelmente a nova tecnologia de ocupação de radar e de deteção de movimento da Ecobee, que permite que o dispositivo detete movimento a uma distância maior do que em modelos anteriores, registrando também movimento em cantos, para alterar as configurações do termostato, receber as notícias, reproduzir música e verificar a temperatura em salas com sensores. O modelo Premium suporta chamadas Alexa Drop In, bem como Alexa Calling and Messaging (Delaney, 2022).



Figura 10: Ecobee Smart Thermostat Premium (Fonte: Delaney, 2022)

Permite ajustar a temperatura de casa através do site ou pelo aplicativo de telemóvel. Além disso, o dispositivo pode verificar na internet quais são as condições climáticas da zona para deixar o ar-condicionado na temperatura ideal para quando chegar a casa.

Avaliações dos utilizadores:

A revisão deste termostato pela PCMag consta com 4.5 (“Exceptional”) e escolha dos editores (Delaney, 2022). Tal como na Amazon (2022) este com 650 avaliações dos consumidores está classificado com 4.5.

Apple Smartwatch Series 8

O *Apple Watch Series 8* (Figura 11) é um *smartwatch* lançado em 2021 que, entre outras funcionalidades, permite a realização de chamadas, reprodução de músicas, GPS, monitorização de sono, contador de passos, monitorização de menstruação e gravidez, lembrete sedentário e até mesmo um dispositivo que alertará ao usuário quando ele estiver fora do alcance bluetooth (Low, 2022, Wetsman, 2022, Apple, 2021).



Figura 11: Apple watch series 8. (Fonte: Apple, 2021)

A monitorização do ciclo menstrual é feita através de verificação da temperatura no pulso dos usuários a cada cinco segundos durante a noite. O utilizador terá que dormir pelo menos 5 noites com o *smartwatch* para estabelecer uma linha de base (Wetsman, 2022). Se o *smartwatch* não estiver bloqueado com uma palavra-passe, é possível aceder a praticamente todas as informações do telemóvel associado, como aplicações de mensagens, pedómetro e Apple Pay, contactos e outras (Song, 2022, Perry, 2022).

A Apple, após várias críticas relacionadas com violação de privacidade, utilizou uma estratégia de marketing ao relatar vários resgates de pessoas através das mais recentes funcionalidades (Sherr, 2022). Estas funcionalidades tiveram a intenção de recuperar a confiança dos seus utilizadores, sendo possível adicioná-las mesmo nos aparelhos mais antigos (Ramirez, 2022). Assim, pode-se concluir que estas novas atualizações trouxeram novas formas de controlar e rastrear as vítimas através de satélites, mesmo sem o telemóvel ou em locais sem rede móvel (Ramirez, 2022; Prakash, 2022; Sherr, 2022; Colby, 2022).

Avaliações dos utilizadores:

Este *smartwatch* foi classificado pela PCMag como 4.5/5 (“Outstanding”) e pelo TheVerge como 8.0/10. As principais vantagens mencionadas são o seu sistema operativo, a nova funcionalidade de deteção de acidentes de carro e uma maior duração da bateria (até 24h). As desvantagens são o design igual ao modelo anterior, uma funcionalidade de monitorização de menstruação e gravidez limitada e a sua compatibilidade apenas com dispositivos da Apple (Wetsman, 2022, Song, 2022).

Yale Assure Lock 2

A Yale Assure Lock 2 é uma fechadura inteligente com um teclado que permite a abertura da casa sem a utilização de uma chave (Figura 12). Possibilita também uma interoperabilidade com outras funcionalidades normalmente presentes em *smart homes*. Além do teclado, possibilita também abrir a porta por *bluetooth* através da *app* da Yale ou utilizando o Apple HomeKit (Tuohy, 2022).



Figura 12: Yale Assure Lock 2, fechadura inteligente. (Fonte: Yale, 2022)

Estas fechaduras digitais podem, no entanto, ser utilizadas com o intuito de vingança por parte de abusadores. Há relatos de vítimas sobre a perda de controlo sobre estes aparelhos “os números de código da fechadura digital na sua porta da frente mudavam todos os dias e ela não conseguia perceber porquê” (“*the code numbers of the digital lock at her front door changed every day and she could not figure out why*”) (Bowles, 2018). Alguns exemplos são códigos que eram alterados diariamente ou portas que abriam misteriosamente. O *site* oficial da Yale (2022) relata que são recebidas notificações cada vez que a porta abre e quando, e ainda é possível visualizar um *feed* de atividades 24 horas por dia. O que pode vir a facilitar a monitorização forçada.

Avaliações dos utilizadores:

Este produto foi classificado pela PCMag como 4.0/5 (“Excelent”) e pelo TheVerge como 7/10. Como vantagens enumeram o seu design atraente, as diversas opções de uso (teclado, bluetooth, etc.) e a compatibilidade com os principais sistemas inteligentes (Touhy, 2022). Ainda segundo o Tuohy (2022), as desvantagens são mencionadas problemas com a bateria como tempo curto de aviso quando tem bateria fraca e baixa duração da bateria no modelo *Wi-Fi*.

Ring Cam on Mount

A Ring Indoor Cam é uma câmara de segurança interior. Esta câmara (Figura 13) conta com um sistema de áudio nas duas direções, permitindo assim a comunicação entre diferentes espaços da casa (Delaney, 2019). Segundo Vigderman & Turner (2022), é compatível com vários sistemas de “*smart homes*” e a sua “app mobile” permite fazer “*livestream*”, algo que é benéfico, por exemplo, para pais que querem cuidar dos seus filhos quando não estão em casa.



Figura 13: Ring Cam on Mount, câmara de vigilância. (Fonte: Delaney, 2019)

No entanto, estas funcionalidades têm as suas desvantagens em casos de abuso doméstico. A funcionalidade de “*livestream*” pode ser usada para o controlo obsessivo das vítimas, invadindo assim a sua privacidade e permitindo a intimidação destas (Vigdor, 2019). Pode também ser usado para obter gravações e utilizá-las com fins maliciosos, como chantagens com conteúdos de nudez, por exemplo. Já o seu sistema de som pode ser utilizado para intimidar e insultar as vítimas (Vigdor, 2019; Chen, 2020). Um aparelho geralmente utilizado para segurança, nas mãos erradas, pode tornar-se na maior fonte de angústia de uma vítima (Chen, 2022).

Avaliações dos utilizadores:

Esta câmara, foi avaliada com um 9.5/10 pelo *website* security.org, mencionando a *app* “Ring Neighbours” como um dos principais pontos fortes em relação às marcas concorrentes no mercado (Vigderman and Turner, 2022). Esta é uma *app* que conta com algumas funcionalidades com um objetivo de comunicação entre vizinhos para melhorar a segurança nas vizinhanças. No entanto, há alguns relatos de hackeamento destes aparelhos e uso do seu sistema de áudio para insultar várias famílias. Há também notícias sobre ex-funcionários da empresa que foram apanhados a verem vídeos de clientes. A empresa respondeu a estas “*headlines*” reforçando que a empresa tem feito esforços contínuos na melhoria do seu sistema de segurança (Chen, 2020). O ritmo destas melhorias tem, no entanto, sido questionado por experts nestes sistemas de segurança. Já na PCMag, segundo Delaney (2019) foi classificado como 4.0/5 (“Excelent”).

Philips Hue Smart Light Starter Kit

Este kit de luzes inteligentes permite criar cenas de cores personalizadas ou escolher entre as opções predefinidas através do uso de um aplicativo Philips que permite a instalação em IOS e Android (Figura 14). De acordo com Staff (2019), este kit oferece a possibilidade de criar rotinas diárias, como quando ligá-los ou desligá-los e controlar grupos de luzes simultaneamente, tudo através da aplicação comum a todos os utilizadores. São ainda lâmpadas reguláveis, com três cores diferentes, branco, espectro de cores e iluminação branca ajustável. Tem em média um valor aproximado a 170€ e está disponível no mercado há cerca de 3 anos (Hildebrand, 2020). Um dos pontos mais positivos das luzes inteligentes é a poupança de energia, o que gera um maior interesse por parte do público.



Figura 14: Phillips Hue *Smart Light Starer Kit*, luzes inteligentes. (Fonte: Staff, 2019)

O sistema é igualmente compatível com a Amazon Alexa e o Google Assistant, entre outros, o que permite controlar o dispositivo pela voz. Tem ainda correspondência via *bluetooth*. Com o uso desta tecnologia, os interruptores de luz já existentes tornam-se inúteis, o que oferece alguma resistência, pois, convencer a família a usar o controle de voz requer a criação de um novo hábito. Neste, como em todos os avanços dos *smart products* verificam-se aspetos negativos (Bowles, 2018).

Um exemplo disso é Ferial Nijem, uma vítima de abuso tecnológico e violência doméstica, em que a testemunha afirma, que é muito conveniente o utilizador ter o “total acesso e controle sobre toda a sua casa” (“*total access and control over your entire home*”), (Ghebresslassie, 2018). Mas adianta que, à medida que a sua experiência com a tecnologia doméstica se tornou negativa, apercebeu-se dos perigos e implicações do que esse tipo de tecnologia pode fazer, como o facto de que nunca está fora do alcance do seu agressor (Ghebresslassie, 2018). Embora a tecnologia inteligente, dispositivos controlados pela web nas luzes inteligentes, possa fornecer conveniência e uma sensação de segurança para alguns, essas ferramentas estão sendo cada vez mais usadas por outros para monitorar, assediar, perseguir e intimidar. E nas situações que decretaram abuso as vítimas disseram que ao “desligar o sistema significava desligar a casa, desligar o sistema de iluminação para mim também” (Ghebresslassie, 2018). Concluindo assim que, a monitorização dos abusadores reflete nos utilizadores que sentem perder o controlo da sua própria casa.

Avaliações dos utilizadores:

De acordo com a PCMag, este kit conta com várias avaliações de “excelente” (Staff, 2019). Na Amazon (2020) verificaram-se 3299 comentários sobre este produto com 4.6 estrelas, sendo que 5% dessas avaliações são negativas, conta com 3% das classificações de 3 estrelas e maioritariamente, correspondendo a 92% são comentários bastante positivos.

Computador, iPad ou Tablet

Estes produtos tecnológicos têm finalidades muito idênticas, pois processam informações eletronicamente na forma de dados e podem ser programados para as mais diversas tarefas. Estes dispositivos (Figura 15) veem os dados como 1s e 0s, mas sabem combiná-los para formar coisas muito mais complexas, como uma foto, um vídeo, um website, um jogo e muito mais (Brant, 2020, Segan 2022). Para realizar as tarefas, os computadores e os tablets usam uma combinação de hardware e software.



Figura 15: Computador e Ipad. (Fonte: Google images)

Através de um computador, iPad ou um tablet é possível ter controlo quase que absoluto sobre todos os passos da vida de outro utilizador (Nield, 2020). Idênticos a um telemóvel, estes aparelhos têm quase todas as coisas em comum, como o facto de ser possível Stalkerware, como indica o termo em inglês, é um aplicativo que rastreia todas as atividades realizadas no produto de uma vítima específica e repassa as informações ao *stalker*, que pode ser um parente controlador ou um parceiro ciumento (Nield, 2020). Silenciosos e portanto, mais difíceis de serem detetados os *Stalkerwares* são *softwares* projetados para monitorar a vida de um alvo específico. Instalados sem o consentimento da vítima, essas aplicações são capazes de rastrear informações como localização do aparelho, histórico de navegação, mensagens SMS e conversas em redes sociais, alguns deles podem, inclusive, gravar vídeos ou áudios (Nield, 2020). Estes dispositivos suscitam números elevados de violência, pois oferecem cada vez mais programas e aplicações que permitem a invasão de privacidade.

Avaliações dos utilizadores:

Como referência um computador da Apple Macbook Air, na PCMag está avaliado pelos utilizadores com um total de 4.0 estrelas (Brant 2020). Comparativamente, o mesmo aparelho na Amazon (2020), conta com 4.8 estrelas. Num total de 1363 avaliações, sendo 96% delas positivas, 1% classificou o mesmo com 3 estrelas e apenas 3% avaliaram de forma negativa. Em relação ao Ipad Air 2022, observa-se que na PCMag a avaliação é de 4.5 estrelas (Segan, 2022). Sobre o mesmo Ipad na Amazon (2022) as avaliações têm uma média de 4.8 estrelas num total de 1205, onde 94% são extremamente positivas, com 3 estrelas tem cerca de 2% das avaliações e 4% são negativas.

Xiaomi Mi Smart Power Plug

Uma *smart plug* (tomada inteligente) é um dispositivo (Figura 16) que se conecta ao Wi-Fi e permite, por meio de *apps* para telemóveis e tablets controlar equipamentos domésticos. São

pequenos dispositivos que permitem integrar aparelhos domésticos à rede de internet, dessa maneira, é possível controlar luzes e eletrodomésticos à distância.



Figura 16: Tomada inteligente Xiaomi Mi Smart Power Plug. (Fonte: You Get)

As *smart plugs*, possuem o recurso de desativar automático em caso de pico de energia ou outros incidentes elétricos. Elas também mandam notificações sobre a oscilação de energia ou alertas quando os números de itens conectados nela podem apresentar riscos, têm ainda a capacidade de monitorar o gasto de energia. Além disso, encontram-se a preços acessíveis, desde 20€ e permitem a automatização da casa sem grandes reformas ou troca de equipamentos. Alguns aparelhos oferecem suporte a plataformas integradas, como a Alexa da Amazon, o Google Home, entre outros. Contudo, este *smart product* tem também pontos negativos, pois permite o acesso à privacidade e controlo da vida e da habitação de outra pessoa.

Avaliações dos utilizadores:

Através de uma análise às avaliações referentes à *smart plugs*, na Amazon concluiu-se que grande parte dos utilizadores se mostraram bastante satisfeitos com a sua aquisição, tendo 89% de 9111 comentários avaliativos. Observa-se que, 6% dos clientes classificaram o produto com 3 estrelas e ainda 5% dos utilizadores avaliaram este produto de forma negativa por diferentes motivos, o que se resume em uma média de 4.5 estrelas.

Em contra-análise, observando os dados da PCMag, concluímos que a média de classificação é apenas de 3.5 estrelas.

Todos estes produtos têm *bluetooth* e *wi-fi*. A maioria, além da possibilidade de serem usados em ambiente interno, são também maioritariamente compatíveis com IOS. Tudo isto facilita a partilha e receção de dados, dando origem a muitas das principais formas de violência tecnológica, como clonagem de dispositivos ou o monitorização indesejado.

Foi elaborada a Tabela 8 destes *smart products* e das características comuns, permitindo uma leitura clara e recolha de dados relevantes para o estudo.

Tabela 8: Identificação das características dos smart products.

	Amazon Echo Studio	AirTag	iRobot	Ecobee Smart Thermostat	Apple Smartwatch serie 8	Yale Assure Lock 2	Ring Cam on Mount	Philips Hue Smart Light Starter Kit	Computador, Ipad ou tablet	Xiaomi Mi Smart Power Plug
Função / Características										
Compatível com IOS	X	X	X	X	X	X	X	X	X	X
Compatível com Android	X		X	X	X	X	X	X	X	X
Número de utilizadores*	X		X	X		X	X	X	X	X
Número de dispositivos**	X	X							X	
Controlo de palavra-passe***	X		X		X	X			X	
Ativação por voz	X			X	X			X		X
Ativação pela app de longe	X	X	X	X		X	X	X		X
<i>Fingerprint scanner</i>									X	
<i>Face ID</i>									X	
Botão de desativação	X		X		X		X		X	X
Partilha a localização	X	X			X				X	
Acessa a localização	X	X	X	X	X				X	X
Acesso aos contactos	X				X				X	
Acesso ao microfone	X				X		X		X	
Acesso altifalantes	X	X	X	X	X	X			X	X
Autônomo		X	X	X			X			X
<i>Bluetooth</i>	X	X	X	X	X	X	X	X	X	X
<i>Wifi</i>	X	X	X	X	X	X	X	X	X	X
<i>Touch sensor</i>	X		X	X	X	X			X	
Câmara			X				X		X	
Luz	X		X	X	X			X	X	X
Interior	X	X	X	X	X	X	X	X	X	X
Exteior		X			X	X	X	X	X	

*Permite ter mais que um utilizador

**Permite estar ligado a mais de um aparelho em simultâneo

***(identificação facial, padrão, código, impressão digital)

3.3 Rastreadores GPS

Dos *smart products* analisados percebeu-se também que a maioria dos produtos em estudo têm como funcionalidade principal rastrear e compartilhar a localização do utilizador (Bowles, 2018).

Segundo Silva (2022), as características estão relacionadas à forma como os produtos funcionam e podem separar-se em dois grupos: tipo de dispositivo, sendo mais comuns a escolha por dispositivos físicos e muitas vezes amparados por aplicativos para dispositivos móveis como, telemóveis e tablets, e tecnologias, que determina quais os tipos de tecnologia empregadas nos dispositivos, ambos foram incluídos na Tabela 9 que sintetiza as características dos produtos encontrados na literatura e no mercado. Sendo assim, a literatura tem apontamentos de que o dispositivo físico possa vir a funcionar totalmente por si só. Ainda de acordo com Silva (2022) relativamente à tecnologia empregada nos produtos de mercado, esta refere que alguns produtos físicos usam GPS, *Bluetooth* e GSM (Global System for Mobile Communication) a mesma que é usada para enviar mensagens e fazer chamadas. A privacidade das redes sociais (Facebook, LinkedIn, Instagram e Snapchat) passa muitas vezes por não existir um filtro e qualquer pessoa que pode ver as publicações e o acesso à localização exata que inicialmente é pedida como um requisito para entrar na aplicação, esta pode ser desativada nas definições do telemóvel, contudo não existe um alerta, ou seja o utilizador tem que ter essa consciência (Silva, 2022; Dragiewicz et al. 2018). Além disso, para utilizar estas aplicações o acesso ao microfone, câmara e galeria é implícito como obrigatório, caso contrário a aplicação fica muito vaga. O Snapchat permite a partilha de localização em tempo real com os “amigos”, além de mostrar a maior concentração de pessoas em todos os locais do mundo. Já o Whatsapp, Messenger, Twitter e Reddit, todos sites de discussão, permitem rastrear a localização, além de possibilitarem ver quem está online, partilhar informação pessoal, que muitas vezes leva à partilha apenas por conveniência (Dragiewicz et al. 2018). O casino ainda que com uma finalidade diferente também pede para acessar a localização do utilizador quando este deseja apostar.

Quanto ao Google (2022) o website deriva de informação da utilização dos serviços *Google*: vídeos vistos, anúncios vistos e clicados, localização, sites na web visitados, navegadores e dispositivos utilizados para aceder ao *Google services*, atividade de compra e em sites. Histórico de navegação sincronizado com a conta Google, informação de registo telefónico se utilizar os serviços Google para fazer chamadas telefónicas. Tipo e configurações do dispositivo, sistema operativo, móveis informações sobre a rede (nome da operadora, número

de telefone), aplicação número de versão, endereço IP, relatórios de acidente, atividade do sistema, tudo é aceite nos termos e condições, tal como o *Google maps* que apenas funciona com o comando de aceitar a partilha de localização ativo. Ao fazer uma pesquisa automaticamente assume que é a partir da localização atual exata, e memoriza-a.

As *smartbands* (pulseiras inteligentes) com a finalidade de rastrear utilizam *Bluetooth*, conectividade *Wireless* com qualquer aparelho compatível, uma versão simples aos *smartwatches*. Uma tecnologia emergente que utiliza igualmente *Bluetooth*. Acesso à localização exata através do *Chip UI* com o recurso de “Busca precisa” presente no “*Find My*”, que demonstra a informação precisa de onde se encontra o relógio. Além disso, inclui bússola, altímetro sempre ativo, chamadas de emergência internacionais, *SOS* emergência, altifalante, microfone, *Apple Pay* e *Gymkit* (Song, 2022, Perry, 2022). Os noticiários, compras online e aplicações de encontros, todos têm funções distintas, mas necessitam da localização para detalhes importantes ou mesmo para permitirem a utilização como no caso das aplicações de encontro conseguem saber com quem e quantas vezes os utilizadores se cruzaram na rua.

Tabela 9: Aplicações, websites e dispositivos que rastreiam a localização.

Nome	Tipo de dispositivo	Utilizador -alvo	Tecnologia
Facebook, LinkedIn, Instagram, Snapchat	Aplicação social media para dispositivo móvel / <i>Website</i>	Jovens, Adultos, Idosos	<i>Wifi / GPS</i>
Whatsapp e Messenger	Aplicação para mensagens para dispositivo móvel / <i>Website</i>	Jovens, Adultos, Idosos	<i>Wifi / GPS</i>
Twitter, Reddit	Aplicação de discussão para dispositivo móvel / <i>Website</i>	Jovens, Adultos, Idosos	<i>Wifi / GPS</i>
Casino, Apostas	Aplicação jogos para dispositivo móvel / <i>Website</i>	Jovens, Adultos, Idosos	<i>Wifi</i>
Google	<i>Website</i>	Crianças, Jovens, Adultos, Idosos	<i>Wifi /GPS</i>
Google maps	Aplicação para dispositivo móvel / <i>Website</i>	Jovens, Adultos, Idosos	<i>Wifi / GPS</i>
<i>Smart band</i>	Produto físico	Animais, crianças e Jovens, Adultos, Idosos	<i>Bluetooth</i>
<i>Smartwatch</i>	Produto físico	Jovens, Adultos, Idosos	<i>Bluetooth / GMS</i>
Noticiários, compras online	Aplicação para dispositivo móvel / <i>Website</i>	Jovens, Adultos, Idosos	<i>Wifi /GPS</i>
Aplicações de encontros	Aplicação para dispositivo móvel	Jovens, Adultos, Idosos	<i>Wifi /GPS</i>
Alexa, Amazon echo	Produto físico	Crianças, Jovens, Adultos, Idosos	<i>Bluetooth / Wifi / GPS</i>

No caso dos AirTags, dispositivos criados com o intuito de rastrear objetos (Cole, 2022), este funciona com *bluetooth* para a descoberta de proximidade (secção 3.2). Outras gamas também recentes de rastreadores rivais são os (1) Chipolo, (2) Samsung Galaxy SmartTag, (3) Tile, Tile Mate, Tile Slim e Tile Sticker presentes na Tabela 10.

(1) No caso do *Chipolo*, este funciona com a aplicação “Encontrar” da Apple. Têm também função alarme que pode ser controlada através da *Siri*, *Google assistant* e *Amazon Alexa*. Inclui um sensor de proximidade com o formato de um pequeno disco, discreto.

Distância até 60 metros, ao se perder um objeto/pessoa, a App mostra num mapa a sua última localização conhecida. Consegue uma autonomia de até 2 anos sem trocar a pilha e é resistente à água.

(2) O Samsung Galaxy SmartTag funciona com o *SmartThings Find*, que está somente nos dispositivos *Samsung Galaxy*. Para funcionar, o utilizador tem que ter uma conta Samsung e também oferece a UWB para rastreamento preciso da localização na Galaxy SmartTag+ (Hall, 2021). Inclui além disso *bluetooth* (“low energy”) de baixa energia (BLE), o LogIn de localização é a partir do telemóvel que no caso da *SmartTag* regular, é necessário que o telemóvel seja o Galaxy Note 20 Ultra, o Galaxy S21+ e o Galaxy S21 Ultra. Tem um alcance de 120 metros reclamados e 40 metros efetivos (Hall, 2021).

Finalmente, o (3) Tile, Tile Mate, Tile Slim e Tile Sticker permite a utilização por dispositivos Apple ou Android. apenas os usuários de Tile com o aplicativo instalado conseguem detetar um Tile. Reúne características semelhantes ao Samsung Galaxy Smart Tag pois além de incluir BLE, é igualmente necessário o login de localização a partir do telemóvel (Hall, 2021). As versões mais recentes de Tile oferecem 3 anos de bateria útil, já os mais antigos duram em média 1 ano. Tem um alcance superior aos demais analisados contando com um total de 120 metros reclamados e 80 metros efetivos (Hall, 2021).

Tabela 10: Produto físico, rastreador de localização.

Nome	Tipo de dispositivo	Utilizador -alvo	Tecnologia
AirTag Apple	Produto físico	Animais, crianças, Jovens, Adultos, idosos	<i>Bluetooth</i>
Chipolo	Produto físico	Animais, crianças e Jovens, Adultos, Idosos	<i>Bluetooth</i>
Samsung Galaxy SmartTag	Produto físico	Animais, crianças e Jovens, Adultos, Idosos	<i>Bluetooth</i>
Tile, Tile Mate, Tile Slim e Tile Sticker	Produto físico	Animais, crianças e Jovens, Adultos, Idosos	<i>Bluetooth</i>

3.4 Resultado

Diante dos estudos e análises da revisão de literatura da percepção das lacunas do estudo, em relação à privacidade pessoal, foi possível identificar também preocupações da pergunta que rege a presente dissertação, com foco nos *smart products*.

O propósito deste capítulo foi a validação da (H1) “A violência doméstica pode aumentar devido à falta de privacidade. Há muitos produtos e serviços que violam a privacidade ao partilhar a localização” (Mace and Caxemira, 2021; Faria and Lauriault, 2021; YWCA, 2017).

A partir do contexto, foi criado um quadro teórico de produtos listados neste capítulo, procurou confirmar e comprovar a primeira hipótese.

A privacidade é o fator mais importante para reduzir a violência doméstica (Lau et al. 2018). Este enfoque, verificou que a maioria dos produtos inteligentes precisa de partilhar a localização, no caso do Amazon Echo Studio, além da localização é um dispositivo que permite emparelhar e comandar outros. Observou-se então, que este foi o único encontrado em análises de artigos científicos. A restante a informação sobre os produtos analisados neste capítulo, proveio de revistas tecnológicas e outros sites de informação.

CAPÍTULO 4 | Perceção das Vítimas

4.1 Introdução

“O objetivo de um inquérito é obter informações que possam ser analisadas, extrair modelos de análise e fazer comparações” (Bell, 1997).

A decisão da utilização de metodologia quantitativa, centrou-se numa amostra da população residente em Portugal. Sendo um procedimento metodológico que se apresenta útil na compreensão de fenómenos, como atitudes e opiniões, para além de ser poder ser utilizado em qualquer lugar e em larga escala. A elaboração do questionário iniciou-se com a definição dos objetivos que se pretende alcançar com o estudo (Bogdan & Bilken, 1994). Foram consideradas as hipóteses formuladas, e consideradas variáveis dependentes e independentes. Segundo Fortin (2006), a variável dependente é aquela que sofre o efeito da variável independente. O questionário é o que permite obter um instrumento de medida que traduz os objetivos de estudo em variáveis mensuráveis, além de ajudar a organizar e a controlar dados de maneira rigorosa (Fortin, 1999).

4.2 Inquérito por Questionário

O questionário procurou responder a informações mais detalhadas sobre a extensão da vitimação, facilitada pelos *smart products*. Através do resultado da análise das experiências pessoais dos participantes, comparando o modo de como o mesmo dispositivo é utilizado pelo género masculino e feminino. Partindo deste pressuposto, foi importante implementar dois contextos, quem geralmente é a vítima e de que forma esta está ligada aos *smart products*, para compreender a influência que estes podem ter na prática do abuso. Para este fim, foi lançado o questionário online e presencialmente, este método ajudou a uma coleta de dados superior à esperada, tendo em conta o tempo que o questionário esteve disponível online.

4.2.1 Participantes

A definição da população, é uma das questões importantes a considerar no design da metodologia fundamental, pois a mesma corresponde ao grupo sobre o qual o investigador tem interesse em recolher informações e extrair conclusões (Tuckman, 2012; Almeida and Freire, 2008).

309 respondentes essencialmente adultos e jovens, compreendidos com idades entre 15 e 81 anos, (M=36,48; DP= 14,86), 233 feminino (M=37,17, DP=14,91) e 75 masculino (M=

34,53, DP=14,51) todas as respostas foram admitidas numa primeira fase de seleção, pelo contributo mínimo.

Uma vez que o objetivo se centra nos mais representados entre os utilizadores de tecnologia e as vítimas de violência de parceiros íntimos, o recrutamento de participantes aconteceu em três meios presencial, digital e eletrónico, que implicou uma combinação de convites diretos, divulgação por meio de plataformas digitais, entre elas redes sociais tais como, Facebook, LinkedIn e Instagram, e por correio eletrónico para serviços onde foram enviados um total de 459 emails diretos a organizações de serviços através de endereços de correio eletrónico individuais e de organizações identificadas a partir da combinação de pesquisas na web, por serviços de apoio a vítimas de violência doméstica, sexual, e comunidades especializadas no âmbito do estudo amostra composta por serviços de aconselhamento e assistência social generalista (incluindo o bem-estar da comunidade e serviços de apoio), como é o caso da Cruz Vermelha Portuguesa, que foi enviado email para todos os distritos, serviços de apoio à vítima APAV, onde também foi enviado para todas as associações de Portugal, tais como para comunidades LGBTQ+, para a associação ILGA. Como tal, o estudo é com base numa amostra probabilística aleatória, mas, no entanto, é reflexo de uma consulta substancial com número de intervenientes do setor de apoio a vítimas, maioritariamente pela APAV de Braga e Porto.

Todas as respostas foram consideradas válidas, pelo que foi necessário dividir a discussão, pois a violência doméstica e os smart product dependem de um terceiro fator, inicialmente foi o género (masculino, feminino ou prefiro não dizer). O género influencia tanto na violência doméstica como na quantidade de *smart products* que o género feminino têm em relação ao masculino. O género no caso é a variável independente, e tanto a vitimação como os *smart products* são variáveis dependentes. Posteriormente após esse diagnóstico dividiu-se em dois grupos de análise (1) foi vítima pelo menos uma vez e (2) não foi vítima, conforme a Tabela 11.

Em relação ao género, foi notória a diferença do género feminino (75,4% mulheres, 24,3% homens e 0,3% prefiro não dizer). Dividida em três grupos foi possível observar que todos os inquiridos da amostra tinham pelo menos um aparelho inteligente (M=3,8, Anexo VI, figura 44).

Tabela 11: Frequência para toda a amostra.

Geral N (%)	Idade M (DP; Min.; Max)	Género N (%)			Residente em Portugal N (%)		Smart Devices M (DP; Min.; Max)
		Masculino	Feminino	Prefiro não dizer	Sim	Não	
Total							
309 (100)	36,4 (14,86; 15,81)	76 (24,6)	233(75,4)	1(0,3)	289 (96,4)	11 (3,6)	3,80 (1,50; 1; 11)
1. Vítimas pelo menos uma vez							
194 (62,8)	33,8 (14,15; 15; 78)	53 (17,2)	142 (46)	0 (0)	187 (60,5)	7 (2,3)	3,90 (1,10; 1; 11)
2. Não Vítimas							
115 (37,2)	41,9 (14,94; 15; 81)	23 (7,4)	91 (29,4)	1(0,3)	111 (35,9)	4 (1,3)	3,79 (1,59; 1; 10)

4.2.2 Material e Procedimentos de Recolha de Dados

Face ao objetivo da dissertação, a técnica do questionário revela-se um bom meio de recolher opiniões, atitudes, conhecimentos e experiências positivas e negativas relacionadas à tecnologia. Com a finalidade de obter-se respostas fiáveis, o vocabulário contido nas perguntas teve o cuidado de seguir uma linguagem simples para poder ser compreendida por todos. Existiu ainda, o cuidado de salientar (tanto nos emails como presencialmente), o anonimato do questionário para permitir que os participantes o fizessem sem qualquer receio, possibilitando um maior número de histórias pessoais. O questionário foi desenvolvido e realizado no software online Google Forms, exposto online para os participantes durante duas semanas em novembro de 2022.

Pré-teste

O pré-teste do questionário foi efetuado nos dois primeiros dias de novembro de 2022 e pretendia perceber a validade do questionário para atingir os objetivos pretendido, tendo em conta desde o tempo de preenchimento a compreensão de todas as questões e escalas por parte dos participantes, as dificuldades encontradas a nível de vocabulário e a reação geral. Dada a sensibilidade do problema, o questionário foi enviado a 10 pessoas, para se estudar os pontos que deveriam ser melhorados antes do lançamento definitivo. Para cada participante foram anotadas as suas reações e dificuldades.

Cada questionário levou uma média de 10/15 minutos a ser respondido, a dimensão e o tempo de preenchimento do questionário foram fatores apontados como positivos, então a quantidade

de perguntas não foi alterada. Relativamente à dificuldade de compreensão das questões por parte dos participantes, às questões 17, 18 e 22, (Ao utilizar a Internet, alguma vez fez alguma das seguintes coisas para ajudar a proteger a sua privacidade? Alguém já lhe fez alguma das seguintes coisas? Já fez alguma das seguintes coisas para se proteger a si mesmo/a do assédio ou abuso online?) suscitaram dúvidas em alguns inquiridos. As perguntas pediam resposta em escala Likert (1-muito frequentemente a 5- nunca), pelo que, os respondentes afirmaram ser melhor alterar a escala para o número vezes (nunca; 1 vez; entre 2 a 4; mais de 5; sempre), é de salientar que as dificuldades sentidas relativamente às questões anteriores estavam apenas relacionadas com o método de resposta.

Dividido em cinco seções, com 63 itens incluídos num total de 26 perguntas organizadas de acordo com: (0) termo de consentimento informado, logo a seguir a seção (1) coleta de dados socioeconômicos, demográficos (questão 1 à 8); Para as restantes seções do questionário (2) a experiência tecnológica (questão 9 à 16): (3) observa a privacidade pessoal (questão 17 à 19); (4) dedicada ao abuso online (questão 20 à 21); e (5) para obter informação sobre o impacto do abuso (22 à 26), foram estruturadas com base em 3 questionários:

0) Termo de consentimento livre e informado: foi apresentado junto com uma breve descrição do propósito do questionário aos participantes, mesmo antes do início do questionário, descrevendo o número de perguntas e tempo que demora, tal como o anonimato dos dados prestados pelo inquirido (Anexo IV).

1) Dados socioeconômicos, demográficos: tais como localidade, género, idade, nível educacional, habitação, emprego e outras características de interesse para o estudo, nomeadamente como descreve o seu relacionamento.

2) Experiência tecnológica: composta por 25 itens, incluídos em 16 questões, estruturadas com base em dois questionários: O “*Measuring Cyber Abuse Survey*” por Princeton Survey Research Associates International para o Instituto de Investigação de Dados e Sociedade Para efeitos deste estudo, Lenhart et al. (2016). Este instrumento de medição permite identificar a vitimação e a perpetuação de comportamentos abusivos, através de um formato de perguntas fechadas com respostas de múltipla escolha para os seguintes determinantes: hábitos e influência da tecnologia no dia-a-dia. O segundo questionário “*Violência, Perseguição, Vigilância e Privacidade no Smart Prosuming Home do Futuro*” por Sovacool et al. (2021) em que segundo os autores, este estudo

além de explorar até que ponto as tecnologias e sistemas inteligentes podem atuar como potenciais facilitadores de violência doméstica, também explora como o uso desses sistemas inteligentes pode também impedir possíveis mecanismos para reduzir e fornecer proteção às vítimas. À medida que estes dispositivos, e as plataformas e redes que os utilizam, se tornam mais integrados na nossa vida quotidiana, proporcionam espaços importantes para interagir com os outros e aprender coisas novas. Como em todos os lugares onde as pessoas se juntam, existe o potencial para interações positivas e de apoio, e também para experiências negativas e prejudiciais em online (Lenhart et al. 2016). Para que os espaços online facilitem o livre fluxo de informação e a troca de ideias, todos devem sentir-se confortáveis a habitar e a interagir nesses espaços. Para melhor compreender estas experiências, precisamos de saber mais sobre o teor da vida social online e qual a frequência e conhecimento na utilização desses aparelhos.

3) Privacidade pessoal: composta por 16 itens repartidos em 3 questões, esta seção agregou dados do questionário “*Measuring Cyber Abuse Survey*”, Lenhart et al. (2016)

4) Abuso tecnológico: composto por 4 itens em 2 questões baseadas no segundo questionário já referido anteriormente na seção dois, “*Violência, Perseguição, Vigilância e Privacidade no Smart Prosuming Home do Futuro*” por Sovacool et al. (2021) e o terceiro questionário “*Experiências de Vitimização de Agressão por Parceiro Íntimo em diferentes contextos sociais*” por Marganski & Melander (2018) que explora a extensão da vitimização por agressão cibernética em relacionamentos íntimos e sua co-ocorrência com experiências pessoais de violência psicológica, física e sexual por parte do parceiro.

5) Impacto do abuso: a última seção compôs 10 itens, incluídos em 5 questões em que três eram de resposta aberta e as outras duas foram estruturadas mais uma vez com base em “*Measuring Cyber Abuse Survey*”, Lenhart et al. (2016).

Somando um total de 309 respostas da amostragem probabilística aleatória, os participantes do estudo representam a população e, com isso, os processos de generalização tornam-se mais adequados. Este método foi o escolhido fundamentalmente por ser mais fácil recolher dados. No entanto, a composição da amostra com tais propriedades tende a depender do conhecimento populacional de quem participa.

Todos os participantes foram completamente voluntários, não foi dada qualquer compensação económica, como também todos os participantes receberam o mesmo formulário de consentimento informado para tomarem conhecimento do estudo, e só depois encaminhados para um link para completar o questionário online (Tabela 12). Além disso, o autor (Alonso et al. 2005), alerta que informação recolhida através da técnica do questionário consiste não no que as pessoas pensam, mas no que dizem que pensam, não no que elas preferem, mas no que elas dizem que preferem. Essa afirmação levou a considerar alguns dos itens, tanto formulados no sentido positivo como outros no sentido negativo, através da utilização maioritariamente de escalas Likert, escala muito utilizado em estudos que envolvem a identificação de atitudes, com o objetivo de se controlar a discrepância nas respostas (Bogdan & Bilken, 1994). Consequentemente utilizou-se três tipos de questões: questão de resposta aberta, as de questão de resposta fechada e questões em grelha. As questões de resposta aberta, permitiam ao inquirido construir a resposta com as suas próprias palavras, permitindo deste modo a liberdade de expressão, e pode envolver uma história real ou inclusão de histórias de participantes (Bell, 1997). Já as de resposta fechada, expõem um significado claro de possíveis respostas, sem ambiguidades e em número adequado, em termos de extensão, para não criar desmotivação aos participantes. As questões apresentam-se em grelha ou tabela para registar respostas a uma ou mais questões ao mesmo tempo (Bell, 1997).

Tabela 12: Descrição das perguntas e secções do questionário.

Questionário	
Secção 1 – Dados demográficos	<p>Atualmente vive em Portugal? Em que cidade vive? Idade género Com quem vive atualmente? Nível educacional? Qual dos seguintes o/a descreve melhor? Como descreve o seu relacionamento?</p>
Secção 2 - Experiência tecnológica	<p>Quanto diria que percebe sobre sistemas inteligentes? Quanto diria que percebe sobre rastreador de GPS? Por favor, digam-me se alguma vez utilizou a Internet para fazer alguma das seguintes coisas. Indique outras situações da Internet em que necessita de partilhar a sua localização. Utiliza essas redes de conexão e aparelhos tecnológicos? Indique sistemas/produtos inteligentes que incluem rastreador de GPS que utiliza para além dos mencionados acima. Estou confortável com a monitorização de sistemas inteligentes. Indique os sistemas/produtos inteligentes que utiliza.</p>
Secção 3 - Privacidade pessoal	<p>Ao utilizar a Internet, alguma vez fez alguma das seguintes coisas para ajudar a proteger a sua privacidade? Alguém já lhe fez alguma das seguintes coisas? Alguém já lhe fez alguma das seguintes coisas?</p>
Secção 4 - Abuso baseado em Tecnologia	<p>Responda à tabela seguinte Há o risco de que sistemas de rastreamento GPS sejam intrusivos?</p>
Secção 5 - O impacto do Abuso online e presencial	<p>Já fez alguma das seguintes coisas para se proteger a si mesmo/a do assédio ou abuso online? Já deixou de publicar algo online porque se preocupou com a possibilidade de ser rastreada a sua localização devido a essa publicação? Tem alguma história/acontecimento (seu ou de outra pessoa), que se tenha lembrado sobre o abuso digital? Tem alguma história/acontecimento (seu ou de outra pessoa), que se lembre sobre abuso físico? Quais as suas preocupações relacionadas com produtos inteligentes e violência doméstica?</p>

As respostas foram também obtidas por meio presencial onde aconteceu num espaço físico de uma loja em Braga (Figura 17) durante 4 dias consecutivos. Dando início no dia 4 de

Novembro até dia 8 de Novembro de 2022, os questionários foram recolhidos através de um ipad colocado propositadamente na área de espera da loja, esta zona era composta por um sofá, uma poltrona e uma mesa, foi escolhida esta zona por se tratar de área com menos barulho e facilitava a adesão pois as pessoas teriam que esperar pela sua vez e enquanto isso preenchiam. A recolha ocorria assim que os clientes entrassem e fossem instruídos para a zona de espera pela dona do estabelecimento.

Guiões dos questionários foram elaborados, com objetivo de diferenciar três abordagens distintas, no Anexo I, relativamente à abordagem em meio presencial, no Anexo II, consta o guião de abordagem em questionário para associações (Apav, Ilga e Cruz Vermelha Portuguesa) e no Anexo III, de uma forma mais casual focalizado para publicação em redes sociais e mensagens diretas.



Figura 17: Imagens do espaço de recolha presencial.

A abordagem realizada antes mesmo de se sentarem, (Anexo I) baseava-se numa breve explicação e caso concordasse, que aconteceu 100% das vezes, era então entregue o iPad, no final entregavam o iPad de volta, era feito um breve agradecimento, e prosseguia-se para o participante seguinte, que normalmente já se encontrava à espera, ou então, quando o iPad se encontrava ocupado, e previa-se a demora devido a vários fatores: (1) tinha acabado de começar a preencher; (2) era logo atendido e o questionário ficava em espera; e (3) pessoa idosa que não conseguia ver bem. Nessas situações, era pedido ao participante que respondesse pelo seu telemóvel pessoal, alcançando-se assim um maior número de respostas, no distrito de Braga (209).

Dos 309 inquiridos, um total de 209 foram pré-selecionados e analisados como vítimas (ou já foram vítimas em algum momento), com base em verificações de qualidade. Essas verificações de qualidade incluíam que nas respostas às questões 18, 19 ou 20, pelo menos tivessem passado por uma das situações apresentadas como “abuso tecnológico” ou que nas questões 24/25 narrassem algum acontecimento (por exemplo, seu ou de outra pessoa). As restantes respostas foram tratadas com não vítimas, um total de 100 respondentes que não se enquadraram em nenhum dos abusos questionados. Estes dois grupos (1) vítimas pelo menos uma vez e (2) não vítimas, foram fonte de análise. A agressão tecnológica analisada das respostas, foi definida pelo uso de tecnologias socialmente interativas, como mensagens de texto e redes sociais ou *smart products* utilizados para rastreamento e monitorização por um indivíduo para facilitar o comportamento de assédio contra outro indivíduo. Após a entrega e recolha dos questionários a análise dos dados foi o passo seguinte.

4.3 Análise e Discussão dos Resultados

Em primeiro lugar, após recolhidos os dados as respostas foram extraídas e sujeitas a tratamento no editor Microsoft Excel, antes da apresentação dos resultados abordou-se o tratamento dos dados e respetivamente os métodos estatísticos utilizados, em como as respostas de texto foram transformadas em unidades de sentido, sintetizando a análise interpretativa dos dados através de padrões de resposta, conjugados em categorias e subcategorias, que serviam de base à análise realizada.

Para a realização de todas as análises quantitativa estatística recorreu-se ao *software* informático IBM *Statistical Package for the Social Sciences* (SPSS), *for Windows*, versão 29.0, para relatar a frequência das respostas e variáveis chave de interesse, tais como táticas abusivas

utilizadas, tecnologias utilizadas e preocupações para o futuro no desenvolvimento de serviços de respostas e prevenção.

Nos dados qualitativos foram sustentados pela análise temática indutiva da pesquisa e submeteu-se à separação em diferentes categorias que se distinguem por características não numéricas, ditas escalas nominais e ordinais, apresentaram-se do tipo discreto (Afonso and Nunes, 2019). Ao final, as variáveis inseridas no questionário foram classificadas em seis categorias distintas: (i) sociodemográficas, (ii) geográfica, (iii) conhecimento tecnológico, (iv) monitorização, (v) abuso de privacidade e (vi) opinião. As tabelas (Anexo V) apresenta as categorias e variáveis do questionário

Uma análise adicional foi realizada, análise qualitativa, sobre a qualidade das respostas das perguntas abertas colocadas ao longo do questionário, a fim de identificar situações recorrentes, preocupações futuras e recomendações pelos participantes, que de outra forma não seriam possíveis.

Posto isto, o passo seguinte caracterizou-se segundo Hill and Hill (2005) pela determinação da confiabilidade do questionário, aspeto importante a ter em consideração quando se procede à construção e aplicação de um questionário com intuito de medir atitudes ou outro tipo de variável similar. Fiabilidade tem a ver com a replicação do estudo e validade, sem referir que é a interna, com a correspondência entre as respostas e o procurado. Procura-se que as conclusões sejam coerentes com a investigação, ou seja, verifica-se se o estudo “mede ou descreve o que supostamente deve medir ou descrever” (Bell, 1997).

A ferramenta utilizada para medição da fiabilidade de escalas foi o Alfa de Cronbach, e a correlação item total corrigido que verifica se os itens correlacionados entre si fazem sentido. Precisa-se que o Alfa de Cronbach seja $> 0,7$. Percebe-se pela figura 18, que este valor está bastante aceitável (0,855). Na matriz de correlações entre itens, (Anexo VI), a matriz diz o quanto os itens estão relacionados com os outros itens da mesma escala. Ao estarem bem correlacionados, fazem sentido juntos. Neste caso, os itens têm que ser superiores a 0,5. Nos casos em que foi inferior, foi necessário entender se fazia sentido fazer alguma modificação. Para isso, o Alfa de Cronbach teria que ficar com um valor maior, o que não aconteceu, daí todas as questões permanecerem iguais e foram analisadas dessa forma.

Alfa de Cronbach	Alfa de Cronbach com base em itens padronizados	N de itens
,855	,838	84

Figura 18: Estatísticas de confiabilidade.

Este estudo foi concebido para determinar os efeitos dos *smart products* na violência doméstica e para descobrir os métodos que os perpetradores utilizam para praticar o abuso nas vítimas. A demonstração dos resultados foi apresentada em três partes, de acordo com as seguintes características: Perfil Demográfico; Experiência tecnológica e padrões de abuso; Impacto dos *smart products* nas vítimas. Esta seção inclui as conclusões e discussões dos resultados.

Seção 1. Perfil Demográfico: Com o objetivo principal de perceber se os *smart products* podem viabilizar novas formas de perseguição e abuso na violência do parceiro íntimo, trezentos e nove questionários foram distribuídos maioritariamente a participantes residentes em Portugal (96,4%, N=298). A taxa de resposta foi de 77,3% (N=238; Anexo VI; ver Figura 36) na zona do Norte do país, seguindo-se por Lisboa (N=28), Faro (N=12), Centro (N=11), Alentejo (N=6), Ilhas (N=3) e o restante a fora de Portugal (N=11). A Figura 19, apresenta a prevalência da maioria identificada como género feminino (75,4%, N=233), uma representação esperada dada a recolha presencial ter ocorrido num estabelecimento predominantemente frequentado por mulheres e dada a representatividade das colaboradoras femininas que agrega as associações de apoio contactadas.

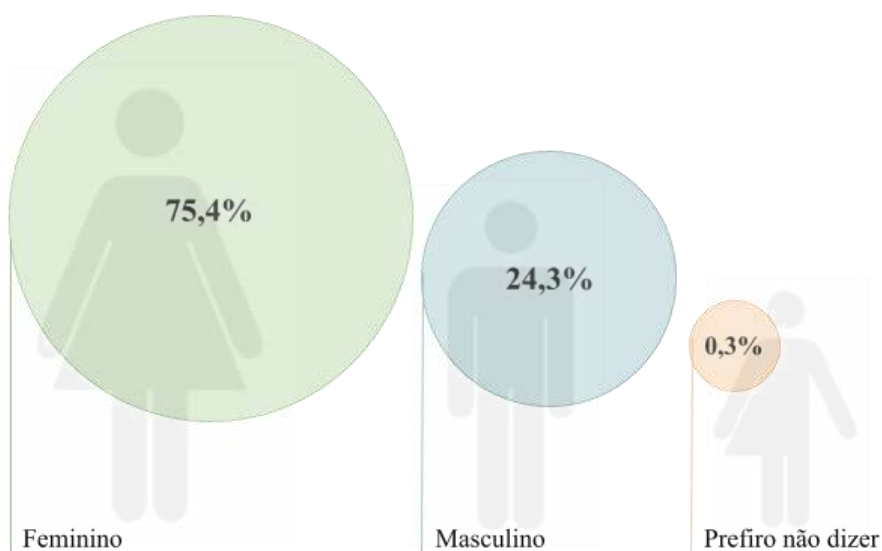


Figura 19: Perfil Demográfico.

Globalmente, a média de idades dos participantes foi de 36,4 (com um intervalo de 15 a 81 anos). Uma porção esmagadora dos participantes trabalhava a tempo inteiro (N=181) ficando em segundo lugar os estudantes (N=50).

Na Tabela 13, entre os dados demográficos dos participantes do questionário, não consta a análise do gênero “prefiro não dizer”, pois foi obtida apenas uma resposta (0,3%). Relativamente à residência, este participante insere-se no grupo dos 3,6% que não residem em Portugal e não mencionou nenhum acontecimento pertinente para o estudo.

Quanto ao nível de educação, observou-se uma maior afluência de respondentes com licenciatura 31% (N=96) e ensino secundário 28,8% (N=89). Entre os restantes, 41 participantes afirmaram ter mestrado, 39 tinham formação profissional, 34 ensino básico, 5 doutoramento, 3 apenas sabiam ler/escrever, e 2 recorreram à opção “outros”, em que um afirmou ter pós-graduação.

Dos participantes, 75,1% tinham atualmente um parceiro e 24,9% estavam solteiros no momento. No geral, 3,9% dos participantes descreveram seu relacionamento como novo, 0,6% descreveram seu relacionamento como casual/aberto, 14,6% descreveram seu relacionamento como estável, 19,1% descreveram seu relacionamento como sério, 1,9% declaram estar noivos/as e, por último, mas com uma percentagem bastante elevada, 35% afirmam estar casados/as.

Conforme anteriormente visto nas estatísticas da revisão de literatura, de acordo com a APAV (2019), a idade mais frequente das vítimas foi dos 25-34, 35-44 e 45-54 anos. No que diz respeito aos participantes, percebeu-se que a idade das vítimas era maioritariamente dos 18-24 anos, o que difere dos resultados de 2019 da APAV. Neste sentido, é possível observar um crescente aumento da população de jovens que se tornam vítimas cada vez mais cedo. Importante referir que este questionário foi apenas focado na violência tecnológica e física. Sendo que tendencialmente a população mais jovem está mais associada à tecnologia, estas percentagens são o reflexo dessa parcela da amostra de respondentes.

Tabela 13: Características sociodemográficas global.

	Total (309)	M (N= 75)	F (N= 233)
	M (DP; Min.; Max) % (N ^a)	M (DP; Min.; Max) % (N ^a)	M (DP; Min.; Max) % (N ^a)
Atualmente vive em Portugal			
Sim	96,4 (298)	23,3 (72)	73,1 (226)
Não	3,6 (11)	1 (3)	2,3 (7)
Idade**	36,48 (14,86; 15, 81)	35,79 (14,09; 17, 74)	36,62 (15,09; 15, 81)
15-17 anos	1,9(6)	0,6 (2)	1,3 (4)
18-24 anos	28,2 (87)	7,1 (22)	21,1 (65)
25-34 anos	22 (68)	5,8 (18)	16,2 (49)
35-44 anos	14,2 (44)	3,6 (11)	10,7 (33)
45-54 anos	21,7 (67)	4,2 (13)	17,5 (54)
55-64 anos	8,1 (25)	2 (6)	6,1 (19)
65 -74 anos	2,6 (8)	0,7 (2)	1,9 (6)
75-81 anos	1,4 (4)	0,4 (1)	1 (3)
Com quem vive atualmente			
Sozinho/a	5,5 (17)	1,9 (6)	3,6 (11)
Familiares	48,5 (150)	12 (37)	36,6 (113)
Amigos	2,6 (8)	0,3 (1)	2,3 (7)
Parceiro/a romântico/a (PR)	15,8 (49)	4,9 (15)	14,6 (34)
PR e filho/a/os/as	25,2 (78)	4,9 (15)	20,1 (62)
*Familiares e Amigos	0,3 (1)	0 (0)	0,3 (1)
*Família e PR e filho/a/os/as	1,6 (5)	0 (0)	1,6 (5)
*Amigos e PR.	0,3 (1)	0,3 (1)	(0)
Nível de educação			
Ler/escrever	1 (3)	0 (0)	1 (3)
Ensino Básico	11 (34)	3,6 (11)	7,4 (23)
Ensino Secundário	28,8 (89)	8,1 (25)	20,7 (64)
Formação profissional	12,6 (39)	4,9 (15)	7,8 (24)
Licenciatura	31,1 (96)	5,2 (16)	25,9 (80)
*Pós-graduação	0,3 (1)	0 (0)	0,3 (1)
Mestrado	13,3 (41)	2,6 (8)	10,4 (32)
Doutoramento	1,6 (5)	0 (0)	1,6 (5)
Outro	0,3 (1)	0 (0)	0,3 (1)
Emprego			
Desempregado/a	8,7 (27)	2,3 (7)	6,5 (20)
Estudante	16,2 (50)	3,2 (10)	13 (40)
Trabalhador/a estudante	7,1 (22)	1,9 (6)	5,2 (16)
Trabalhador/a part-time	2,3 (7)	0,6 (2)	1,6 (5)
Trabalhador/a	58,6 (181)	15,5 (48)	42,7 (132)
Reformado/a	5,2 (16)	0,6 (2)	4,5 (14)
Outros	1,9 (6)	0 (0)	1,9 (6)
Como descreve o seu relacionamento			
Solteiro/a	24,9 (77)	7,1 (22)	17,8 (55)
Relacionamento novo	3,9 (12)	1,3 (4)	2,6 (8)
Relacionamento casual/aberto	0,6 (2)	0,3 (1)	0,3(1)
Relacionamento estável	14,6 (45)	3,9 (12)	10,7 (33)
Relacionamento sério	19,1 (59)	5,2 (16)	13,6 (42)
Noivo/a	1,9 (6)	0,3 (1)	1,6 (5)
Casado/a	35 (95)	6,1 (19)	24,6 (76)
*Viúvo/a	2,3 (7)	0 (0)	2,3 (7)
*Divorciado/a	1,6 (5)	0 (0)	1,6 (5)
*Celibato	0,3 (1)	0 (0)	0,3 (1)

Legenda: (M) masculino; (F) feminino; (PR) Parceiro Romântico (N) número; (DP) Desvio Padrão; (M) Média; (Min) Mínimo; (Max) Máximo.

*(novo) Resultados da resposta "outros" do questionário

** Baseado em APAV(2019).

Seção 2. Experiência tecnológica: Esta parte apresenta os resultados relativos à seção dois do questionário, onde são exploradas as experiências dos indivíduos com a internet e situações de monitorização. Para isso, a primeira pergunta de variável dependente procura explorar o conhecimento dos usuários sobre sistemas inteligentes. Aqui, tal como na pesquisa de Sovacool et al. (2021), o foco era perceber a experiência dos respondentes em duas áreas sistemas inteligentes e rastreadores por GPS. Para os sistemas inteligentes, o interesse na resposta dos participantes a esta questão era um fator relevante, visto que, não ter conhecimento nesta área pode facilitar aos abusadores ferramentas para consentir com mais abuso.

Segundo Dimond et al. (2011) e Chatterjee et al. (2018), as vítimas sentiam-se menos experientes em tecnologia que os seus agressores. Esta falta de experiência leva as vítimas a serem pressionadas a resolver os problemas, sendo que muitas das vezes não possuem o conhecimento para identificar e lidar. Com base nas evidências apresentadas na revisão de literatura, mulheres sentiam que eram menos experientes em tecnologia. Os resultados da Figura 20, onde as barras de erro indicam intervalo de confiança de 95%, mostram que a maioria das mulheres (42,9% em 75,4%) apenas tem uma vaga ideia do que são sistemas inteligentes. Já em relação aos homens, a sua maioria (9,7% em 24,3%) também responderam ter uma vaga ideia. É possível ainda perceber que apenas 4,85% das mulheres têm uma boa ideia do que são sistemas inteligentes, o que mesmo assim é uma percentagem bastante baixa e vai de encontro aos resultados da revisão de literatura.

Relativamente aos rastreadores GPS, percebeu-se existir uma clara confusão com os GPS habitualmente conhecidos, pelas respostas dadas nas perguntas abertas. A maioria dos respondentes realmente referiam ter esse aparelho, mas não um rastreador por GPS. Por essa razão, devido à incoerência e incerteza, decidiu-se anular a análise desta questão, pois resultaria em discórdia com os restantes resultados.

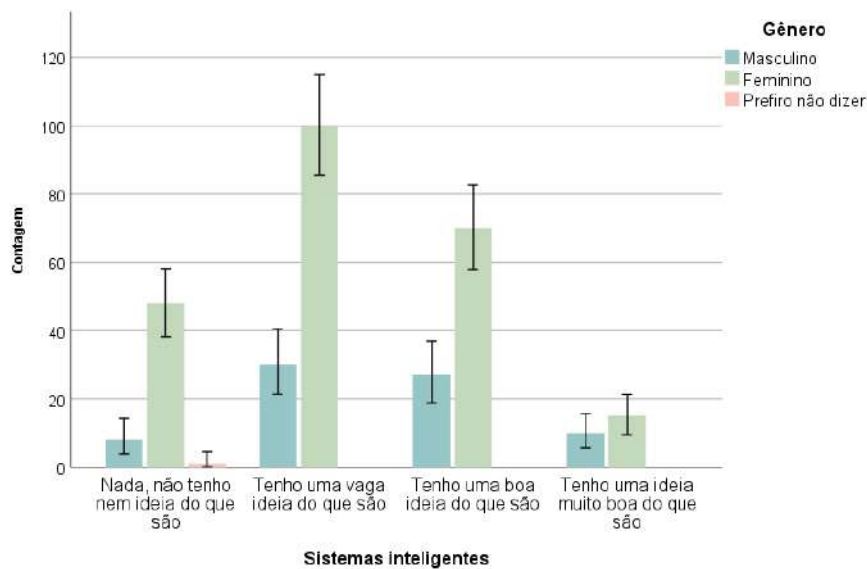


Figura 20: Diferenças de conhecimento sobre sistemas inteligentes.

De acordo com Freed et al. (2018), a falta de conhecimento das vítimas proporciona aos agressores maior facilidade a aceder a contas e dispositivos digitais e usá-los para controlo. É perceptível que os sistemas inteligentes estão relacionados à privacidade de dados pessoais.

A pesquisa com as partes interessadas pediu aos participantes que respondesse a 4 itens, que mediam a frequência da utilização de redes de conexão e 4 itens que mediam a frequência de utilização em aparelhos tecnológicos. No geral, 71,2%, a maior frequência de utilização relatada pelos participantes afirmou “muito frequentemente” para as redes sociais Facebook, LinkedIn ou Instagram, e a 98,3% na utilização de telemóvel.

Comparando as respostas do género feminino e masculino na Figura 21, mas tendo em conta a discrepância no volume de respostas de ambos, percebeu-se que o género masculino centrou-se no “*muito frequentemente*”. Já em relação ao género feminino existiu uma maior variação nas respostas. No que diz respeito a sites de discussão referidos na tabela como “Twitter” e “Reddit”, observou-se que, dos 24,3% do género masculino mais de metade (14,5%) utilizam pelo menos “ocasionalmente” estas redes de conexão, contando a maioria 7,7 em “muito frequentemente”. No que diz respeito aos 75,4% do género feminino, 34,3% nunca utiliza ou não tem, constando a maioria das respostas no “nunca”. Igualmente se verificou no item de jogo e videojogos, em que a maior concentração de inquiridos (35,6%) que responderam “nunca” foi do género feminino. Todos estes dados coincidem com os dados recolhidos na pesquisa mais recente do Pew Research Center. Nesta pesquisa segundo Vogels et al. (2022), os adolescentes do género masculino são mais propensos que o género feminino a usarem o

YouTube e Reddit e têm mais probabilidade de dizer que têm acesso a consolas de jogos e vídeo jogos.

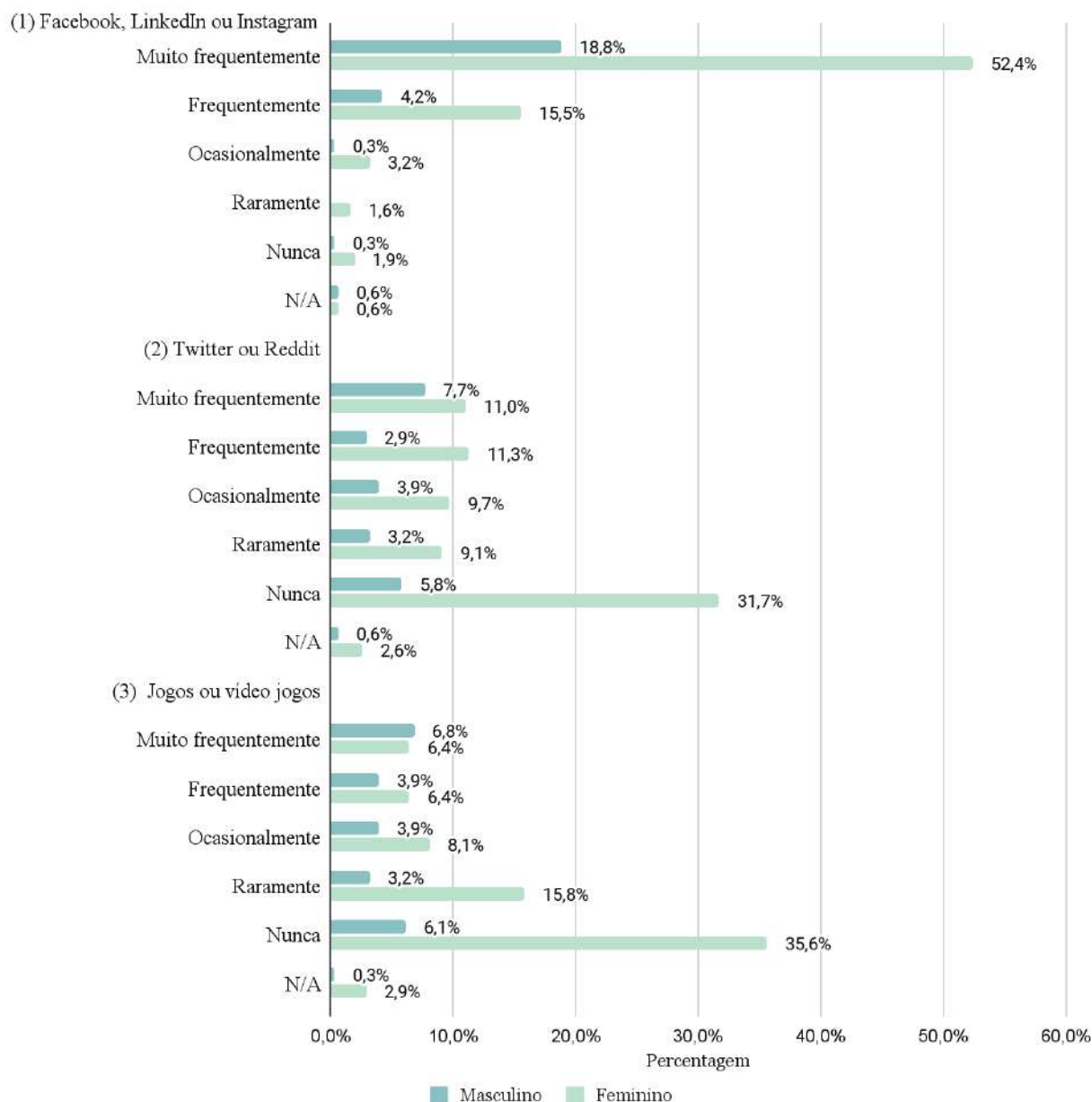


Figura 21: Resultados da frequência de utilização da internet.

Para clarificar, os dados que se seguem foram abordados mais uma vez com base na lente de género (Anexo VI, Tabela 34). Foi questionado aos participantes a frequência da utilização diária de sistemas e de alguns *smart products* (seção 3.2), e agrupados de 1 a 5, respetivamente (Figura 22). Relativamente à “(1) internet e correio eletrónico”, o que se pôde constatar é que, no geral, a maioria dos inquiridos (95,3%) revelam acessar à internet ou o correio eletrónico pelo menos “muito frequentemente” ou “frequentemente” no seu dia-a-dia. Não se revelou

nenhuma surpresa, considerando todo o histórico do crescimento da tecnologia e a dependência cada vez maior abordado no capítulo 2. Indubitavelmente, na utilização de “(2) telemóvel” e “(4) computador e tablet”, 98,3% têm um telemóvel conectado à internet e a maioria das respostas centraram-se na utilização “frequente” destes aparelhos, o que significa que é necessário existir um maior cuidado na análise destes. Com a sua utilização diária e as múltiplas aplicações que existem, torna-se um acesso fácil a abusadores de por meio destes ter controle sobre outros.

No caso “(3) *smartwatch*”, 54,1% do total de participantes afirma ter este *smart product*, mas apenas 26,5% do total refere a sua utilização como “muito frequente”. Por último, no “(5) AirTag”, 63,1% dos participantes respondeu “nunca” sobre a frequência de utilização. Como indicado anteriormente (Capítulo 3), segundo Cole (2022), a Apple lançou o primeiro AirTag em abril de 2021. Isto traduz claramente os resultados de Portugal, visto se tratar de um *smart product* bastante recente no mercado e ainda desconhecido aos olhos da maior parte dos participantes. Nos casos onde se confirmou a posse deste produto, alguns dos casos deviam-se a fatores de proteção como “fui assaltada e agora uso AirTag na minha carteira”. Outros exemplos relatam abuso com esse dispositivo: “uma amiga minha tinha um AirTag dentro do carro, mas ela tinha um Samsung só descobriu porque uma amiga tinha um iPhone e recebeu a notificação que existia um AirTag por perto”. Relativamente a respostas que falavam sobre apresentar queixa sobre este aparelho, nenhuma relatou ter avançado realmente, um dos exemplos foi a resposta: “nunca apresentou queixa porque não descobriu quem lhe fez aquilo e porque tinha um pouco de medo das perguntas que a polícia fizesse”.

Comparando os resultados e correlacionando-os com o tipo de vitimização, percebeu-se que as “vítimas pelo menos uma vez”, relatam utilizar mais a internet que as que nunca foram vítimas. Relembrando que, as “vítimas pelo menos uma vez” fazem parte de 62,8% (n=194) da amostra total, e as “não vítimas” dizem respeito a 37,2% (n=115).

Relativamente a vitimização, analisou-se entre “vítimas pelo menos uma vez” e “não vítimas” a frequência de utilização da tecnologia. Para medir o impacto que esta tem na vida das vítimas, percebeu que, o grupo das vítimas no que diz respeito a redes de comunicação, utiliza muito mais as redes sociais do que os inquiridos que nunca foram vítimas (Anexo IV).

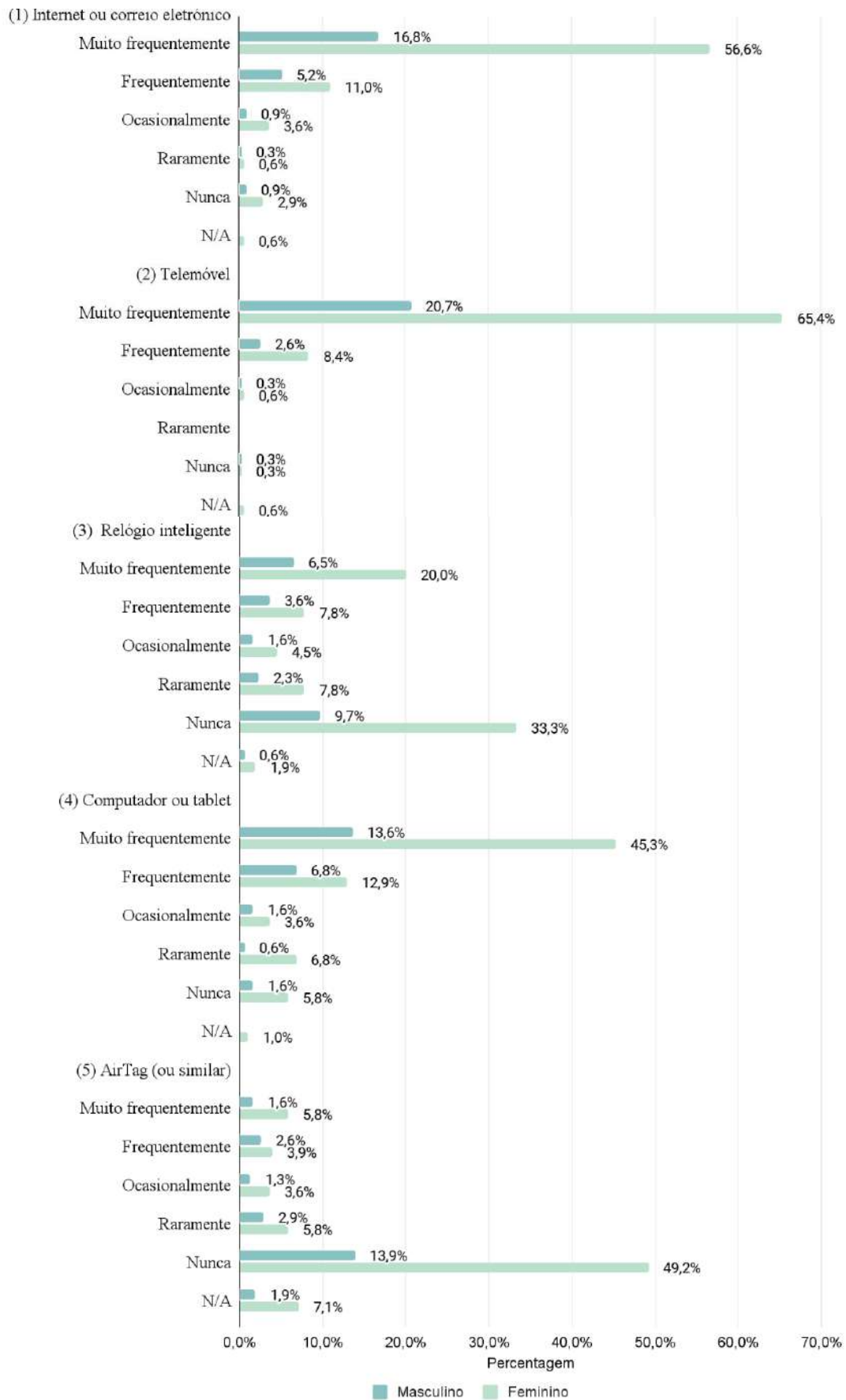


Figura 22: Resultados da frequência de utilização de sistemas e *smart devices*.

A Figura 23 apresenta a prevalência e os géneros diferentes para cada item relativo às formas de monitorizar estudadas. A partir da revisão de literatura, vários autores (Sovacool et al. 2021; Bugeja et al. 2018; Marwick, 2012; Lenhart et al. 2016) afirmaram que:

(H5) Dada a omnipresença da tecnologia, algum grau de vigilância social como o de monitorar podia ser considerado uma parte aceitável nos relacionamentos íntimos. Para validar esta hipótese na questão 15 do questionário foi incluída uma tabela com doze subquestões de escala Likert (5 pontos, discordo totalmente - concordo totalmente). Questionou-se o conforto com a monitorização de sistemas inteligentes.

Observando os resultados, é claro que monitorização é um legítimo componente dos relacionamentos íntimos. Estes resultados mostram uma prevalência nas respostas que se conformam com a monitorização, nos mais variados casos.

Como foi possível observar, a maioria dos participantes mostrasse de facto confortável com a monitorização em alguns casos analisados no estudo. Isto é especialmente notório na “segurança doméstica”, em que 49,5% responderam “concordo totalmente” a estarem confortáveis com a monitorização. Como no caso dos “menstruação e gravidez”, 41,4% está confortável com a monitorização. No “histórico financeiro” com 40,7%, também contém a maioria das respostas em “concordo”, igualmente em “roupa e lavandaria” com 45%, “alimentação e dieta” (40,1%) e “rastrear carros e veículos” (47,2%). Pode-se dizer que apenas nos dados relativos a “rastrear os membros da família” existiu uma maior discordância, o que não interferiu com o resultado.

Outros dados preocupantes, foi relativo a “idosos e doentes” e “crianças”, onde a unanimidade dos participantes mostra que assuntos relativos a estas tipos de população deve ser um foco maior em estudos de monitorização (Vigdor, 2019). Na generalidade, as respostas “discordo” ou “discordo totalmente” foram as menos selecionadas. Estas estatísticas comprovam que as pessoas estão confortáveis com a monitorização.

No entanto, para determinar se veracidade da hipótese 5 e assim determinar se a monitorização é ou não aceitável nos relacionamentos íntimos, seriam necessários dados mais específicos. Poderiam ser incluídas questões mais direcionadas a relacionamentos íntimos.

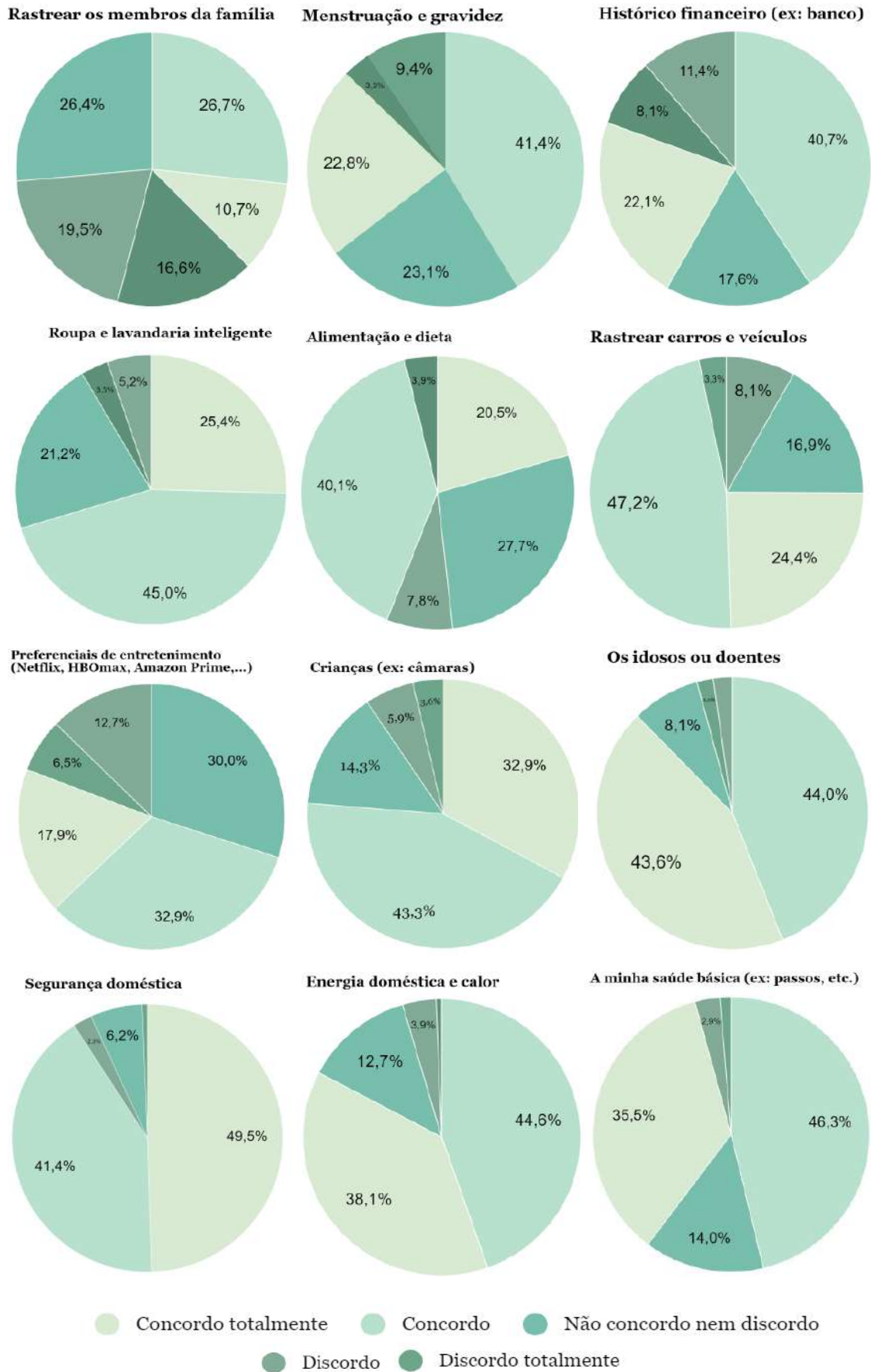


Figura 23: Resultados da questão 15, sobre conforto com a monitorização.

Relativamente à questão 16, dado que não existiu outro método para obter determinadas respostas, decidiu-se optar por analisar entre “vítimas pelo menos uma vez” e “não vítimas”. Para isso foi questionado aos participantes que descrevessem a lista de *smart products* que estes atualmente detêm. Esta pergunta aberta, originou uma lista variada de produtos por participante que ajudou na validação da terceira hipótese. Na Figura 24 é possível observar que no caso da “vítima pelo menos uma vez” a média de *smart products* é visivelmente superior 3,90(0,13; 1; 11), do que a média das “não vítimas” 3,79(0,15; 1; 10). Observando estas conclusões e conciliando com o anterior analisado sobre o tema (seção 2.6), interligando com a frequência de utilização, foi notório que os *smart products* são uma componente legítima para controlo e violência doméstica podendo viabilizar novas formas de violência (Anexo VI, figura x).

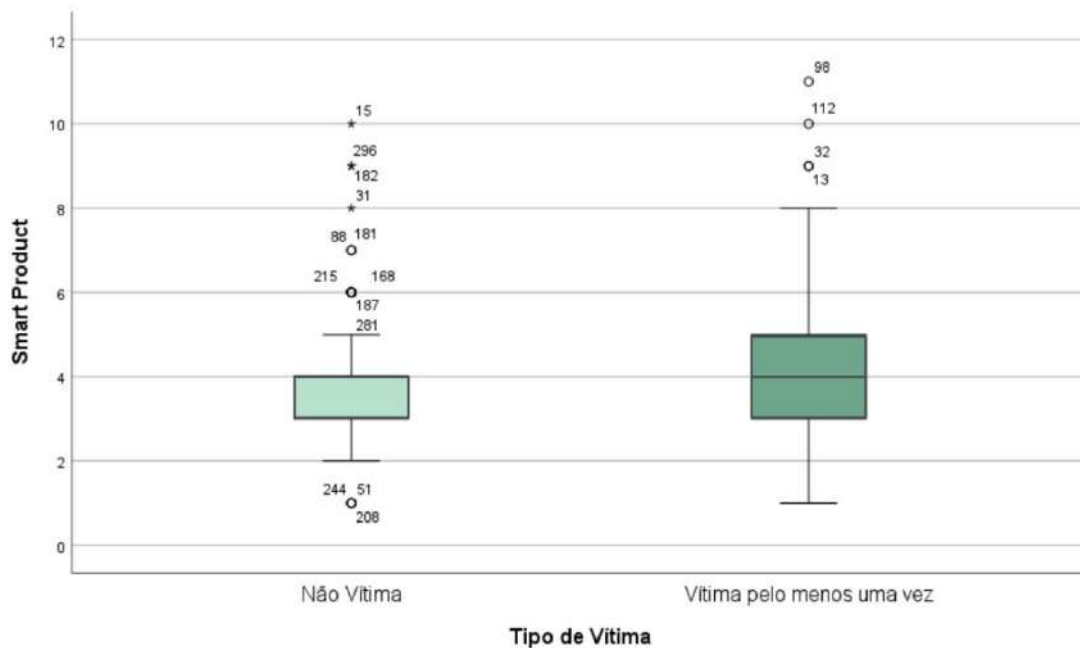


Figura 24: Resultados à pergunta 16, quantidade de *smart products*.

Na Figura 25, foi analisada igualmente a quantidade de *smart products*, desta vez comparando o género masculino, feminino e prefiro não dizer. Percebeu-se que as respostas entre masculino (M=3,96) e feminino (M=3,83) sofrem poucas variações, lembrando que o número de participantes do género feminino (N=233) é visivelmente superior ao masculino (N=75) no questionário. Esperava-se uma margem superior no grupo feminino (Anexo VI, Figura 44). de *smart products* visto que também são uma maioria. Ao contrário do esperado verificou-se que o grupo masculino em média detêm mais *smart products* que o grupo feminino.

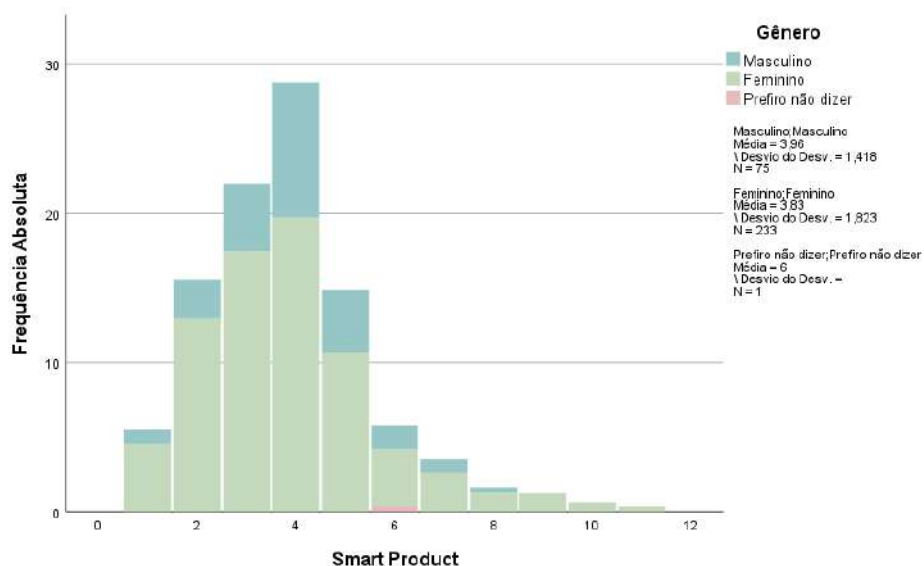


Figura 25: Resultados da média de *smart products* por gênero.

Tendo em conta os dados analisados acima, verificou-se que o gênero feminino que já foi vítima pelo menos uma vez é largamente superior ao do gênero masculino, considerando a revisão de literatura (Capítulo 2) a mulher sofre mais vitimação, pelo que esta estimativa de resultados vem a reforçar o concluído em estudos anteriores.

H4) Existe uma maior taxa de prevalência em vítimas de tecnologia do gênero feminino do que masculino. Apesar do gênero feminino ter um maior número de vítimas (N=233), o gênero masculino (N=75) por sua vez tem vindo a ganhar espaço no campo da vitimação com o passar dos anos, podendo dever-se ao facto de que atualmente os meios de comunicação de apoio à vítima têm sofrido avanços significativos a nível de inclusividade, e rápida resposta, o que antigamente não acontecia, necessitando a vítima de se dirigir a um posto da polícia em caso de emergência, o que não era igualmente visto pela sociedade (secção 2.5).

Mesmo assim, observando as conclusões, tanto na análise dos questionários como na revisão de literatura foi possível perceber na Figura 26, onde as barras de erro indicam intervalo de confiança de 95%, mostram que para todos os efeitos é evidente que o gênero feminino com 46% (N=142) e o gênero masculino com 17% (N=52) participantes inseridos em “vítima pelo menos uma vez”, tem uma taxa de prevalência na violência tecnológica superior ao gênero masculino.

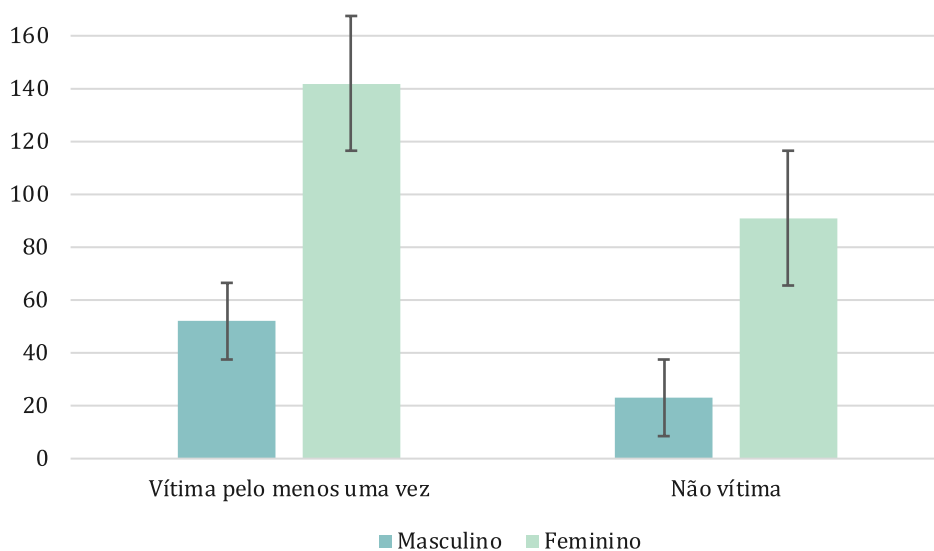


Figura 26: Resultados de gênero sobre o tipo de vítima.

Seção 3. Privacidade pessoal: Segundo Lenhart et al. (2016), a invasão da privacidade pessoal causa danos às vítimas, através do acesso não autorizado aos seus pertences ou exposição de informação pessoal. Ainda refere que estas experiências incluem: ser hackeado, ter informações ou imagens da pessoa expostas online sem sua permissão, alguém fazer-se passar pela pessoa, ser monitorado e ser rastreado online.

A questão 17 do questionário é referente a possíveis acontecimentos em ordem de frequência, praticados pelo participante para se proteger online. Esta questão foi analisada com base no critério de análise “vítima pelo menos uma vez” e “não vítima”. Este resultado refletiu que os participantes que já foram vítimas pelo menos uma vez tomavam mais medidas de proteção, como é o caso da Figura 27. No primeiro gráfico sobre dar informação falsa ou inexata para proteger a privacidade pessoal do participante, percebeu-se que as vítimas tinham mais frequência em tomar esta atitude do que as não vítimas. Este padrão de resposta repetiu-se nos exemplos seguintes (Anexo VI). Na coluna do “nunca”, é notória em todos os exemplos uma superioridade para as “não vítimas”. É relevante ainda referir que se percebe que a opção “mais de 5 vezes” teve sempre uma aglomeração bastante elevada de respostas.

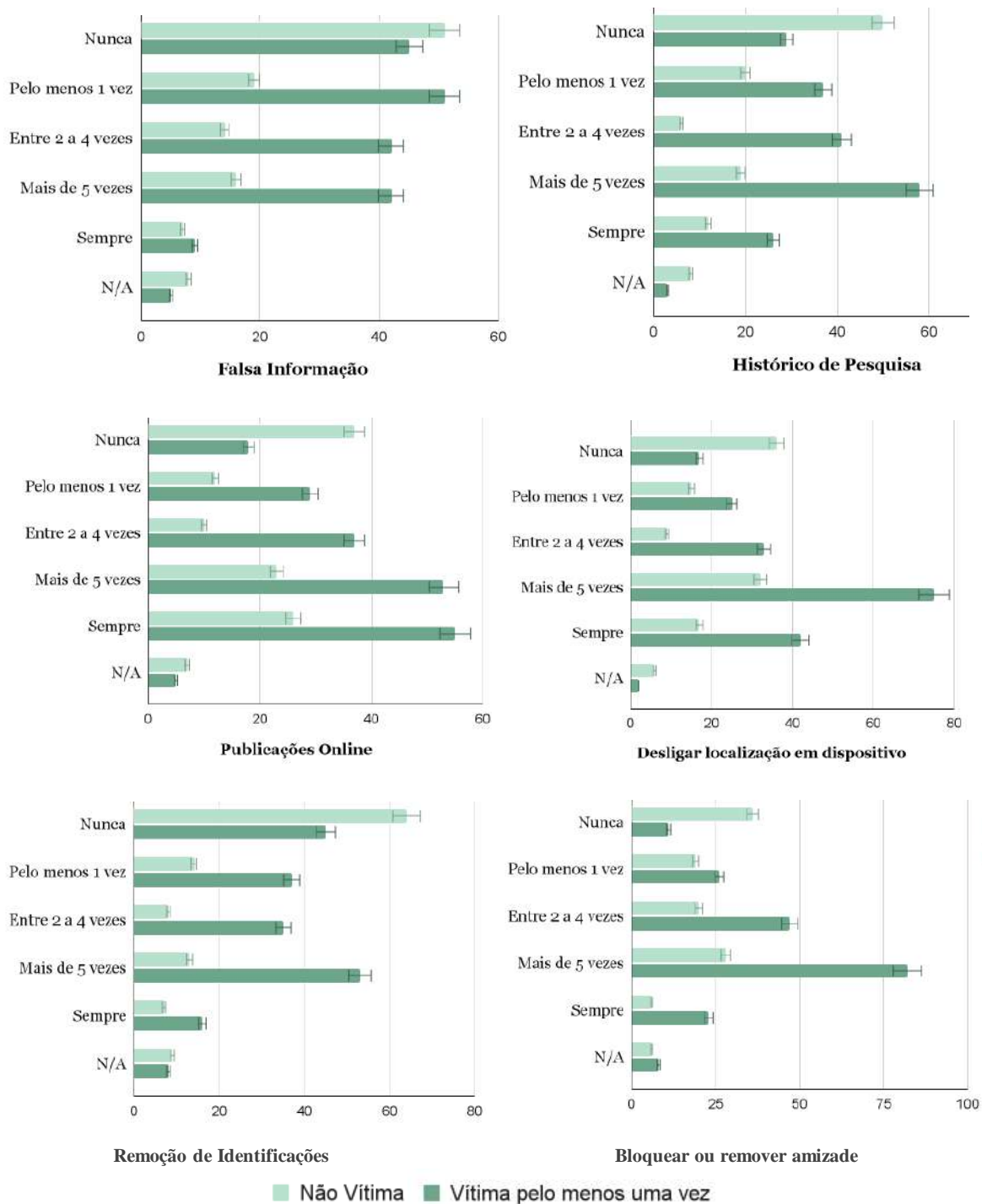


Figura 27: Resultados questão 17, privacidade pessoal.

As questões 18 e 19, não constaram na análise dos resultados, pois percebeu-se que, nas questões em que era perguntado diretamente quem era o praticante de abuso, as respostas eram maioritariamente “nunca”, sendo que, os dados recolhidos não foram suficientes para se obter uma conclusão sobre eles.

Seção 4. Abuso Tecnológico: Para se analisar os padrões e características das vítimas de abuso desenvolveu-se a questão 20 que, por sua vez, foi retirada da análise, pois não demonstrou a quantidade de respostas que se esperava (Anexo V, secção 4) para responder à pergunta e objetivos de investigação. Por essa razão, a resposta a esta conta apenas nos anexos IV. Segundo Lenhart et al. (2016), para entender melhor o abuso é necessário perguntar que tipo de comportamentos de assédio ou abuso elas testemunham. Para isso, selecionou-se os padrões de abuso mais comuns (Lenhart et al. 2016 and Sovacool et al. 2021), para se identificar a violência facilitada pela tecnologia. Daí foram solicitados a identificar quem era o perpetrador desse abuso.

A questão 21 mediu o risco de sistemas de rastreamento GPS serem intrusivos, na Figura 28. As barras de erro indicam intervalo de confiança de 95% e mostram que a maioria dos respondentes concordou com esta afirmação, tanto no género feminino como no masculino. Uma parcela muito pequena dos respondentes referiu que discorda com a afirmação ou que discorda totalmente (Anexo IV). Para a validação de (H6), “o género influencia a tolerância e confiança ao risco de *smart homes* e tecnologias domésticas inteligentes”, mediu-se a concordância e discordância do risco da percepção dos géneros.

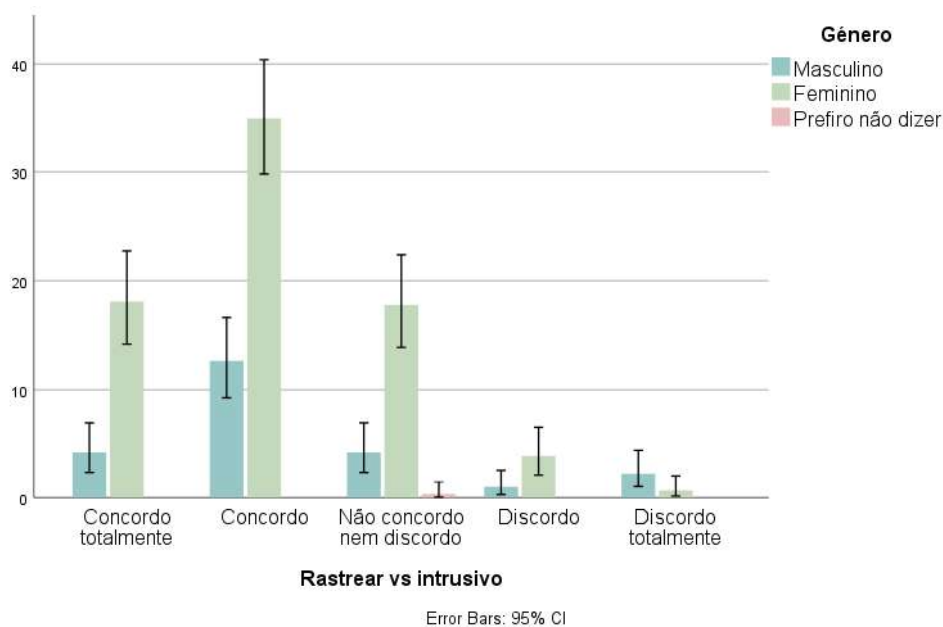


Figura 28: Resultados do questionário em SPSS, rastrear é intrusivo.

Seção 5. Impacto do Abuso: Entre as vítimas de abuso tecnológico, 58 usaram pelo menos uma estratégia de proteção. Algumas das vítimas desconectaram-se da internet, redes sociais ou telemóvel como efeito colateral do abuso. Segundo Lenhart et al. (2016), o assédio e abuso

podem ter consequências em isolamento ou desconexão dos aparelhos e internet, geralmente pela tensão que esse abuso colocou no relacionamento íntimo. A questão 22 (Anexo IV) apresenta em todos os exemplos a maioria dos resultados na opção “nunca”, então não se mostrou pertinente analisar, pois o resultado não traria nenhuma novidade ao estudo.

Seguiu-se então a análise da questão 23 (escala likert de 10 pontos, 1- discordo totalmente, 10- concordo totalmente), referente a deixar de publicar algo online pela preocupação da possibilidade de ser rastreada a localização devido a essa publicação. Percebeu-se, na Figura 29, que a predominância de respostas “concorda completamente” com a questão. Por essa razão, foi possível aferir que mais uma vez existe este receio ligado à segurança, privacidade e gerenciamento de dados (Bugeja et al. 2017).

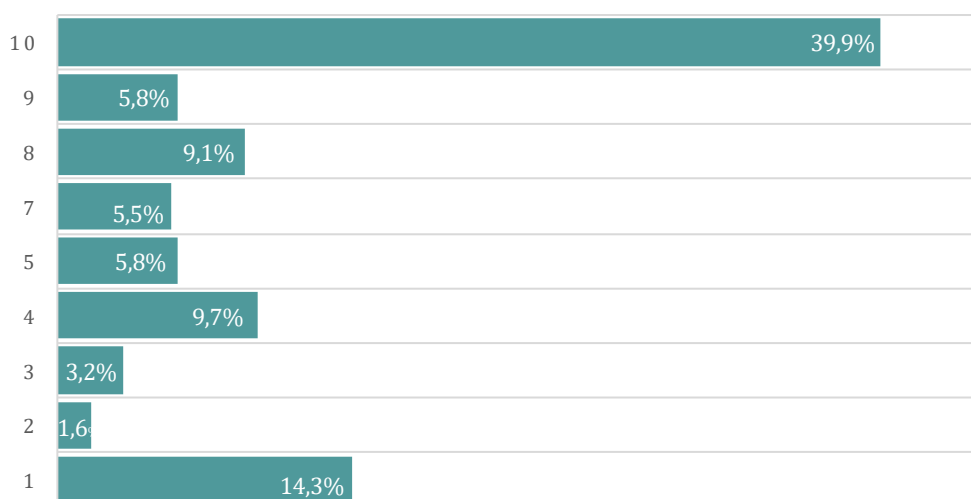


Figura 29: Preocupação de que seja rastreada a localização ao fazer uma publicação.

Nas restantes questões de resposta aberta, nomeadamente a 24 sobre vitimização digital guiou grande parte do estudo na escolha de analisar entre “vítima pelo menos uma vez” e “não vítima”. Já na 25, foi questionado aos participantes sobre acontecimentos e histórias suas ou de alguém que conheciam acerca de violência física.

Observou-se, por exemplo, um participante do género masculino com 47 anos e residente no Porto. Após relatar vários acontecimentos como vítima de abuso tecnológico numa relação anterior no questionário, este admitiu na pergunta 24 que: “Sim, uma ex-namorada clonou o meu telemóvel para aceder às minhas conversas e devido a isso foi o fim do relacionamento”. Até então, o participante parecia tratar-se apenas de uma vítima, mas na resposta da questão 25, este respondeu: “Sim, a minha ex-namorada clonou o meu telemóvel e eu quando descobri espetei-lhe um par de chapadas no focinho e de seguida tentei-a estrangular até ela perder os

sentidos, mas felizmente para mim ela sobreviveu”. Percebeu-se então que este abuso tecnológico terminou em agressão. Pode tratar-se de um ato único, mas é perceptível pela resposta dada pelo respondente que poderia ter terminado tragicamente. Este participante tinha um total de 6 *smart products*, nomeadamente, campainha inteligente, telemóvel, termostato, tablet, computador e carro. Nos restantes dados analisados da questão 24, observou-se mais 6 inquiridos que também referiram que pessoas próximas a eles lhes tinham clonado o telemóvel. Em dois desses casos, descobriram ainda existir um chip no carro para rastrear a localização. Sabe-se também que, é possível muita gente estar a ser monitorizada e não ter descoberto ainda. Nem todas as histórias relatadas na violência física se deviam a relacionamentos entre casais. Por exemplo: “Sim, já agredi um homem que estava a assediar a minha atual esposa. Ele foi para o hospital e esteve 3 meses em coma porque lhe dei muitos socos, pontapés na cabeça e parti-lhe as costelas”. As respostas foram as mais diversas, constando, nos Anexos V, as principais analisadas ou várias vezes repetidas.

4.4 Resultado

Esta seção foi dedicada a compreender a perspectiva das vítimas. Com base nos resultados, podem ser tiradas várias conclusões relativas aos efeitos da tecnologia sobre a violência doméstica.

As conclusões desta secção indicaram que os *smart products* afetam negativamente o controle e abuso doméstico. A preocupação com futuros produtos tecnológicos ficou clara nos participantes, que relataram o “controle abusivo” e “a insatisfação na proteção de dados” como algo a melhorar. Por conseguinte, os *smart products* não podem ser considerados apenas uma questão individual porque a redução da sensação de segurança dos utilizadores tem efeito direto na confiança ao utilizar os produtos.

Como forma de responder à questão de investigação, quatro hipóteses foram consideradas nesta seção: (H3) Os *smart products* atuam como potenciais viabilizadores de controle e violência doméstica. (H4) Existe uma maior taxa de prevalência em vítimas de *smart products* do género feminino do que masculino. (H5) Dada a omnipresença da tecnologia, algum grau de vigilância social como o de monitorar pode ser considerado uma parte aceitável dos relacionamentos íntimos. (H6) O género influencia a tolerância e confiança ao risco de *smart homes* e tecnologias domésticas inteligentes. Foi possível identificar duas das quatro como totalmente validadas, enquanto as outras duas foram parcialmente validadas.

De todos os produtos analisados, os produtos domésticos foram os mais citados como viabilizadores de violência. Como em média 7 em cada 28 participantes têm este tipo de *smart*

products e foram vítimas pelo menos em algum momento, pode-se inferir que os *smart products* são facilitadores para gerar controlo abusivo e conseqüentemente violência.

Apesar de várias questões terem sido mal compreendidas ou não terem uma resposta esperada, o questionário cumpriu o seu papel. Os resultados das questões abertas, presentes igualmente no questionário, serviram de portal para o estudo de cenários possíveis, observando o design especulativo como base. O designer tem o papel de intervir, para obtenção de uma leitura completa dos factos, dados e ameaças futuras.

CAPÍTULO 5 | Design Especulativo e Cenários Possíveis

5.1 Introdução

O objetivo deste capítulo é entender como o design especulativo, abordagem que aproxima design e ficção, pode ajudar a refletir sobre a realidade. Para isso, o capítulo inclui observações de design especulativo como ferramenta que contribuiu para a metodologia de construção de cenários, onde possíveis realidades ficcionais exemplificam situações de *smart products* na violência doméstica, baseadas nas respostas à pergunta aberta 24 do questionário (Anexo IV, seção 5).

DiSalvo (2012) define design especulativo como a utilização do design para demonstrar a previsão de maneiras convincentes, tanto muito provocativas por vezes, com intuito de envolver o público em considerações sobre o que poderia ser. Observou-se a conveniência de pensar como o design especulativo poderia de algum modo significar mais do que ser usado para provocação, para permitir um envolvimento mais significativo com o assunto abordado do problema. Apesar da resolução de problemas ser o aspecto central design, para os pesquisadores Dunne & Raby (2013), especular através do design abre espaços dinâmicos entre futuros possíveis e futuros preferíveis, onde cenários retratam situações do cotidiano que podem tornar-se um impulsionante catalisador para debate público.

5.2 Os Princípios de Design Especulativo na Investigação de Design

Em *Speculative Everything*, Anthony Dunne e Fiona Raby, designers e pesquisadores, dominadores do “design crítico” no final de 1990, propõem um tipo de design que é usado como uma ferramenta para levar à discussão reflexiva a ao debate sobre valores culturais dominantes (Dunne e Raby 2001). Já no início dos anos 2000 e 2010, o termo que outrora tinha o nome de “design crítico” alterou para “design especulativo”, argumentando se tratar de uma prática que usa artefactos de design para explorar futuros alternativos possíveis e plausíveis, de forma a gerar discussões do que seria um futuro preferível tornando visível tudo aquilo que era invisível e perdido na familiaridade do cotidiano (Malpass, 2016).

Para Dunne and Raby (2013) o design é visto como um meio de especular sobre como as coisas poderiam ser ao imaginar possíveis futuros. Embora muitas vezes esteja voltado para o futuro, não se trata de prever o futuro, mas sim provocar reações, serve para fazer perguntas sobre política e nas configurações sociais, econômicas e tecnológicas que atualmente se vivencia e assim criar um mundo subjacente à sua representação atual (Wong & Khnovaskaya

2018). Essas ideias libertadas pelo design especulativo aumentam as probabilidades de alcançar futuros desejáveis. Dunne and Raby (2013) utilizam "e se" nas perguntas destinadas a abrir os debates e a discussão sobre o tipo de futuro que as pessoas desejam (e não desejam). O'Regan (2020) acrescenta que, apesar da necessidade de percorrer sistematicamente o espaço que se pode desenrolar, para desenvolver um ponto de vista sobre os tipos de futuros que se deseja.

Para Dunne and Raby (2013), ao se especular mais sobre toda a realidade, torna a realidade futura mais maleável. Conceberam então um modelo representado no Figura 30, para considerar cenários potenciais para o futuro. De modo que, Voros (2001) mostra que os cones concêntricos representativos à expansão das possibilidades com a passagem do tempo podem ser representados com diferentes tamanhos. O cone mais largo, "*possible futures*", é limitado apenas pelo que é imaginável e pode até transgredir as leis da física. O seguinte, "*problable futures*", retrata as extrapolações mais viáveis das tendências existentes, ou mesmo, as delimitações do atual entendimento e competência. Segue-se o mais estreito, "*plausible futures*", que representa novas práticas sociais ou descobertas científicas. Dunne e Raby (2013) delimitam uma área centrada com cor mais escura que pode oferecer "*preferable futures*", segundo Voros (2001), opiniões emocionais e baseadas em juízos de valor, já que se trata de uma área de articulação da desejabilidade. Quando se trata do futuro, existem muitas partes móveis e muitas incógnitas. O design especulativo não é apenas sobre futuros preferíveis.

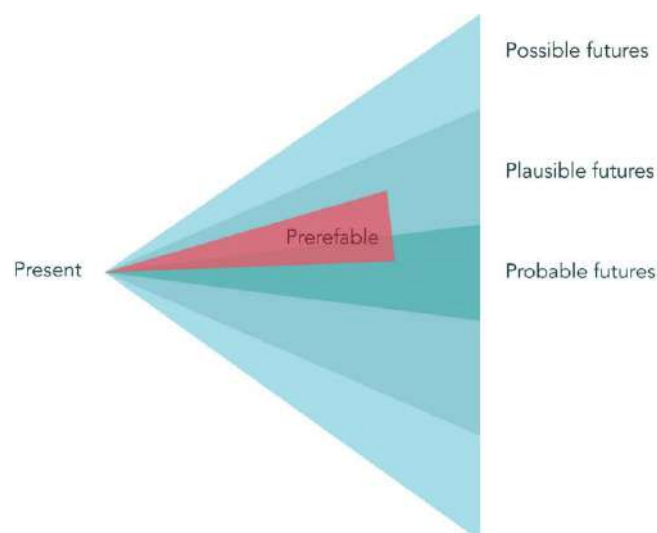


Figura 30: Diagrama PPPP de futuros potenciais (Dunne & Raby, 2013).

Ao explorar-se futuros especulativos, é fornecida uma nova abordagem detalhada sobre quais futuros não são desejáveis. Essa demonstração, chama a atenção explicitamente, o que permite antecipar situações e tomar ações corretivas e evasivas (O'Regan, 2020). O autor ainda

refere que, no meio da incerteza, muitos designers operam no provável a menos que aconteça alguma causa externa.

É neste contexto que a investigação explora a utilização de respostas provenientes dos questionários (Capítulo 4) e aplica as suas representações como futuros possíveis que podem não ser realistas no momento. O design especulativo utilizou ferramentas e metodologias de design, os cenários, juntamente com a técnicas, a revisão de literatura para criar provocações ou 'elementos narrativos para prever e explicar possíveis futuros para o design' (Tanenbaum et al., 2012).

Estes cenários são criados pela combinação de elementos realistas e imaginativos. O design especulativo permite imaginar possibilidades, enumerar o potencial de resultados e o que é importante ter em conta eticamente. O design especulativo, obriga a pensar mais além, com o intuito de “reflexão e crítica”. De acordo com Dunne e Ruby (2013), o foco deixa de estar na arquitetura, produtos e ambiente, e passa a destacar leis, ética, sistemas políticos, sociais crenças, valores, medos e esperanças, traduzidos a expressões materiais, tornando-se pequenos pedaços de outra realidade. Os autores defendem que a criação de cenários que tecem o filosófico, social e tecnológico em conjunto num só, pode acrescentar uma camada adicional de credibilidade (Dunne e Ruby, 2013).

Instrumentalizar a elaboração especulativa de maneira a que se preste procedimentos adicionais e experiências pode ser desafiador (Bleecker, 2009). No entanto, Johannessen, Keitsch, & Pettersen (2019) apresentam um procedimento de três passos a considerar em qualquer conceção especulativa e crítica:

- 1 - Definir um contexto a debater: A maioria dos cenários que utilizam design especulativo giram em torno de um tópico. Tipicamente, os tópicos são questões éticas criadas por questões que, neste caso concreto, são sobre de tecnologia emergente ou normas sociais (Johannessen et al., 2019).
- 2 - Idealizar, encontrar problemas, e criar um cenário: A utilização do método "e se", popular para se idealizar e imaginar problemas que servem como a ideia principal de um cenário.
- 3 - Materializar o cenário: Envolve transformar o cenário em narrativas, objetos ou uma combinação de ambos (Johannessen et al. 2019). Este tem de ser de elaborado com detalhes, a fim de se conseguir algum tipo de veracidade.

Johannessen et al. (2019) refere que, uma vez que o papel do design especulativo é suscitar comportamentos e pensamentos que ajudem as pessoas a pensar e a reconsiderar o que

antes poderia ser normalizado, precisa-se que os cenários permaneçam em aberto, sejam pouco claros e até complicados, compondo-os com provocações usando humor negro e sátira.

5.3 Design Especulativo nas Preocupações de Privacidade

Embora muitas vezes os *smart products* sugiram futuros conectados, chamativos, e mais seguros, analisar os *smart products* como artefactos especulativos ajuda a trazer à tona aspetos das narrativas encontradas nas respostas dos questionários que podem não estar em seu foco central, mas podem ter implicações significativas para os utilizadores se essas situações continuarem a acontecer (Wong & Khnovaskaya, 2018). Por exemplo, na análise benchmarking (Capítulo 3), a análise crítica dos dispositivos listados sugere que várias das características encontradas nos *smart products* constroem uma falsa ilusão de privacidade (Messing et al. 2020). Há, portanto, a necessidade de abordagens que permitam e facilitem uma visão sobre as complexidades da privacidade e segurança, assim como a medição das perceções dos utilizadores, utilizando o design especulativo sobre as potenciais decisões morais decorrentes da intervenção tecnológica que os *smart products* poderiam estar a submeter no futuro. Cada vez mais, estes produtos tomam lugar num “ideal” lar inteligente, e ao mesmo ritmo cresce também as preocupações com a privacidade dos utilizadores.

Vários estudos documentam preocupações de privacidade e segurança em torno de rastreio, altifalantes inteligentes e observam que os utilizadores têm vindo a trocar a privacidade por conveniência em diferentes níveis (Lau et al. 2018).

Além disso, a vigilância omnipresente é relatada por vários autores (Belknap, Chu e DePrince, 2012; Dimond et al. 2011 ; Finn e Atkinson, 2009 ; Southworth et al., 2007 ; Woodlock 2017 ; Zaidi, Fernando & Ammar, 2015) como consequência da utilização de redes sociais, mensagens de texto e telefonemas. Esta vigilância omnipresente torna-se assim cada vez mais fácil para o parceiro/a íntimo/a, reunido com novas tecnologias que se conectam a dispositivos, como sistemas de segurança doméstica, assistentes domésticos conectados à Internet (Messing et al. 2020), que arquivam e compartilham dados on-line.

5.4 Cenários Possíveis

Com uma combinação de ficção de design, histórias e cenários, pode-se essencialmente fazer perguntas mais profundas e pontuais sobre o papel potencial das tecnologias utilizadas atualmente. Esse ponto de vista molda-se através do que se pode e deve fazer para que aconteça. Para tal, foram reconhecidas situações em que a tecnologia dos *smart products* muitas vezes

necessitam de acesso à localização ou informações pessoais, para o produto ou aplicação funcionar.

Os cenários explorados procuram compreender as interações humanas e utilizador/objeto, uma vez relacionadas à privacidade. O primeiro cenário procura relatar a experiência teórica de uma aplicação fantasma. O cenário é aberto à interpretação, como seria esta situação no mundo real passada entre duas pessoas, demonstrando que uma monitoriza todas as ações da outra através de uma aplicação fantasma. Especificamente este primeiro cenário inclui situações de tensão e controlo abusivo. Procura compreender os utilizadores, a falta de experiência tecnológica ou a aceitação de ações específicas podem orientar a discussão. Isto pode implicar mais do que oferecer escolhas. É mais sobre como essas aplicações funcionam e como são detetadas.

Cenário 1: Aplicações *Stalkerware*

Problema: Aplicação camuflada que regista as conversas, localização e todas as ações efetuadas no dispositivo móvel (baseado em Chen, 2021).

Necessidades do utilizador: Privacidade de dados.

Contexto: Por insegurança e ciúmes por parte da namorada de 30 anos, o casal teve uma forte discussão (Figura 31). Mais tarde, nessa noite, fizeram as pazes, conversaram e resolveram ir para casa dele dormir. Ainda pensativa e inconformada com a situação, sem acreditar nas palavras do namorado, decide aproveitar que este está a dormir e desbloqueia o seu iPad, através da impressão digital. De seguida, instala uma aplicação *Stalkerware*, que pelo facto de esta estar camuflada de calculadora, concede-lhe o total acesso ao iPad e, sucessivamente, todas as aplicações em comum com o telemóvel do seu parceiro sem que este se aperceba de nada. Esta aplicação “invisível” fornece toda a informação privada existente no telemóvel como, por exemplo, a localização precisa, o histórico de navegação, as fotos, as mensagens, bem como o registo, gravação de chamadas e acesso à câmara (Whittaker, 2022). Durante algum tempo, começa a monitorar o parceiro e decide confrontá-lo com o que viu. Após semanas de acusações feitas pela parceira, este começa a ficar desconfiado de toda esta situação e fica assustado. Não sabe como a sua parceira sabe tanto dos acontecimentos mais recentes sem que lhe tenha contado e mesmo após alterar várias vezes as suas palavras-passe.



Um casal discute por problemas de insegurança e ciúmes por parte da namorada.



A namorada pede desculpa, fazem as pazes e dorme na casa do seu parceiro.



Pensativa e sem acreditar no parceiro, desbloqueia o iPad e instala uma aplicação *Stalkerware* disfarçada.



Nas semanas seguintes, monitora a localização e vê as mensagens trocadas pelo parceiro com outras pessoas.



Decide confrontá-lo com informações que viu na aplicação.



Fica assustado e surpreendido como a namorada sabe tantas informações privadas dos últimos tempos.

Figura 31: Cenário dedicado a aplicações *salkerware*.

Solução: Existem muitos métodos para detetar estas aplicações, mas apenas detetá-las não resolve o problema. Estas “aplicações para ciumentos” são um universo cada vez mais comum.

O uso de soluções de proteção torna-se essencial: proteger o telemóvel com palavras-passe e não partilhar com ninguém, alterar palavras-passe de todas as contas, fazer download de aplicações apenas de fontes oficiais, como *Google Play* ou *App Store*. Em caso de já estar a ser vítima, ao tomar estas atitudes ou desinstalar a *app* pode estar a dizer ao abusador que sabe e colocar-se em perigo. Neste caso, o mais indicado seria a troca de telemóvel e aí sim tomaria todas as medidas de proteção e procurar ajuda junto de entidades competentes. Existem softwares de segurança, porém é importante lembrar que um *software* de segurança não pode atuar como uma “solução” universal para quem acredita já ter o *stalkerware* instalado nos seus dispositivos.

Cenário 2- iRobot

Problema: Aplicação permite ativação do iRobot longe da habitação, mesmo quando outros utilizadores estejam em casa e não queiram que este seja ativado

Necessidades do utilizador: Privacidade

Contexto: Enquanto os filhos do casal estão na escola e só regressam a casa no fim da tarde, junto com o pai, a mulher aproveita para recuperar algum sono perdido, visto que saiu mais cedo do trabalho (Figura 32). Está então decide avisar o marido de tal para não ser perturbada. Adormece, mas cerca de 30 minutos depois, é acordada repentinamente pelo barulho do iRobot a funcionar, sem que ela lhe tenha dado permissão para tal. Sem perceber como isso aconteceu, e assustada, desliga-o, mas com a sensação que ultimamente tem ativado coisas e não se lembra. O marido vê na aplicação que ela desligou o aparelho e percebe que conseguiu atormentar o seu descanso e volta a ativar o robô para uma hora depois.



Animada, envia mensagem ao marido a dizer que vai descansar, pois saiu mais cedo do trabalho.



O marido, ainda no trabalho, decide ligar o iRobot, para atormentar a mulher, sem que esta saiba.



A mulher começa a ouvir um barulho e acorda.



Zangada e assustada, não entende como o robô de limpeza se ligou.



Pensou que ela mesma teria agendado uma limpeza para aquela hora e tanta desligar o robô.



O marido vê na aplicação que o iRobot se encontra desligado. Ao perceber que conseguiu atormentar, este volta a programar o robô para as próximas horas.

Figura 32: Cenário dedicado a iRobot.

Solução: A possível solução encontrada para este cenário passa por, quando existirem duas ou mais pessoas com acesso à mesma aplicação, a própria aplicação ter acesso à localização para

saber quem está em casa. Se não estiver ninguém em casa, automaticamente o aspirador robô aceita a ordem e, se estiver alguém em casa, primeiro envia uma notificação a esse utilizador a dizer que tal utilizador da conta está a ordenar uma ação e pergunta se aceita ou não ativar. Por exemplo, relativamente ao caso exposto, o problema do controlo e confusão da vítima podia ser resolvida ao ser possível: 1) quando alguém fora de casa (com telemóvel na aplicação) tenta ativar o robô, 2) a aplicação envia notificação ao utilizador que estiver em casa (no caso do cenário acima seria enviaria uma notificação para a mulher), a pedir aceitação de ordem de ativação e refere quem está a pedir essa ação (no caso em que a mulher se encontrava a dormir possivelmente com o telemóvel sem som, esta receberia a notificação a dizer que o seu marido estava a querer ligar o dispositivo doméstico de aspiração, mas esta não aceitaria a ativação e este não se ligaria sem essa permissão). 3) Assim, quem tentou ativar o aparelho recebe uma notificação a dizer: "iRobot não tem permissão para avançar". Desta forma, quem tenta ativar fora da habitação nunca percebe se a ação foi rejeitada ou cancelada.

Cenário 3- Luzes inteligentes

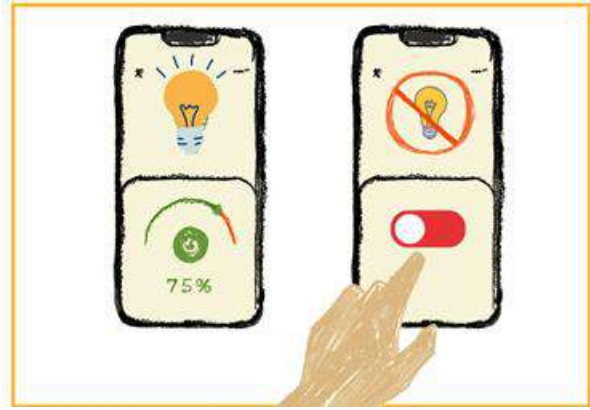
Problema: Aplicação que gere as luzes inteligentes da casa tem o mesmo servidor para todos os utilizadores.

Necessidades do utilizador: Privacidade

Contexto: Baseado em Moog (2019), no vídeo *World Design Organization*. Uma família de 3 pessoas, um casal e uma criança, mudaram-se para uma casa inteligente. Tudo parecia mais fácil, pois tudo era automático, tal como as luzes. Facilitava muito o dia a dia, pois um dos elementos do casal trabalhava mais em casa, a mulher. Com estas luzes, era possível escolher a cor e serem ligadas e desligadas, mesmo fora da casa através de uma aplicação que todos tinham acesso (Figura 33). Um dia, estava apenas a senhora em casa e as luzes apagam-se todas. Ela acha estranho e volta a acender. Novamente voltam a apagar-se. A situação repete-se e este começa a pensar que tem algum problema a casa, porque as luzes não ficam acesas mais que 5 minutos. Esta envia uma mensagem ao marido, a explicar todo o sucedido e este diz-lhe que ela não percebe nada de tecnologia e que o problema é dela, não são as luzes.



Um dia, um casal muda-se para uma casa inteligente. A mulher está sozinha em casa na sala, a ver um filme no fim da tarde.



O seu marido através da aplicação comum da casa desliga as luzes.



Fica admirada e com medo pois está sozinha. Apercebendo-se que já não é a 1ª vez que ocorre.



Volta a ligar, mas desligam-se novamente e esta vai até ao interruptor porque pensa que a aplicação está com algum problema.



O abusador vê na aplicação que as luzes estão ligadas novamente e volta a desligá-las.



Confusa manda mensagem ao marido a explicar a situação. Este aproveita a situação que criou, para a insultar.

Figura 33: Cenário dedicado às luzes inteligentes.

Solução: Notificações instantâneas enviadas apenas aos utilizadores que estiverem dentro de casa, outro tipo de solução seria haver contas diferentes de utilizador e dar para ver qual conta

está a controlar a casa caso, neste caso a apagar e acender as luzes. Isto invalida o facto de o marido poder insultar gratuitamente a sua esposa e querer que esta comece a pensar que realmente não percebe nada e que o problema é ela. Ao conseguir saber quem estava a provocar estas situações na casa para a perturbar, conseguia desta forma obter “provas” para apresentar uma denúncia.

Cenário 4: Rastreador de localização

Problema: O ex intrometido (baseado em, Fleishman, 2021).

Necessidades do utilizador: Privacidade

Contexto: Um ex-casal que aparentemente terminou o relacionamento de 2 anos cordialmente, (Figura 34) quando um dos membros deste casal, saía de casa para encontrar um amigo, ir a um café, ou até fazer compras, começou a ficar farto de situações em que o seu ex aparecia convenientemente em intervalos regulares em várias partes da cidade.

Após vários encontros “acidentais” este considerou estar a ser perseguido, e por isso pesquisou online sobre possíveis métodos de rastreamento, onde verificou que o seu iPhone poderia estar a ser rastreado. Mas entre a análise feita, parecia não ter sido *hackeado*. O seu ex aparecia mesmo quando deixava o seu telemóvel em casa e levava apenas o *Apple Watch*. Ao fim das semanas, com situações parecidas, foi ao trabalho de uma amiga sua, que não via há muito tempo e contou-lhe sobre esses episódios. Após esta conversa apercebem-se que este só se esbarrava com o seu ex apenas quando conduzia para algum lugar. Com a ajuda sua amiga vasculharam o carro e acabaram por encontrar um Air Tag escondido na placa da matrícula.

Ambos ficaram bastante assustados, após ler no site da *Apple*, achou que já deveria ter sido notificado e que o aparelho localizador certamente já teria emitido sons em vários momentos, contudo, depois de analisar as configurações do seu iPhone, apercebeu-se que a função *Find My* estava desativada pois não gostava da ideia de participar de uma rede de rastreamento global, (desativou através do: “*Find My Network em Configurações > Nome da Conta > Find My > Find My iPhone*” (Baseado em Fleishman, 2021). Essa escolha significava também que o iPhone não monitorava AirTags que viajassem com ele. Com essas informações, ficou com bastante medo e assustado por não conseguir anular o ex-parceiro, temendo pela sua própria vida e pelos episódios seguintes.



Enquanto fazia compras tranquilamente, assustou-se ao ver o seu ex pela terceira vez consecutiva na mesma semana.



Preocupado por pensar estar a ser vigiado pesquisa em vários sites, para saber se tem o seu telemóvel *hackeado*, e percebe que não está.



Decide ir ao trabalho da amiga contar o que se andava a passar, mencionando que mesmo deixando o telemóvel em casa, eles cruzavam-se.



A amiga ao ouvir a história fica perplexa e os dois percebem que possivelmente estaria a ser rastreado com algum dispositivo de localização.



Decidem procurar no carro e encontram um AirTag escondido atrás da matrícula.



Fica assustado ao aperceber-se da situação em que se encontra e desespera por não saber o que fazer.

Figura 34: Cenário dedicado a rastreadores de localização.

Solução: Para situações em que o próprio produto já é um problema, pois foi criado para rastrear, seria necessário repensar no produto como algo a melhorar. Tendo em consideração a

privacidade do utilizador a solução para este problema passaria por ser obrigatório, em todos os rastreadores de GPS, serem compatíveis com iOS e Android, primeiramente. Mas também, avisarem qualquer telemóvel com acesso à internet. Caso um AirTag, se encontre perto de um telemóvel e o detentor deste telemóvel começasse a deslocar-se, surgiria um alerta de rastrear por perto. Assim, as necessidades do utilizador seriam cumpridas e que a marca transpareceria mais segurança.

5.5 Resultado

Considerando os resultados, é evidente que o design especulativo pode ajudar a mostrar potenciais resultados e possibilidades de design que devem surgir no futuro, como foi possível validar a hipótese com a criação de cenários possíveis. Ao observar-se o problema retratado no cenário 1 (*stalkerware*), foram consideradas as respostas que envolviam clonagem de dispositivos ou o acesso ao telemóvel sem autorização. 13 participantes que identificaram situações idênticas: “o namorado da minha filha clonou-lhe o telemóvel”, “um ex namorado, já mexeu no meu telemóvel sem minha autorização e leu as minhas conversas todas”, “o esposo da minha tia clonou-lhe o telemóvel para ter acesso às suas conversas”, “situações contadas por outras pessoas a afirmarem que os companheiros costumam pedir a partilha de localização”, “uma ex amiga minha quando tivemos uma discussão entrou no meu telemóvel, acedeu ao Instagram alterou-me os dados e fez-se passar por mim, ofendendo-me e postando fotos minhas em criança”, e outras. Como as pessoas não têm tanto conhecimento em Portugal sobre esses aplicativos de clonagem, estes cenários eram esperados. Todas estas respostas deram origem a um só cenário interior, passado numa casa, onde os ciúmes resultaram na invasão de privacidade.

Além disso, para o cenário 2 (iRobot), foi relevante perceber-se que 20 participantes do questionário, 7 homens e 13 mulheres, utilizavam aspirador robô no seu quotidiano. Este cenário é igualmente retratado em uma habitação, onde um dos membros do casal utiliza a *app* comum da casa para atormentar a vítima, ligando o iRobot, deixando-a confusa.

Para o cenário 3 (luzes inteligentes), 18 participantes, 6 homens e 12 mulheres, responderam que têm luzes inteligentes. Além disso, este cenário baseou-se na análise de Moog (2019) sobre *smart homes*, onde dá exemplos de episódios de abuso doméstico. Situações semelhantes foram encontradas em respostas: “um ex companheiro de uma amiga minha colocou câmeras para vigiar o que ela fazia na sua ausência”. Este cenário passa-se na habitação

do casal. Assim como no cenário anterior, o abusador, apodera-se da aplicação das luzes inteligentes impedindo a vítima de ligar as luzes da casa.

Por último, no cenário 4 (rastreador de localização) centraram-se a maioria das respostas, em: 309 respostas 48 falavam de formas de rastrear. Isto comprova de alguma forma o observado na teoria, como casos de clonar dispositivos e rastreadores GPS: “O marido da minha filha clonou o telemóvel dela para a vigiar e colocou um chip no carro para a seguir e saber onde ela anda”, “Uma amiga minha tinha um rastreador GPS da Apple dentro do carro mas ela tinha um Samsung e só descobriu porque quando fomos sair com outra amiga nossa, de carro, essa amiga tinha um iPhone e recebeu a notificação que existia um AirTag por perto. Ela nunca apresentou queixa porque não descobriu quem lhe fez aquilo e porque tinha um pouco de medo com as perguntas que a polícia fizesse”, “O namorado de um amigo próximo meu comprou na Internet um rastreador GPS (smart Tag da Samsung) para ter controle sobre onde ele andava”, “O meu marido ofereceu-me um carro novo, com o intuito de me controlar. rastrear todos os meus passos através do GPS que está ligado ao telemóvel dele”, Este cenário envolveu ambientes internos e externos. A proteção de dados dedicada a este produto inteligente precisa de previsão da vitimização tecnológica por parceiro íntimo, pois é tão ou mais comum do que as experiências pessoais de violência por parceiro íntimo e relacionar-se-á com o relato de experiências off-line.

CAPÍTULO 6 | Conclusão e Trabalhos Futuros

6.1 Conclusões e Implicações da investigação

Esta dissertação teve o objetivo principal de responder à questão de investigação: os *smart products* podem viabilizar novas formas de perseguição e abuso na violência do parceiro íntimo? Este capítulo inclui a resposta aos objetivos secundários traçados, resumindo os capítulos anteriores e as suas contribuições para responder à questão de investigação. A parte posterior discutirá as implicações da investigação, seguindo-se pelas limitações e futuras investigações propostas, incluindo qualquer pensamento final.

A partir do resultado obtido na revisão de literatura, foi possível definir um quadro de análise de *benchmarking* de *smart products* maioritariamente conhecidos e utilizados no quotidiano, tanto em ambientes internos como externos. A partir daí, percebeu-se quais eram importantes para colocar em foco nos questionários realizados. Os resultados indicam que o objetivo geral de identificar se os *smart products* podem viabilizar novas formas de perseguição e abuso na violência do parceiro íntimo foi plenamente atendido.

Foram quatro os objetivos específicos no campo de análise:

(i) Investigar a revisão da literatura sobre o atual quadro teórico examinado em estudos e as características da violência doméstica, os tipos de violência e fatores influenciadores envolvidos no processo de utilização de produtos/dispositivos e casas inteligentes. Foi realizada uma pesquisa estatística do quadro atual de violência que recolhe dados especificamente para a população portuguesa, seguindo as referências da APAV (2021) e INE (2020). Ainda para maior qualidade do estudo, juntamente com o levantamento da literatura, foi feito um repertório de associações que atualmente atuam no campo de apoio às vítimas.

(ii) Navegar nas áreas de *smart products* e de *IOT*, bem como compreensão do que são produtos inteligentes e como são inteligentes. Mostrar como os produtos podem ser conceptualizados de formas distintas. Foi levantada uma análise *benchmarking* com foco em 10 *smart products* dedicados ao uso quotidiano recorrente, fazendo, numa primeira parte, um diagnóstico detalhado das funcionalidades correspondentes a cada produto e, numa segunda, focado naqueles que incluíam rastreador GPS.

(iii) Identificar as perceções e experiência dos usuários em sistemas inteligentes e rastreadores GPS em relação à confiança, monitorização, rastreamento e vigilância.

Após o levantamento da revisão de literatura, e *benchmarking*, foi realizado um questionário online na plataforma Google Forms, dividido em 5 secções e compartilhado em redes sociais e presencialmente.

(iv) Especular o efeito da utilização indevida das tecnologias domésticas inteligentes através das lentes de género e como as pessoas percebem as oportunidades e desvantagens. Como resultado do questionário, foi elaborada uma pesquisa de design especulativo que concluiu por último, numa análise de possíveis futuros dos quais deram origem a 4 cenários de abuso tecnológico, apresentados em formato visual para interação entre problema e possível solução.

Para começar, o capítulo 1 introduziu o contexto de toda a pesquisa efetuada, começando por fornecer a justificativa da utilização do termo em inglês, “*smart product*”, escolhido por ser comumente usado como diferenciador entre o genérico nome atribuído, “produto inteligente”, que, além de ter conotações bastantes amplas, não distingue precisamente o que é realmente um produto inteligente.

No capítulo 2, a revisão de literatura introduziu a questão da violência, primeiro de um modo geral ao apresentar o que é, quais os tipos que existem, para além do ciclo e a extensão da mesma, incluindo maioritariamente referências internacionais por falta de estudos focados em Portugal. De seguida, a abordagem sociotécnica da violência doméstica com a tecnologia, começou por definir o que é uma casa inteligente. Uma vez que a violência doméstica facilitada pela tecnologia tem múltiplas formas, o foco situou-se nas casas inteligentes, o que permitiu reconhecer que a violência doméstica facilitada pela tecnologia na casa inteligente pode ocorrer em outros relacionamentos além de parceiros íntimos. Isso foi reconhecido principalmente na análise dos questionários (secção 4.3.2). Ainda no capítulo 2, começou por fornecer um breve contexto sobre os IoT e a popularidade emergente dos *smart products*. A revisão de literatura envolveu um conjunto de conceitos, pontos de vista de vários autores e subjetividades. Foi dividida em cinco categorias principais: 1) design contra o crime, 2) conceito de violência, 3) enquadramento legal atual em Portugal, 4) associações de apoio às vítimas, 5) tecnologia e a violência doméstica. Descobriu-se, ao analisar o começo do IoT, que havia uma ideia estabelecida sobre o género e uma ligação entre *smart home* atualmente e tecnologia doméstica em 1990 (secção 2.6.1). Descobriu-se também que a perpetuação da violência podia ser dividida em em três categorias (1) assédio direto; (2) invasão de privacidade e (3) acesso negado (secção 2.6). Uma grande maioria das pesquisas académicas é centrada no assédio direto, existindo uma visível limitação de estudos sobre a invasão de privacidade relativamente a *smart products*

e poucas pesquisas acadêmicas e legislação sobre acesso negado. Esta tese abordou algumas dessas falhas.

Para ilustrar a urgência de discutir a violência doméstica facilitada pela tecnologia e expandir o contexto dado no capítulo 1 e no capítulo 2, foi conduzida uma análise de mercado, *benchmarking*. O capítulo 3 forneceu uma estrutura teórica propositadamente para facilitar a análise detalhada de uma variedade de *smart products* referidos no *selection criteria*. Juntos eles formam uma tabela que identifica todas as características e relacionamentos dos dispositivos para que estes fossem organizados e compreendidos.

Para complementar o referencial teórico, o capítulo 4 incluiu um método de análise adotado para responder à questão de investigação: um questionário com base em três questionários existentes (seção 4.2.2). Para incluir seções diferentes, essas adaptações facilitaram a análise do resultado pela capacidade de incluir apenas o desejado. Conforme descrito no capítulo 4, este método foi escolhido devido à sua vantagem na proporção e rapidez na coleta de dados. Percebeu-se que o resultado de algumas questões não foi o esperado. Apesar da utilização de palavras simples e breves explicações, o termo ‘rastreador de GPS’ foi sucessivamente confundido em alguns casos, levando participantes a pensar que se tratava do GPS comum. Isto implicou a anulação de algumas questões durante a análise dos resultados (seção 4.3.2).

O capítulo 5 aplicou outro método de análise, escolhido devido tanto ao resultado dos questionários, como pelo facto do início do capítulo dedicar-se ao estudo do design especulativo. Deste modo, as descobertas levaram à criação de 4 cenários futuros, baseados em respostas dadas nos questionários nas questões de resposta aberta. Isto existiu uma outra implicação sobre a forma como foram feitas: ao invés de “obrigar” a uma resposta extensa, a forma fechada de como foi colocada permitia respostas de apenas “sim” ou “não”, não fornecendo os detalhes pretendidos.

No geral, esta seção foi essencial para responder à pergunta de investigação, sobre a possibilidade dos *smart products* viabilizarem novas formas de perseguição e abuso na violência do parceiro íntimo. Além disso, pode-se argumentar que, na criação dos cenários futuros, o exercício de selecionar um dispositivo inteligente, como foi o caso de iRobot, luzes inteligentes e AirTag, e examinar como este pode ser mal utilizado, não valida apenas a violência doméstica facilitada por tecnologia, como também atua como um exemplo ilustrativo de que os pesquisadores separam a violência facilitada pela tecnologia das outras formas de violência, ao descrever-se e analisar-se os riscos do dispositivo abordado.

O presente trabalho aborda uma visão diferente dos demais relacionados a este tema. A maioria dos trabalhos na literatura estão direcionados para a apresentação de um novo produto *smart safe*. Outros apresentam reflexões de revisões bibliográficas de outros artigos (ex, Karunya and Kalaiselvi, 2019; Selvi et al. 2020; Philomina et al. 2019). Já outra maioria foca na saúde mental da vítima (Vogels, 2021, Kim et al., 2022, Shoham, et al, 2010). Esta investigação diferencia-se assim das demais. Procurou-se trazer uma visão diferente no levantamento de funções dos *smart products*, focando apenas nas que podem ser utilizadas para controle ou perseguição e recorrendo a fontes do meio acadêmico e de mercado, em cenários futuros e posteriormente suas possíveis soluções.

Este trabalho permite ainda enumerar algumas implicações.

Implicações para produtos: existe ainda uma idealização de produtos tendo em conta um valor monetário e não respeitando a real necessidade do consumidor. O designer tem o poder de fazer com que produtos de má qualidade ou prejudiciais sejam retirados do mercado, pois antes de tudo o designer é um cidadão e tem a responsabilidade moral, social e profissional de se fazer ouvir como cidadão.

Implicações para designers: os designers devem ter em mente um design inclusivo, conjugando criatividade e moralidade num mundo de tecnologia. Segundo uma estimativa, haverá mais de 64 bilhões de *smart products* no mundo até 2025. O aumento no uso da tecnologia não deve criar mais oportunidades de assédio entre parceiros íntimos e familiares. Para isso, deve-se manter em mente a violência doméstica, incluindo ativamente sobreviventes no processo de desenvolvimento de novos produtos ou aplicativos (Joshi, 2022).

Implicações para o futuro: com os avanços tecnológicos e o aparecimento de novos produtos, é importante pensar na proteção de dados, respeitando a privacidade e aumentando a segurança do consumidor. Estes avanços na tecnologia, também aumentam a importância que deve ser dada ao desenvolvimento de mais estudos da violência tecnológica como uma forma de violência. Com a crescente busca por uma maior consciência social, o papel do design como disciplina passa por perspetivar as atividades das novas gerações de designers e assim antecipar danos futuros na criação de novos produtos, potenciais caminhos e recomendações para o design (design socialmente consciente). Comprovando assim que o design de produto enquanto disciplina de design é uma atividade indispensável na elaboração de pesquisas de produtos inteligentes, para e só assim ser possível antecipar e evitar situações, antes mesmo de serem lançados para o mercado.

“Todavia, ser bom é subjetivo e alguém pode ser um bom (ou ótimo) designer sem necessariamente ser um bom cidadão. Mas se o bom design (independente de estilo ou

maneirismo) acrescenta valor à sociedade, seja pelo investimento no invólucro cultural ou pela manutenção do status quo em um alto nível, então design e cidadania devem andar de mãos dadas.” (Heller, 2003)

6.2 Limitações e Futuras Investigações

Existiram algumas limitações neste estudo, mais especificamente no questionário. As respostas têm uma maior incidência no gênero feminino e na cidade de Braga. Além disso, as respostas não são 100% fidedignas pois é muito comum participantes que têm vergonha de admitir os abusos. Além disso, durante a chamada etapa “lua de mel”, a vítima é iludida a acreditar que já não o é e que estes abusos não acontecerão novamente, o que pode comprometer as suas respostas. Percebeu-se ainda que seria necessária uma recolha de respostas presencial para conseguir dados mais exatos em relação à população mais idosa, pois não têm tanto conhecimento/experiência em relação às tecnologias mais recentes.

Na análise do *benchmarking* de produtos do mercado, não há acesso a informação científica, sendo a maioria da informação obtida de sites de revistas e lojas de tecnologia.

Para recomendações de futuras investigações, sugere-se a recolha de dados em comunidades mais específicas como comunidades *queer*, idosos ou crianças.

Outra recomendação que se mostrou necessária durante o trabalho foi o teste de cenários de forma a encontrar possíveis soluções para novas orientações no design de futuros “*smart products*”.

Por fim, seria também plausível considerar substituir os questionários por entrevistas, pois algumas das perguntas podem não ser corretamente interpretadas, já que as respostas obtidas nem sempre foram suficientemente claras.

REFERÊNCIAS BIBLIOGRÁFICAS

- Afonso, A. & Nunes, C. (2019). Probabilidades e Estatística. Aplicações e Soluções em SPSS. Versão revista e aumentada. Universidade de Évora. <http://hdl.handle.net/10174/25959>
- Alonso, F., López, G., Manrique, D. & Viñes, J. (2005). An Instructional Model for Web-based e-learning Education with a Blended Learning Process Approach. *British Journal of Educational Technology*. 36. 217 - 235. <https://doi.org/10.1111/j.1467-8535.2005.00454.x>
- APAV (2012). Violência Doméstica. <https://apav.pt/vd/index.php/features2>
- APAV (2019). Estatísticas Associação de Portuguesa de Apoio à Vítima. https://apav.pt/apav_v3/images/pdf/Estatisticas_APAV-Relatorio_Anual_2019.pdf
- APAV (2023) A Nossa História, Contexto Histórico de Surgimento da APAV. https://apav.pt/apav_v3/index.php/pt/apav-1/a-nossa-historia
- Apple (2021). WatchOS 8 brings new access, connectivity and awareness features to Apple Watch <https://bitly.com/ZLkWR>
- Amazon (2020). Apple reviews Mac Laptop. Amazon.es. <https://www.amazon.es/dp/B08N5WM84C?th=1>
- Amazon (2020). Opiniones de clientes, Philips Hue - Bombilla inteligente, E27, Puente Philips Hue incluido, Luz blanca y colores, Compatible con Alexa y Google Home - Pack de 2 Bombillas LED Inteligentes. Amazon.es. <https://bitly.com/hHcoE>
- Amazon (2022). Review Apple 2022 Ipad Air. Amazon.es. <https://www.amazon.es/dp/B09V4GLCC2?th=1#customerReviews>
- Amazon (2022). Review ecobee Smart Thermostat Premium with Siri and Alexa and Built in Air Quality Monitor and Smart Sensor. Amazon. <https://bitly.com/GtQRT>
- Amirteimoori, A., Sahoo, B. K., Charles, V. & Mehdizadeh, S. (2022). Benchmarking. In: Stochastic Benchmarking. *International Series in Operations Research and Management Science*. Springer, 317. https://doi.org/10.1007/978-3-030-89869-4_1
- Baker, A. (2005). Parental alienation strategies: A qualitative study of adults who experienced parental alienation as a child. *American Journal of Forensic Psychology*, 23, 41–63. <https://psycnet.apa.org/record/2005-15205-003>
- Benedictis, T., Jaffe, J. & Segal, J. (2006). Domestic Violence and Abuse: Types, Signs, Symptoms, Causes, and Effects. <https://bit.ly/3hFG0QF>

- Bell, J. (1997). Como Realizar um Projeto de Investigação. 3ª edição. Lisboa: Gradiva.
<https://soclogos.files.wordpress.com/2014/09/como-realizar-um-p-de-investigac3a7ao-bell.pdf>
- Björklund, T. A. (2013). Initial mental representations of design problems: Differences between experts and novices. *Design Studies*, 34(2), 135–160.
<https://doi.org/10.1016/j.destud.2012.08.005>
- Bleeker, J. (2009). Design Fiction: A short essay on design, science, fact and fiction. Near Future Laboratory.
https://drbfw5wflxon.cloudfront.net/writing/DesignFiction_WebEdition.pdf
- Bogdan, R. & Biklen, S. (1994). Investigação qualitativa em educação. Porto: Porto Editora. 48-52.
- Bonino, L. (2004). Los micromachismos. Revista La Cibeles n2 del Ayuntamiento de Madrid.
<https://www.mpd.org/sites/default/files/micromachismos.pdf>
- Bowles, N. (2018, June 23). Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. *The New York Times*. <https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.htm>
- Bracewell, K., Hargreaves, P. & Stanley, N. (2020). As consequências do bloqueio do COVID-19 na perseguição à vítima. *Revista de Violência Familiar*. Springer.
<https://doi.org/10.1007/s10896-020-00201-0>
- Braga, L. L., Fiks, J. P., Mari, J. J. & Mello, M. F. (2008). The importance of the concepts of disaster, catastrophe, violence, trauma and barbarism in defining posttraumatic stress disorder in clinical practice. *BMC Psychiatry*. 8-68.
- Brant, T. (2020, March 20) Apple MacBook Air (2020) ReviewA redesigned keyboard and lower price make the Air easy to recommend. PCMag.
<https://www.pcmag.com/reviews/apple-macbook-air-2020>
- Breiding, M., Basile, K. C., Smith, S. G., Black, M. C. & Mahendra, R. R. (2015). Intimate partner violence surveillance : uniform definitions and recommended data elements. National Center for Injury Prevention and Control (U.S.). Division of Violence Prevention. 2. <https://stacks.cdc.gov/view/cdc/31292>
- Brock, J. K. U. (2019). The evolution of marketing technology. In Handbook of advances in marketing in an era of disruptions: Essays in honour of Jagdish N. Sheth. ed. A. Parvatiyar and R. Sisodia New Delhi: Sage Publications India, 343–359.
<https://dx.doi.org/10.4135/9789353287733>
- Bugeja, J., Jacobsson, A., & Davidsson, P. (2017). An analysis of malicious threat agents for the smart connected home, *IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 557-562, 10.1109/PERCOMW.2017.7917623.

- CETA (2022, August 17) Mobile Spyware Concern Tips Guide, Compiled by the Clinic to End Tech Abuse.
https://www.ceta.tech.cornell.edu/files/ugd/c4e6d5_3711c453b0134dde989e996554a63125.pdf
- CETA (2022). Resources, Step-by-step How-to Guides. Clinic to End Tech Abuse.
<https://www.ceta.tech.cornell.edu/aboutus>
- Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., et al. (2018). “The Spyware Used in Intimate Partner Violence,” em IEEE Symposium on Security and Privacy (San Francisco: IEEE), 441–458. doi:10.1109/SP.2018.00061
- Chen, B. X. (2020, February 19). Your Doorbell Camera Spied on You. Now What? *The New York Times*.
<https://www.nytimes.com/2020/02/19/technology/personaltech/ring-doorbell-camera-spying.html>
- Chen, B. X. (2022, November 2) Security Cameras Make Us Feel Safe, but Are They Worth the Invasion? Internet cameras like Amazon’s Ring come at a high cost to our privacy. *The New York Times*.
<https://www.nytimes.com/2022/11/02/technology/personaltech/security-cameras-surveillance-privacy.html>
- Cheyne, N., & Guggisberg, M. (2018). Stalking: An age old problem with new expressions in the digital age. In M. Guggisberg & J. Henricksen (Eds.), *Violence against women in the 21st century: Challenges and future directions* (pp. 161–190). Hauppauge NY: Nova Science Publishers.
- Coelho, L. P. B., Gonçalves, J. P. S., Gonçalves, P. H. S., Netom, T. R. B., Jesus, J. V. M., Dias, M. J. & Rodrigues, R. F. N. (2021) Evolução das Smarts Homes em Função das Tecnologias. *Anais do Simpósio Nacional de Ciência e Engenharias- SINACEN*, 6(1), 125-129. <http://anais.unievangelica.edu.br/>
- Colby, C. (2022, March 22). A Data Breach Can Compromise Your Information. Here's How to Safeguard It. *CNET Your guide to a better future*.
<https://www.cnet.com/tech/services-and-software/a-data-breach-can-compromise-your-information-heres-how-to-safeguard-it/>
- Delaney, J. R. (2019, December 2). Ring Indoor Cam Review. *PCMag*.
<https://www.pcmag.com/reviews/ring-indoor-cam>
- Delaney, J. R. (2022, June 1). Ecobee Smart Thermostat Premium Review. More than just a smart thermostat. *PCMag*. <https://www.pcmag.com/reviews/ecobee-smart-thermostat-premium>
- Dimond, JP, Fiesler, C. & Bruckman, AS (2011). Violência Doméstica e Tecnologias de Informação e Comunicação. *Computação interativa*. 23 (5), 413–421. doi:10.1016/j.intcom.2011.04.006

- DiSalvo, C. (2012, Jun 12). Spectacles and Tropes: Speculative Design and Contemporary Food Cultures. *FibreCulture Journal*, no. 20. 109–122.
<https://fibreCulturejournal.org/fcj-142-spectacles-and-tropes-speculative-design-and-contemporary-food-cultures/>
- Dhir, A., Kaur, P., Chen, S. & Pallesen, S. (2019). Antecedentes e consequências do cansaço das redes sociais. *Jornal Internacional de Gerenciamento de informações*, 48, 193–202
<https://doi.org/10.1016/j.ijinfomgt.2019.05.021>
- Domestic Violence Resource Center (2020). Rebuilding Safe And Hopeful Lives In Washoe County Since 1977 (formerly the Committee to Aid Abused Women/CAAW)
- Dragiewicz, J., Bagwell-Gray, M., Brown, M. L., Kappas, A. & Durfee, A. (2020). Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement. *Journal of Family Violence*, 35, 693–704.
<https://doi.org/10.1007/s10896-019-00114-7>
- Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, P. N., Woodlock, D. & Harris, B. (2018). Tecnologia facilitou o controle coercitivo: violência doméstica e os papéis concorrentes das plataformas de mídia digital, *Feminist Media Studies*, 18(4) , 609-625, <https://doi.org/10.1080/14680777.2018.1447341>
- Dunne, A. & Raby, F. (2001). *Design Noir: A Vida Secreta dos Objetos Eletrônicos*. Birkhauser.
- Dunne, A. & Raby, F. (2013). Speculative Everything – Design, Fiction, and Social Dreaming. 3(4). 159-189.
- Dunn, S. (2020) Technology-Facilitated Gender-Based Violence: An Overview. Centre for International Governance Innovation.
https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1774&context=scholarly_works
- Dutton, D. G. (2006). *Rethinking Domestic Violence*. UBC press. 1943.
- Eklblom, P., & Tilley, N. (2000). Going equipped. *The British Journal of Criminology*, 40, 376–398. doi:10.1093/bjc/40.3.376
- Eklblom, P. (2011). *Crime Prevention, Security and Community Safety Using the 5 Is Framework*. Basingstoke, UK: Palgrave MacMillan.
- Elder, J. (2019, Outubro 2). O primeiro aparelho da Internet das Coisas: a torradeira "inteligente" de John Romkey. *Avast*, <https://blog.avast.com/pt-br/the-internets-first-smart-device>
- Esposito, S., Sgandurra, d. & Bella, G. (2022). Alexa versus Alexa: Controlling Smart Speakers by Self-Issuing Voice Commands. 10-15, <https://arxiv.org/pdf/2202.08619.pdf>

- Faria, O. (2020). Internet of Torment: The Governance of Smart Home Technologies against Technology-Facilitated Violence o [Unpublished master's thesis]. Carleton University.
- Faria, O. & Lauriault, T. P. (2021, February 2021). Smart Home Technology Facilitated Violence. Community Solutions Network Research Brief. Future Cities Canadá.
- Fox, J., & Tokunaga, R. S. (2015). Attachment, dependence, distress, and post-dissoution online surveillance via social networking sites. *Cyberpsychology, Behavior, and Social Netwrking*, 18(9), 491–498.
- Fortin, M. F. (1999). O Processo de Investigação Da Concepção à Realização. Lisboa, Lusodidacta. 9789728383107
- Fortin, M. F. (2006). Fundamentos e etapas do processo de investigação. Lisboa, Lusodidacta
- Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T. & Dell, N. (2018). “A Stalker's Paradise”: How Intimate Partner Abusers Exploit Technology. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM Digital Library. 667, 1-13. <https://doi.org/10.1145/3173574.3174241>
- Getzels, J. W. (1975). Problem-finding and inventiveness of solutions. *Journal of Creative Behavior*, 9 (1), 12–18. <https://doi.org/10.1002/j.2162-6057.1975.tb00552.x>
- Ghebresslassie, M. (2018, November 2). 'Stalked within your own home': Woman says abusive ex used smart home technology against her. CBC News. <https://www.cbc.ca/news/science/tech-abuse-domestic-abuse-technology-marketplace-1.4864443>
- Goodin, D. (2022). Os invasores podem forçar o Amazon Echos a se hackear com comandos auto emitidos. *Ars Technica*. <https://arstechnica.com/information-technology/2022/03/attackers-can-force-amazon-echos-to-hack-themselves-with-self-issued-commands/>
- Google (2022, Dezembro 15). Política de privacidade. Google. https://www.gstatic.com/policies/privacy/pdf/20221215/qi5mvafl/google_privacy_policy_pt-PT_eu.pdf
- Greenwald, W. (2022, Junho 23). Avaliação do Amazon Echo Studio. PCMag. <https://www.pcmag.com/reviews/amazon-echo-studio>
- Hall, C. (2021, Outubro 12) Apple AirTag vs Tile vs Galaxy SmartTag: Como é que os rastreadores se comparam? Pocket-lint. <https://bityli.com/vqZgM>
- Harbour Research (2021, Agosto 24). Movendo os luditas de casas inteligentes para a frente. Harbour Research. <https://harborresearch.com/smart-home-luddites/>
- Harris, B. & Woodlock, D. (2022). Spaceless violence: Women’s experiences of technology-facilitated domestic violence in regional, rural and remote areas. *Trend & Issues in crime*

- and criminal justice. https://www.aic.gov.au/sites/default/files/2022-02/ti644_spaceless_violence.pdf
- Hargreaves, T., & Wilson, C. (2017). Smart homes and their Users. Springer Internacional [.https://doi.org/10.1007/978-3-319-68018-7](https://doi.org/10.1007/978-3-319-68018-7)
- Heller, S. & Vienne, V. (2000). Citizen Designer. New York: Allworth Press. 87-89.
- Hellevik, P. & Øverlien, C. (2016). Teenage intimate partner violence: Factors associated with victimization among Norwegian youths. *Scandinavian Journal of Public Health*, 44(7), 702–708. <https://doi.org/10.1177/1403494816657264>
- Henry, N., Flynn, A. & Powell, A. (2020). Technology-facilitated domestic and sexual violence: A review. *Violence Against Women*, 26(15–16), 1828–1854. <https://doi.org/10.1177/1077801219875821>
- Hildebrand, Y. (2020). Philips Hue vale a pena? Veja prós e contras das lâmpadas inteligentes. *Techtudo*. <https://www.techtudo.com.br/noticias/2020/10/philips-hue-vale-a-pena-veja-pros-e-contras-das-lampadas-inteligentes.ghtml>
- Hill, M. M., & Hill, A. (2005). *Investigação por questionário (2ª ed.)*. Lisboa: Edições Sílabo
- ILGA (2022). *Porque existimos. Intervenção Lésbica, Gay, Bissexual, Trans e Intersexo*, <https://ilga-portugal.pt/associacao/porque-existimos/>
- Interpret (2022, Abril 27). How AI is transforming the smart home business. Interpret Weekly Insights, IOT & Smart home <https://interpret.la/how-ai-is-transforming-the-smart-home-business/>
- Jacobs, J. M & Lees, L. (2013). Defensible Space on the Move: Revisiting the Urban Geography of Alice Coleman. *International Journal of Urban and Regional Research*, 37 (5) 1559-1583. <https://doi.org/10.1111/1468-2427.12047>
- Johannessen, L. K., Keitsch, M. M., & Pettersen, I. N. (2019). Speculative and Critical Design—Features, Methods, and Practices. *Proceedings of the Design Society: International Conference on Engineering Design*, 1(1), 1623–1632. <https://doi.org/10.1017/dsi.2019.168>
- Joshi, N. (2022, Março 24) Does IoT Help Or Harm Victims Of Domestic Violence? Allerin. <https://www.allerin.com/blog/does-iot-help-or-harm-victims-of-domestic-violence>
- Kane, G. C. (2017). The evolutionary implications of social media for organizational knowledge management, *Information and Organization*, 27 - 1 <https://doi.org/10.1016/j.infoandorg.2017.01.001>
- Karunya, S. & Kalaiselvi, K. (2019). A Persist Evaluation in Women Tracking System Based on Current Epoch. *International Journal Of Recent Technology And Engineering*.

- Kees, A., Oberländer, A. M., Röglinger, M. & Rosemann, M. (2015). Understanding the Internet of Things: A Conceptualisation of Business-to-Thing (B2T) Interactions <https://doi.org/10.18151/7217376>
- Kim, C. & Ferrareso, R. (2022). Examining Technology-Facilitated Intimate Partner Violence: A Systematic Review of Journal Articles, *Trauma, Violence, & Abuse*, 0(0), 1–19 <https://doi.org/10.1177/15248380211061402>
- Knoblauch, F. D.C. (2020). A utilização da tecnologia na luta contra a violência doméstica no confinamento domiciliar. *Revista de género, Sexualidade e Direito*, 6(2), 66-83 [10.26668/2525-9849/index_law_journals/2020.v6i2.7056](https://doi.org/10.26668/2525-9849/index_law_journals/2020.v6i2.7056)
- Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, Are You Listening?: Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW, Article 102, 31. <https://doi.org/10.1145/3274371>
- Lenhart, A., Ybarra, M., Zickuhr, K. & Price-Feeney, M. (2016). pData and Society Research Institute, 3-58
- Low, C. (2022, September 15) Apple Watch Series 8: A week with the new best smartwatch (for now). The upcoming Watch Ultra might well unseat it. *Engadget*. <https://bityli.com/UWZwB>
- Luliu, H., Babes, B. (2018) Smart Homes for older people involved in rehabilitation activities- reality or dream, acceptance or rejection. University of medicine and Pharmacy; Faculty of Economics and Business Administration, Department of Business Information Systems.
- Mace, R. & Caxemira, C. (2021, December 30). Are Apple AirTags Being Used to Track People and Steal Cars? *The New York Times*. <https://www.nytimes.com/2021/12/30/technology/apple-airtags-tracking-stalking.html>
- Mair, J. S. & Mair, M. (2003). Violence prevention and control through environmental modifications. *Annual Review of Public Health*. 24. 209-25
- Malpass, M. (2016). Critical Design Practice: Theoretical Perspectives and Methods of Engagement. *The Design Journal*, 19(3) , 473–489. <https://doi.org/10.1080/14606925.2016.1161943>
- Mancini, M. (2018, Maio 7). A história da Internet das Coisas ou Internet of Things (IoT). LinkedIn. <https://www.linkedin.com/pulse/hist%C3%B3ria-da-internet-das-coisas-ou-things-iot-m%C3%B4nica-mancini/?originalSubdomain=pt>
- Marganski, A., & Melander, L. (2015). Vitimização da violência por parceiro íntimo no mundo cibernético e real: examinando a extensão das experiências de agressão cibernética e sua associação com a violência no namoro em pessoa. *Journal of Interpersonal Violence* , 33 (7), 1071–1095. <https://doi.org/10.1177/0886260515614283>

- Mascarenhas, A. P. F. M., Fernandes, S. M., Freitas, F. D., Calheiros, G. B., Lefrançois, G. L. G., Bahia, M. B., & Raton, V. F. B. (2021). Desenvolvimento de produtos IOT / IOT products development. *Brazilian Journal of Development*, 7(1), 4711–4724. <https://doi.org/10.34117/bjdv7n1-320>
- McCue, M. L. (2008). *Domestic Violence: A Reference Handbook*. ABC-CLIO. 2
- Messing, J., Gray, M. B., Brown, M. L., Kappas, A. & Durfee, A. (2020). Intersections of Stalking and Technology-Based Abuse: Emerging Definitions, Conceptualization, and Measurement, *J Fam Viol* 35, 693–704 (2020). <https://doi.org/10.1007/s10896-019-00114-7>
- Michau, L., Voices, R., & Uganda, K. (2005). Good practice in designing a community-based approach to prevent domestic violence. UN Division for the Advancement of Women
- Mitew, T. (2014). Do objects dream of an Internet of Things?. *The Fibreculture Journal* .23. 1-25. <https://ro.uow.edu.au/lhapapers/1828/>
- Moog, E. P. (2019, March 3) Designing against Domestic Violence by Eva PenzeyMoog. [Video]. YouTube. <https://www.youtube.com/watch?v=P64RHUSRtSA&t=54s>
- Moscaritolo, A. (2021, November 10) iRobot Roomba j7+ Review. *PCMag*. <https://www.pcmag.com/reviews/irobot-roomba-j7-plus>
- Mosley, M. A. & Lancaster, M. (2019). Affection and Abuse: Technology Use in Adolescent Romantic Relationships, *The American Journal of Family Therapy*, 47(1), 52-66, [10.1080/01926187.2019.1586592](https://doi.org/10.1080/01926187.2019.1586592)
- Nascimento, D. R., & Esslin, S. R. (2021). Avaliação de desempenho de Smart Home: um mapa de literatura. *Produto & Produção*, 22(2). 2-4. <https://seer.ufrgs.br/ProdutoProducao/article/view/107595/61402>
- Newman (1972). *O. Defensible space*. New York: Macmillan,
- Npr (2016, Novembro 1). An Experiment Shows How Quickly The Internet Of Things Can Be Hacked, NPR. <https://www.npr.org/sections/alltechconsidered/2016/11/01/500253637/an-experiment-shows-how-quickly-the-internet-of-things-can-be-hacked>
- ONS (2021). The lasting impact of violence against women and girls, *Census 2021*. <https://bityli.com/BhkaRC>
- ONU (2022) Violência contra as mulheres- um problema so séc. XXI. ONU. <https://unric.org/pt/violencia-contra-as-mulheres-um-problema-do-sec-xxi/>
- Open North (2021, July 28). Open Smart Communities: Emerging Issues - Smart Home Technology-Facilitated Violence. Vimeo. <https://vimeo.com/580683555>

- O'Regan, S. (2020, July 3) Deployment Age #11: Futures Funnel. *The Deployment Age*. <https://deploymentage.substack.com/p/deployment-age-11-futures-funnel>
- Pardo, C. Ivens, B. S. & Pagani, M. (2020). Are products striking back? The rise of smart products in business markets, *Industrial Marketing Management*, 90. 205-220 <https://doi.org/10.1016/j.indmarman.2020.06.011>
- Pease, K. (2001). Cracking crime through design. *London, UK: Design Council*.
- Pereira, F. S. (2015). Ciberassédio na adolescência: Prevalência(s), reações à vitimação e mediação parental o [Master's Doctoral dissertation, Universidade do Minho]*. Repositório Institucional da Universidade do Minho. <https://repositorium.sdum.uminho.pt/bitstream/1822/42549/1/Filipa%20da%20Silva%20Pereira.pdf>
- Perry, H. (2022, December 16). The Best Smartwatches, Fitness Trackers, and Running Watches. *The New York Times*. <https://www.nytimes.com/wirecutter/reviews/best-smartwatches/>
- Pesando, L. M. (2022). Safer If Connected? Mobile Technology and Intimate Partner Violence. *Demography*, 59 (2): 653–684, <https://doi.org/10.1215/00703370-9774978>
- Peskin, M. F., Markham, C. M., Shegog, R., Temple, J. R., Baumler, E. R., Addy, R. C., Hernandez, B., Cuccaro, P., Gabay, E. K., Thiel, M. & Emery, S. T. (2017). Prevalence and correlates of the perpetration of cyber dating abuse among early adolescents. *Journal of Youth and Adolescence*, 46(2), 358–375. <https://doi.org/10.1007/s10964-016-0568-1>
- Pillan, M., Varisco, L. & Bertolo, M. (2017). Facing Digital Dystopias: A Discussion about Responsibility in the Design of Smart Product. In Alonso, M. B. , & Ozcan, E. , (Eds.). Proceedings of the conference on Design and Semantics of Form and Movement. IntechOpen. <https://doi.org/10.5772/intechopen.70847>
- Philomina, S., Jasmina, M. & Subbulakshmi, K. (2019, October 19). Possibilities in Enhancing the Security for Women using IoT. *International Journal Of Engineering And Advanced Technology*, 8(62), 718-722.
- Poushter, J. (2016). Smartphone ownership and internet usage continues to climb in emerging economies. Pew research center, 22(1), 1–44.
- Powell, A., & Henry, N. (2018, maio 12). Policiamento da violência sexual facilitada pela tecnologia contra vítimas adultas: perspectivas da polícia e do setor de serviços. *Policiamento e Sociedade*, 28 (3), 291–307.
- Prakash, A. (2022, October 26). How an Apple Watch saved a woman stabbed, buried alive by her husband. *Hindustan Times*. <https://www.hindustantimes.com/technology/how-an-apple-watch-saved-a-woman-stabbed-buried-alive-by-her-husband-101666762617909.html>

- Press, M. & Cooper, R. (2003). A experiência do design: o papel do design e dos designers no século XXI. Routledge, 1. <https://doi.org/10.4324/9781315240329>
- Puri, M., Frost, M., Tamang, J., Lamichhane, P. & Shah, I. (2012) The prevalence and determinants of sexual violence against young married women by husbands in rural Nepal. *BMC Res Notes*, 5, 291. <https://doi.org/10.1186/1756-0500-5-291>
- Raff, S., Wentzel, D. & Obwegeser, N. (2020). Smart Products: Conceptual Review, Synthesis, and Research Directions. *Journal of Product Innovation Management*, 37(5), 379–404 <https://doi.org/10.1111/jpim.12544>
- Ramirez, M. A. (2022, October 26) Apple Watch saves life of woman battling domestic violence — here's how. *Laptop*. <https://www.laptopmag.com/news/apple-watch-saves-life-of-woman-battling-domestic-violence-heres-how>
- Reed, L. A., Tolman, R. M. & Ward, L. M. (2017). Gender matters: Experiences and consequences of digital dating abuse victimization in adolescent dating relationships, *Journal of Adolescence*, 59, 79-89, <https://doi.org/10.1016/j.adolescence.2017.05.015>
- Riley, A. (2020). How your smart home devices can be turned against you. BBC, <https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse>
- Risdijk, S. A. & Hultink, E. J. (2008). How Today's Consumers Perceive Tomorrow's Smart Products. *Journal of Product Innovation Management*, 26 (1), 24-42. <https://doi.org/10.1111/j.1540-5885.2009.00332.x>
- Rittel, H. W. J. & Webber, M. M. (1973). Dilemas em uma teoria geral do planejamento. *Policy Sci*, 4 , 155-169. <https://doi.org/10.1007/BF01405730>
- Romkey, J. (2017). Toast of the IoT: The 1990 Interop Internet Toaster. *IEEE Consumer Electronics Magazine*, 6, 116-119. [DOI:10.1109/MCE.2016.2614740](https://doi.org/10.1109/MCE.2016.2614740)
- Sardinha, L., Maheu-Giroux, M., Stöckl, H., Meyer, S. R. & García-Moreno, C. (2022) Estimativas de prevalência global, regional e nacional de violência física ou sexual, ou ambas, por parceiro íntimo contra mulheres em 2018. *Lancet*, 399 , 803–813. [https://doi.org/10.1016/S0140-6736\(21\)02664-7](https://doi.org/10.1016/S0140-6736(21)02664-7)
- Segan, S. (2022, March 31). Apple iPad Air (2022) Review, The best iPad for creators. <https://www.pcmag.com/reviews/apple-ipad-air-2022>
- Selvi, A., Ashwini, T., Varshini, S. G., Madhumitha, S. & Benedicta, D. S. J. (2020). Smart Mart Security Device for Women Safety Using Iot. *International Journal of Advanced Science And Technology*, 29(7), 1598-1602
- Silent Beacon (2022). Personal Safety Device and Safety APP, <https://silentbeacon.com/>

- Silva, J. B. (2022). Identificação de funcionalidades para um novo dispositivo para promover a segurança feminina. Universidade Federal de Santa Catarina Centro Tecnológico
- Sheridan, L. & Lyndon, A.E. (2010). The Influence of Prior Relationship, Gender, and Fear on the Consequences of Stalking Victimization. *Sex Roles* 66, 340–350. <https://doi.org/10.1007/s11199-010-9889-9>
- Sherr, I. (2022, September 28) Apple Wants the iPhone to Be a Lifesaver, Literally. Apple's betting even bigger on safety, and on convincing you that its products could save your life. *CNET Your guide to a better future*. <https://www.cnet.com/tech/mobile/apple-wants-the-iphone-to-be-a-lifesaver-literally/>
- Shoham, S.G., Knepper, P. & Kett, M. (2010). *International Handbook of Victimology*. CRC Press. 571.
- Smith-Darden, J. P., Kernsmith, P. D., Victor, B. G. & Lathrop, R. A. (2017). Electronic displays of aggression in teen dating relationships: Does the social ecology matter? *Computers in Human Behavior*, 67, 33–40. <https://doi.org/10.1016/j.chb.2016.10.015>
- Snook, Chayn, SafeLives. (2017). Tech vs Abuse. Comic Relief. https://docs.wixstatic.com/ugd/f86f13_366b6514c8fc4e9488fc15edf2148d52.pdf
- Sovacool, B., Furszyfer-Del Rio, D.D. & Martiskainen, M. (2021). Prosuming pode se tornar perigoso? Explorando Sistemas de Controle e Abuso Doméstico nas Casas Inteligentes do Futuro. *Frente. Energia Res.* 9:765817. doi: 10.3389/fenrg.2021.765817
- Song, V. (2022, September 15) Apple Watch Series 8 review: if it ain't broke. *The Verge*. <https://www.theverge.com/23353756/apple-watch-series-8-review-smartwatch-wearables>
- Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Violência de parceiro íntimo, tecnologia e perseguição. *Violência contra as mulheres*, 13 (8), 842–856.
- Staff, M. (2019, September 3). Save \$60 on Philips Hue White and Color Smart Light Starter Kit. *PCMag*. <https://www.pcmag.com/deals/save-60-on-philips-hue-white-and-color-smart-light-starter-kit>
- Storey, J. E., & Hart, S. D. (2011). How do police respond to stalking? An examination of the risk management strategies and tactics used in a specialized anti-stalking law enforcement unit. *Journal of Police and Criminal Psychology*, 26 (2), 128–142.
- Taylor, S. & Xia, Y. (2018). Cyber partner abuse: A systematic review. *Violence and Victims*, 33(6), 983-1011. <https://doi.org/10.1891/0886-6708.33.6.983>
- Tanenbaum, J., Tanenbaum, K., & Wakkary, R. (2012, May). Steampunk as design fiction. In *Proceedings of SIGCHI Conference on Human Factors in Computing Systems*.

- Association for Computing Machinery, Nova York, NY, EUA, 1583-1592.
<https://doi.org/10.1145/2207676.2208279>
- Tanczer, L. (2018). Tech Abuse Policy Brief. Department of Science, Technology, Engineering and Public Policy. https://www.ucl.ac.uk/steapp/sites/steapp/files/giot_policy_.pdf
- Tanczer, L., Patel, T., Parkin, S., & Danezis, G. (n.d.). Written evidence submitted by the 'Gender and Internet of Things' Research Team University College London (UCL). https://www.ucl.ac.uk/steapp/sites/steapp/files/giot_home_affairs_committee_submission_final.pdf
- Tanczer, L. (2020). Gender and Internet of Things: Future proofing Online Harms legislation Department of Science, Technology, Engineering and Public Policy. 171. 1. https://www.ucl.ac.uk/steapp/sites/steapp/files/ucl_giot_online_harms_tech_abuse_one_pager_-_feb2020.pdf
- Tanczer, L., Lopez-Neira, I., Parkin, S., Patel, T., & Danezis, G. (2018). Gender and IoT Research Report: The Rise of Internet of Things and implications for technology-facilitated abuse. Department of Science, Technology, Engineering and Public Policy. 1–9.
- Tanczer, L., Lopez-Neira, I., Patel, T., Parkin, S., & Danezis, G. (2019). Gender and IoT (G-IoT) Resource List (pp. 1–7). Department of Science, Technology, Engineering and Public Policy. <https://www.ucl.ac.uk/steapp/sites/steapp/files/g-iot-resource-list.pdf>
- Tuohy, J. P. (2022, June 14). Smart switches or smart bulbs? How to choose the right smart lighting for your home. *The Verge*. <https://www.theverge.com/23156554/smart-bulbs-switch-lighting-guide-how-to>
- Tuohy, J. P. (2022, October 13). Yale Assure Lock 2 review: a promising all-rounder. *The Verge*. <https://www.theverge.com/23367464/yale-assure-lock-2-touchscreen-keypad-wifi-review>
- Tseng, E., Bellini, R., Ristenpart, T., Sabet, M., Sodhi, H. K., Dell, N. (2022, May 4). Care Infrastructures for Digital Security in Intimate Partner Violence [Conference session] Socio-technical aspects of cybercrime, New Orleans, LA, USA. <https://programs.sigchi.org/chi/2022/index/content/68741>
- Tuckman, B.W. (2012). Manual de investigação em educação. Metodologia para conceber e realizar o processo de investigação científica (4ª edição) Lisboa: Fundação Calouste Gulbenkian.
- UN (2020, May 14). What Is Domestic Abuse? United Nations, Covid 19 Response. <https://bit.ly/2X8pwHi>

- UN Women (2020). Ending violence against women. https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2013/12/UN%20Women%20EVAW-ThemBrief_US-web-Rev9%20pdf.pdf
- Vigderman, A. & Turner, G. (2022, November 23) Ring Home Security Camera Cost and Pricing. *Security.org*. <https://www.security.org/security-cameras/ring/>
- Vigdor, N. (2019, December 15). Somebody's Watching: Hackers Breach Ring Home Security Cameras. *The New York Times*. <https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html>
- Visser, W. (2006). *The Cognitive Artifacts of Designing*. CRC Press, 1. <https://doi.org/10.1201/9781482269529>
- Vogels, E. A. (2021, February 16). Online harassment occurs most often on social media, but strikes in other places, too. Pew Research Center. <https://www.pewresearch.org/fact-tank/2021/02/16/online-harassment-occurs-most-often-on-social-media-but-strikes-in-other-places-too/>
- Vogels, E. A., Gelles-Watnick, R. & Massarat, N. (2022, August 10). Teens, Social Media and Technology 2022. *Pew Research Center*.
- Voros, J. (2001). A primer on futures studies, foresight and the use of scenarios. *Prospect: The Foresight Bulletin*, 6(1)
- Wetsman, N. (2022, September 7) Apple adds souped-up period and ovulation tracking to Apple Watch Series 8 / It'll also flag abnormal period symptoms. *The Verge*. <https://www.theverge.com/2022/9/7/23341259/apple-watch-series-8-ovulation-period-tracking-temperature-sensor>
- WHO (2020). Definition and typology of violence <https://bit.ly/2MvE6qo>
- Wilson, C., Hargreaves, T., Hauxwell-Baldiwin, R. (2017) Benefits and risks of smart home technologies. *Energy Policy*, 103, 72-83.
- Wong, R.Y., Khovanskaya, V. (2018). Speculative Design in HCI: From Corporate Imaginations to Critical Orientations. In: Filimowicz, M., Tzankova, V. (eds) *New Directions in Third Wave Human-Computer Interaction: Methodologies*. Human-Computer Interaction Series. Springer, 2, 175-202. https://doi.org/10.1007/978-3-319-73374-6_10
- Woodlock, D. (2014). Technology-facilitated stalking: findings and resources from the SmartSafe project. *Researchgate*. [10.13140/2.1.4106.9764](https://doi.org/10.13140/2.1.4106.9764)

Woodlock, D. (2017). The abuse of technology in domestic violence and stalking. *Violence Against Women*, 23(5), 584–602. <https://doi.org/10.1177/1077801216646277>

Yale (2022) Yale Assure Lock 2®. <https://shopyalehome.com/pages/yale-assure-lock-2>

YWCA (2017) Technology And Gender-Based Violence. <https://www.ywca.org/wp-content/uploads/WWV-Technology-and-GBV-Fact-Sheet.pdf>

Zheng, P., Wang, z., Chen, C. & Khoo, L, P, (2019). A survey of smart product-service systems: Key aspects, challenges and future perspectives. *Advanced Engineering Informatics*. ScienceDirect. 42. <https://doi.org/10.1016/j.aei.2019.100973>

Legislação

DECRETO-LEI n.º 112/2009 de 16 de Setembro - Regime jurídico aplicável à prevenção da violência doméstica, à proteção e à assistência das suas vítimas

DECRETO-LEI n.º 48/95 artigo 152.º Violência doméstica