UNIVERSIDADE DA BEIRA INTERIOR
Ciências Sociais e Humanas

Cultura da vigilância em Portugal: perceções e práticas

Délcio Otávio Azevedo Faustino

Dissertação para obtenção do Grau de Mestre em
Sociologia: Exclusões e Políticas Sociais
(2º ciclo de estudos)

Orientadora: Profª. Doutora Maria João Simões

Covilhã, janeiro de 2020

Agradecimentos

Não é fácil agradecer a todos os que de alguma forma contribuíram para que eu pudesse completar esta etapa.

Começo por agradecer aos que sempre estiveram comigo desde que nasci - à minha família. Os valores que me foram transmitidos pelos meus pais foram, sem dúvida, fundamentais para todo o meu percurso.

Refletindo ainda sobre quem partilhou inúmeras vivências comigo na ilha de São Jorge, gostaria também de destacar duas pessoas fulcrais para o meu desenvolvimento como pessoa: Rui Pereira e Eduardo Guimarães. O primeiro acompanhou-me de perto desde o meu sétimo ano de escolaridade; ao longo de mais de 13 anos construímos uma relação de amizade difícil de adjetivar. Foste um dos pilares que me acompanhou sempre. Quanto ao professor Eduardo, faltam-me palavras para descrever tudo o que fez por mim. O professor foi, sem dúvida alguma, alguém que teve um profundo impacto na minha vida. A forma como sempre valorizou e estimulou a minha curiosidade, alicerçou as bases para que eu pudesse ser quem sou hoje.

Também gostaria de agradecer à Universidade da Beira Interior, especialmente ao Departamento de Sociologia. Aprendi imenso com o corpo docente, não esquecerei a forma como sempre se disponibilizaram para responder às minhas questões e me transmitiram o seu conhecimento. Há, no entanto, uma professora que merece um apreço especial - a Professora Doutora Maria João Simões. Agradeço-lhe pelo tempo que despendeu comigo e pelos seus conselhos. A sua disponibilidade, o seu profissionalismo e a forma como me orientou, fizeram com que o desenvolvimento desta dissertação fosse extremamente rico em termos científicos e pedagógicos.

Por último, uma palavra de apreço para todos os amigos(as) que conheci ao longo do meu percurso académico. Todos contribuíram para que esta etapa seja recordada com agrado.

Resumo

A vigilância eletrónica pode ser entendida como qualquer processo de recolha, em contexto eletrónico, sistemático, rotineiro e concentrado de dados pessoais para um determinado propósito. Como revelou Edward Snowden, atualmente a vigilância eletrónica já não é somente direcionada a alvos considerados suspeitos, abarca quase todos os cidadãos. Num contexto onde a quantidade de dados que são gerados pelos utilizadores é gigantesca, o acesso a esses dados é cada vez mais importante para diversas entidades. O facto da National Security Agency (NSA), uma entidade governamental, já possuidora de uma enorme quantidade de dados, ter conseguido aceder a dados fornecidos por diversas empresas multinacionais como, por exemplo, o Facebook e a Google, chocou e alertou ainda mais o mundo para a vigilância eletrónica. Porém, os cidadãos já não podem ser vistos apenas como agentes passivos no contexto desta, tanto podem, em certa medida, negociá-la ou tentar resistir-lhe como também exercê-la sobre outros, como ocorre nos casos da vigilância inversa e lateral. Nesta investigação seguiu-se, em grande medida, as questões levantadas pela conceção teórica da vigilância como cultura, procurando-se explorar o papel dos cidadãos nesta. Os objetivos desta investigação são: por um lado, captar o modo como as pessoas percecionam e experienciam a vigilância eletrónica, e por outro, analisar as suas práticas face à vigilância. A metodologia adotada é de carater qualitativo, tendo-se utilizado a entrevista semiestruturada como técnica de investigação.

Palavras-chave

Vigilância (eletrónica); *Big Data*; perceções sociais sobre vigilância; cultura da vigilância; práticas em relação à vigilância; estratégias de neutralização da vigilância;

Abstract

Electronic surveillance can be understood as any personal data collection process that is electronic, systematic, routinized and concentrated for a given purpose. As Edward Snowden revealed, nowadays electronic surveillance is no longer exclusively aimed at suspicious targets, it covers almost every citizen. In a context where the amount of user-generated-data is enormous, the access to that data is increasingly important to different entities. The fact that the National Security Agency (NSA), a government entity already possessing an enormous amount of data, was able to access data provided by several multinational companies such as Facebook and Google, shocked and further alerted the world about electronic surveillance. However, citizens can no longer be seen only as passive agents in the surveillance context, they can, to a certain extent, negotiate or try to resist it, as well as surveil others, as in the case of reverse and lateral surveillance. This investigation followed, to a large extent, the questions raised by the theoretical approach of surveillance as culture, aiming to explore the role that citizens have in it. The objectives of this investigation are, on one hand, to explore how individuals perceive and experience electronic surveillance, and on the other, to analyse their practices concerning surveillance. This research was based on a qualitative methodology, the chosen technique was the semi-structured interview.

Keywords

Electronic Surveillance; Big Data; perceptions about surveillance; culture of surveillance; surveillance practices; neutralization strategies

Índice

Lista de Tabelas

Introdução

A vigilância não é uma novidade. De facto, sabe-se que foi sendo exercida ao longo da História, havendo registos do seu funcionamento em civilizações antigas. A importância de ter um "vigia" era altamente valorizada nestas civilizações devido a motivos securitários, de controlo de subordinados no trabalho e de recolha de taxas, importando referir que esta vigilância era direta pois, antes da invenção da escrita, baseava-se principalmente na observação dos sujeitos. A partir do século XVIII começou-se a recolher e manter, de modo mais centralizado e sistemático, dados, em dossiers, sobre vários indicadores sociais. Esta centralização provou ser especialmente benéfica para os governantes (Giddens, 1990). Já no século XX, em particular nas suas últimas décadas, os incrementos na eficácia e na produtividade que uma recolha mais sistemática possibilitava, estimularam o desenvolvimento contínuo de novos artefactos vigilantes (Lyon, 1994; Weller, 2012).

Através destes tornou-se possível exercer vigilância de uma forma mais indireta. Foram surgindo diversos artefactos como os gravadores de voz, as câmaras de vigilância, entre outros que a possibilitaram. Poder-se-á argumentar que esta sofisticação e os (potenciais) impactos gerados estimularam o interesse sociológico sobre este processo. Nas décadas de 70 e 80, assistiu-se à publicação de algumas das obras mais influentes sobre a vigilância, como por exemplo as de James Rule, Michael Foucault e Anthony Giddens (Lyon, 1994).

Lyon (1994), dado o aumento e sofisticação dos artefactos surgidos assim como o aumento das suas modalidades, referia-se a um aumento intensivo e extensivo da vigilância. Na década de 90, percebeu-se que diversas atividades mundanas como por exemplo: levantar dinheiro; realizar uma chamada telefónica ou utilizar um cartão de crédito, eram registadas e analisadas por várias entidades.

No contexto atual, o uso mais generalizado da internet no mundo ocidental, possibilita novas formas de monitorização. Veja-se por exemplo a ascensão do *display advertising,* baseado no histórico da navegação *online*, ou da utilização de algoritmos cada vez mais sofisticados. Passou-se de um contexto no qual apenas uma parte do nosso quotidiano era monitorizada, para outro no qual o nosso quotidiano é quase constantemente monitorizado (Marx, 2016; Lyon, 2018).

Outra alteração significativa na vigilância, nos últimos anos, prende-se com os seus alvos, enquanto esta inicialmente visava apenas os que eram suspeitos, passou a abarcar, como referiu Snowden, todos os cidadãos. Este também chamou a nossa atenção para o facto de vários dispositivos, que utilizamos todos os dias, serem fornecedores de dados para as entidades vigilantes. Após estas revelações, tornou-se cada vez mais claro que, quer se queira, quer não, não temos alternativa se não lidar com a vigilância e acabar por, em grande medida, fornecer

dados às referidas entidades (Dijck, 2014; Harding, 2014). Além das alterações acima referidas, a incorporação do *Big Data* na vigilância permite que a classificação e categorização de cidadãos em determinados grupos, seja cada vez mais fácil para as grandes empresas e entidades governamentais. Algo que tem levantado diversas questões relacionadas com o aprofundamento de desigualdades sociais (Lyon, 2018).

No entanto, apesar das assimetrias claras de poder existentes entre os cidadãos e as entidades vigilantes, estes não podem ser vistos como meramente passivos perante a vigilância (eletrónica). De facto, a grande maioria dos cidadãos participa ativamente nos processos de vigilância, podendo pactuar com esta, ou/e negociá-la, ou/e tentar resistir-lhe ou/e até exercê-la sobre outros. O cidadão comum nunca contribuiu tanto para a vigilância como no contexto atual. Atualmente a vigilância massificada é possibilitada pelos nossos próprios cliques em diversos websites, pelas mensagens que trocamos e pela nossa atividade nas redes sociais. O conteúdo gerado pelo utilizador adquiriu, portanto, um papel central na vigilância eletrónica atual (Lyon, 2018).

Não há atualmente dúvidas de que a vigilância está integrada na nossa vida quotidiana, por essa razão, há uma série de questões que merecem ser aprofundadas, como por exemplo: o que é que as pessoas pensam sobre a vigilância? Em que situações fornecem (ou não) os seus dados pessoais? Será a vigilância positiva ou negativa? Até que ponto se negoceia\pactua com a vigilância? Quais são as consequências da vigilância? Estas questões orientaram o desenvolvimento desta investigação.

Seguindo as ideias de Lyon (2018) relativamente à sua conceção teórica da vigilância como cultura, esta investigação tenta dar um contributo às questões referidas acima. Para o fazer, tem-se em conta dois objetivos gerais: por um lado, explorar perceções que os cidadãos tenham em relação à vigilância eletrónica; e por outro, aferir a forma como agem perante ela. Para dar resposta aos objetivos gerais formularam-se sete objetivos específicos:

i) Analisar a consciencialização que os indivíduos têm sobre a vigilância eletrónica;
ii) Perceber em que situações cedem (ou não) os seus dados pessoais;
iii) Analisar que mecanismos de recolha conhecem, assim como os modos do seu funcionamento;
iv) Captar os aspetos considerados positivos e negativos da vigilância;
v) Analisar as perceções em relação aos diferentes tipos de vigilância: lateral; governamental e comercial;
vi) Mapear as ações de negociação da vigilância e as razões para a sua utilização;
vii) Averiguar que consequências, da vigilância eletrónica, são identificadas pelos respondentes.

Embora exista, em termos internacionais, um número elevado de publicações científicas sobre a discussão teórica da vigilância, o número de investigações empíricas não é, ainda, muito

significativo (Zureik, 2007; Jansson, 2012). Se atentarmos em Portugal, o número de investigações sociológicas, com dados empíricos, sobre vigilância é bastante baixo. Esta investigação pode ser um pequeno contributo para a discussão científica sobre a vigilância em Portugal.

Quanto à estrutura, esta dissertação divide-se em duas partes, sendo a primeira dedicada à revisão bibliográfica e a segunda referente à parte empírica. A primeira parte é constituída por dois capítulos. No primeiro exploram-se alguns aspetos teóricos e conceptuais sobre a vigilância, assim como a sua evolução e os tipos de vigilância existentes. No Capítulo 2, disserta-se sobre o papel mais ou menos ativo que os cidadãos têm na vigilância, abordando-se as formas como estes podem pactuar ou tentar resistir-lhe.

A segunda parte é constituída pelos Capítulos 3 e 4. No terceiro capítulo, apresenta-se o procedimento metodológico da investigação. Neste clarifica-se a metodologia, a técnica, e a seleção e caracterização dos indivíduos alvo do estudo população-alvo. Por último, no Capítulo 4, apresenta-se a análise e interpretação dos resultados organizados por dimensão de análise.

I – Enquadramento Teórico

Capítulo 1- Em Torno dos Conceitos e Aspetos Teóricos Centrais

Este capítulo, no qual se apresentam os aspetos teóricos fundamentais sobre a vigilância eletrónica, subdivide-se em três secções. Na primeira secção abordam-se diversos conceitos e distinções sobre a vigilância; começa-se por apresentar a origem do termo vigilância e o modo como o conceito se foi alterando em função dos novos desenvolvimentos tecnológicos. De seguida explora-se a evolução dos processos de vigilância, em particular, nas últimas décadas, dividindo-a em quatro períodos. Por último, disserta-se sobre os aspetos positivos e negativos da vigilância.

1.1 - Conceitos e Distinções sobre a Vigilância

Gary Marx (2015), referindo-se à origem do termo vigilância em inglês *surveillance* afirma que a palavra tem a sua raiz latina em *vigilare,* um termo que pressupunha uma certa conotação a algo vagamente sinistro ou ameaçador que podia ser resolvido através de um vigilante. Este significado antigo é refletido na associação, que ainda se efetua, entre, por um lado, atividades policiais e de agências de segurança nacional e, por outro, a vigilância. A ligação entre esta e a segurança é histórica, as práticas de vigilância podem ser rastreadas em civilizações antigas, como vários exemplos o demonstram. Na Bíblia podemos encontrar várias referências à importância de ter um vigia. Os líderes do Antigo Egipto mantinham registos para propósitos de impostos, serviço militar e imigração. Também o povo Israelita realizou censos registando nomes e idades dos membros de cada tribo e clã, tais registos possibilitavam a obtenção, por parte dos seus líderes, do número de indivíduos que estavam prontos para combater (Lyon, 1994; Bauman e Lyon, 2013).

Apesar de ainda se estar longe de alcançar um *state of art* que defina vigilância de forma mais uniforme (Fuchs, 2011), existem algumas definições que importa destacar. Dentro da discussão sociológica da vigilância podem-se encontrar várias tentativas de definição da vigilância. Jeness *et al.* (2007) defendem que a vigilância tem sido entendida na sociologia como o processo de ver, monitorizar, gravar e processar o comportamento de pessoas, objetos e eventos com o objetivo de governar a atividade social. Na opinião dos autores, esta abordagem sociológica vem desde trabalhos clássicos como os de Karl Marx, Max Weber e Georg Simmel até trabalhos mais contemporâneos como os de Michel Foucault, Anthony Giddens e Gary Marx. Em publicações mais recentes podem-se encontrar inúmeras outras definições, que apesar de

conterem pequenas diferenças, não variam muito da apresentada por Jeness *et al*. (2007). Lyon, um dos autores mais influentes nos estudos da vigilância, afirmou que a vigilância pode ser entendida como qualquer processo de recolha sistemática, rotineira e concentrada de dados pessoais para um determinado propósito (Lyon 2007, 2014). Já Fuchs (2011) faz questão de distinguir entre recolha de informação e vigilância. Para o autor a vigilância é um processo menos abrangente que a recolha de informação. Nas suas palavras, a vigilância é um "processo específico dentro da recolha de informação que pressupõe a recolha, o armazenamento, a avaliação e a utilização de informação que envolve danos potenciais ou já existentes, coerção, violência, relações de poder assimétricas, controlo, manipulação, dominação e poder disciplinar" (Fuchs, 2011, pp.126), algo que expressa a sua visão acentuadamente negativa sobre a vigilância.

É importante salientar que a vigilância é um processo característico de sistemas sociais com fronteiras e informação, não é um processo limitado a governos, espionagem ou secretismo (Marx, 2015). Neste sentido é importante distinguir vigilância não-estratégica de vigilância estratégica. A primeira, está relacionada com a rotina, é semiconsciente e está intimamente ligada aos nossos instintos. Através dela podemos captar, através dos nossos sentidos, sinais que podem evitar determinados perigos, como por exemplo a capacidade para detetar fumo ou barulhos, que possam ser ameaçadores. Por sua vez, a vigilância estratégica envolve uma estratégia consciente para recolher informação que pode ser de uma forma cooperativa ou não. Dentro da vigilância estratégica podem-se identificar dois mecanismos destinados a criar ou proibir condições de visibilidade e legibilidade da vigilância: as ferramentas materiais que aumentam (ou bloqueiam) a monitorização e os mecanismos que regulamentam a vigilância (Marx, 2015).

É também possível e fundamental, na contemporaneidade, distinguir entre a "vigilância tradicional" e a "nova vigilância". A nova vigilância pode ser definida como o escrutínio de indivíduos, grupos e contextos baseado na utilização de meios técnicos para extrair ou criar informação. A nova vigilância tende a ser mais intensiva e extensiva, baseia-se nas potencialidades do *Big Data*, esta é, portanto: (i) menos visível; (ii) envolve frequentemente uma conformidade involuntária; (iii) tende a baixar o custo dos processos de vigilância, e, por último, (iv) consegue alcançar localizações mais remotas (Marx, 2015). Alguns exemplos desta nova vigilância incluem câmaras de vigilância, sistemas de GPS, análise da relação entre diversos conjuntos dados, entre outros. A utilização de meios técnicos amplia drasticamente a quantidade de dados recolhidos e transmitidos aos detentores desses meios (Haggerty, 2006; Lyon, 2014). Esta amplificação da recolha pode envolver formas sofisticadas de manipulação, sedução, coerção, por exemplo. A partir dos novos meios técnicos podem ser criadas bases de dados, que influenciam a decisão sobre onde se deve concentrar maior atenção. Obviamente, estas bases de dados variam na sua utilidade, validade e fiabilidade. A definição de nova vigilância ignora a vigilância não tecnológica que faz parte do nosso quotidiano como olhar antes de atravessar a estrada, ou procurar a fonte de algum barulho repentino (Marx, 2015).

A utilização de contextos associados aos indivíduos demonstra que parte da vigilância contemporânea, além de ultrapassar a necessidade prévia de identificar o indivíduo, reconhece padrões de relações entre indivíduos e grupos. Frequentemente uma análise que implique cruzamento de dados, torna dados que por si só seriam irrelevantes, em dados revelantes. A coleção de dados de grupos ou a agregação de dados de um individuo num grupo oferece parâmetros que facilitam a categorização, a classificação, previsão e resposta; contudo são reconhecidas as limitações que as características, identificadas através de eventos do passado, têm em efetuar determinadas previsões sobre o indivíduo. Algumas categorizações e classificações, realizadas através destes cruzamentos de dados, podem ser imprecisas ou até erróneas (Lyon 2006; Marx, 2015).

Seguindo o pensamento de Gary Marx (2015), além da discussão sobre o conceito da vigilância em si, é importante identificar que outros conceitos são necessários para analisar as suas estruturas e processos. O contexto da vigilância reporta-se ao tipo de instituição e/ou organização que recolhe os dados, também fazem parte do contexto os objetivos, as regras e as expectativas, associadas à recolha. O agente de vigilância, refere-se ao observador, vigiador, requerente, inspetor, auditor, entre outros envolvido em processos de vigilância. Já ser sujeito da vigilância significa ser um indivíduo cuja informação é procurada pelo agente de vigilância.

Podemos encontrar vários tipos de agentes de vigilância. A vigilância organizacional é hierarquizada e exercida por organizações de grande dimensão em relação aos seus empregados, clientes ou público. Podendo-se distinguir, dentro desta categoria, entre vigilância interna e vigilância externa. A primeira refere-se ao escrutínio dos "insiders", ou seja, os indivíduos que integram determinada instituição ou organização. Já a segunda refere-se à monitorização de um contexto mais abrangente, onde se pode observar outras organizações/instituições, indivíduos e as tendências sociais (Marx, 2015).

Por outro lado, a vigilância não organizacional tem um carater informal e está regularmente associada a relações e papéis sociais, como por exemplo, entre membros de uma família (pais e filhos). A vigilância iniciada por um agente (vigilante), como o nome indica é iniciada por este e implica inspeções sobre o cumprimento da lei como, por exemplo, as inspeções a determinados veículos previstas pela legislação. A vigilância iniciada pelo indivíduo, é um tipo de vigilância que parte da sua iniciativa, como por exemplo aceitar participar em campanhas que recompensam o consumidor como os cartões de fidelidade. O agente (vigilante) e sujeito da vigilância podem por vezes misturar-se quando o próprio indivíduo decide vigiar-se a si próprio, um bom exemplo é o ato de fazer um teste de álcool em sua casa andes de conduzir. Por fim, a vigilância recíproca e não recíproca: a vigilância não é recíproca quando somente os dados do observado são transmitidos para o observador; é recíproca quando se observa uma relação bidirecional como, por exemplo, em redes sociais online. É necessário ter em atenção que vigilância recíproca não significa necessariamente uma vigilância igualitária. A vigilância recíproca pode ainda ser assimétrica ou simétrica, os governos em sociedades democráticas

têm uma relação de vigilância recíproca com os seus cidadãos, não significando que esta seja simétrica ou igualitária (Marx, 2015).

No contexto atual é fundamental definir os conceitos de *Big Data* e *metadata* dada a importância que estes conceitos adquiriram recentemente. Desde as revelações de Edward Snowden sobre a *National Security Agency* (NSA), têm sido realizados vários estudos que exploram a relação entre *Big Data* e vigilância (Lyon, 2014; Marx, 2015). Os *metadata* são dados, registados de forma automática, que incluem quem comunicou com quem, de que localização e por quanto tempo. Os *metadata* nunca incluem o conteúdo dessas comunicações, por essa razão são por vezes entendidos como sendo "dados dos dados" recolhidos (Dijck, 2014; Lyon 2014). O *Big Data* pode ser definido como capacidade de procurar, agregar e efetuar referências cruzadas entre conjuntos enormes de data, utilizando uma série de práticas, técnicas e *softwares*. Pode ser utilizado em vários contextos, como o marketing, o policiamento urbano e estratégias antiterrorismo. Apesar da forte relação entre os dois conceitos importa esclarecer que os *metadata* fornecem apenas dados com informações básicas de uma determinada comunicação digital que, por si só, não permite a identificação de determinados padrões e tendências, ao contrário do que acontece com o *Big Data* (Lyon, 2014).

Torna-se então pertinente refletir sobre as fontes de dados para o *Big Data*. Nos estudos da vigilância, as fontes de dados para o *Big Data* podem ser analisadas a três níveis: direcionadas, automatizadas e captadas numa base voluntária. Nas fontes direcionadas, os dados são obtidos de forma claramente percetível e recolhidas por um operador humano. Nas automatizadas os dados são recolhidos sem um operador humano intervir, são gravados registos de transferências rotineiras como, por exemplo, as bancárias e outras relacionadas com o consumo e comunicações. Nas terceiras fontes, entendidas como voluntárias, pressupõe-se a recolha de dados autorizada em *websites* como as redes sociais (Lyon, 2014).

Outro conceito fundamental para o estudo da nova vigilância é o *social sorting*. O *social sorting* refere-se ao ato de classificar indivíduos e agrupá-los em categorias com base na recolha de determinados dados provenientes de processos de vigilância. A classificação da vida humana é uma necessidade antiga, a novidade prende-se com a forma virtual e automatizada como a *social sorting* funciona atualmente. As classificações que resultam deste processo são concebidas para permitir ou barrar o acesso e participação a determinados eventos, experiências ou processos. Desta forma, estas classificações podem influenciar populações e indivíduos de forma direta ou indireta, condicionando as escolhas e as hipóteses das pessoas em causa. A digitalização dos sistemas de vigilância possibilitou um *social sorting* automatizado, obtido por códigos e algoritmos complexos. A automatização deste processo levanta questões ao nível da desumanização da vigilância, já que apenas se recolhe e analisa dados sem se ter em conta o contexto sociocultural, desde a criação dos dados até à análise dos mesmos (Lyon, 2006).

O tratamento diferenciado motivado pelo *social sorting*, especialmente o que utiliza o *Big Data*, tende a reforçar marginalizações e desvantagens já existentes. As populações marginalizadas, se forem identificadas por algoritmos preditivos, podem ser sujeitas a uma quantidade maior de processos de vigilância com impactos prejudiciais ao indivíduo, sejam eles exercidos por agentes (vigilantes) do domínio público ou do privado (Lyon, 2019). Além da potencial discriminação, existe a hipótese de ocorrer uma análise errónea de dados pessoais, podendo-se agrupar indivíduos em categorias erradas (Park, Chung e Shin, 2018).

Apesar do *social sorting* poder contribuir para aspetos positivos, como por exemplo, no caso da vigilância comercial, possibilitar que sejam oferecidas promoções e sugestões personalizadas que tendem a beneficiar mais os consumidores quando comparadas com promoções e sugestões sem suporte do *social sorting*, a possível discriminação, resultante deste processo, levanta questões importantes sobre desigualdade social, nomeadamente ao nível da sua intensificação e manutenção (Lyon, 2019).

1.2 - Evolução dos Processos de Vigilância

Os processos de vigilância têm estado em constante evolução, a partir do século XVIII, começou-se, de um modo mais sistemático, a recolher e manter registos sobre o número de nascimentos, casamentos e mortes de forma mais centralizada (Giddens, 1990). No campo económico privado, as empresas modernas começaram a monitorizar o trabalho e a manter registos precisos sobre o progresso dos seus trabalhadores. Desde então têm-se assistido a uma sofisticação da quantidade e precisão de dados recolhidos por processos de vigilância devido aos desenvolvimentos tecnológicos, em que destacamos o desenvolvimento meteórico da vigilância eletrónica. A prática da vigilância não é uma novidade dos últimos anos, as formas de intercetar comunicações já faziam parte de métodos utilizados por agências de espionagem e por serviços secretos. No entanto, a vigilância atingiu, no século XX, dimensões nunca antes vistas. Destacam-se algumas alterações, mais significativas, que ocorreram durante este período. Uma alteração fundamental foi o facto de as rotinas do quotidiano passarem a ser alvo de processos de vigilância. Nunca o quotidiano de o cidadão comum havia sido alvo de um escrutínio tão forte e abrangente na história da civilização humana (Lyon, 1994; Weller 2012). Apesar da vigilância ser um processo social antigo, nos últimos 40 anos, ela emergiu como prática dominante de organização da nossa sociedade. Esta alteração fundamental, assinalou o ponto de partida para a compreensão e análise crítica dos desenvolvimentos da vigilância (Lyon, Haggerty e Ball, 2012). A expansão da vigilância foi de tal forma intensa e abrangente que alguns autores denominaram a nossa sociedade de Sociedade da Vigilância (Lyon, 1994; Wood, 2009).

Para pormenorizar a evolução, mais recente, dos processos de vigilância, podem-se identificar períodos nos quais os processos de vigilância e o seu uso mudaram significativamente. Optou-

se destacar quatro: as décadas de 60 e 70; a década de 90; o pós-11 de setembro de 2001 e, por último, o período pós-revelações de Snowden.

Nas décadas de 60 e 70 o foco estava nos EUA, o contexto mundial era de crise generalizada, motivada pelo fim do colonialismo, a Guerra Fria e a do Vietnam, e ainda a crise de instituições modernas. Nos Estados Unidos da América (EUA) dois medos distintos, mas relacionados, estavam presentes na população. O medo de uma desordem distópica, e o pesadelo da ordem imposta por processos de vigilância semelhantes aos presentes no *Big Brother* Orwelliano (Wood, 2009).

Quanto ao primeiro medo, nestas décadas a população americana estava preocupada com diversas ameaças, as que o comunismo poderia trazer, as provocadas pelo ativismo radical da população negra e ainda os protestos contra a guerra do Vietname. Após uma série de protestos violentos, como o caso de Watts, o pânico moral era visível nos EUA (Wood, 2009).

Os governos americanos atuaram para tentar apaziguar a situação, adotando um planeamento urbano defensivo e uma postura de vigilância mais musculada, esta postura motivou o segundo medo referido, o medo do próprio Estado. Nas décadas de 60 e 70 dois presidentes tentaram estabelecer uma nova base de dados central e estatal de informação pessoal, esta seria possibilitada pelo desenvolvimento dos computadores (Wood, 2009; Lauer, 2012). Algo que, juntamente com situações de monitorização governamental, gerou uma onda de críticas relacionadas com a invasão de privacidade dos cidadãos, algo relacionado com o elevado número de abusos e até crimes por pessoas ligadas ao Estado que decorreram neste período. O escândalo de Watergate e a descoberta de listas de vigilância que continham alvos duvidosos, como por exemplo, todos os estudantes negros que estavam envolvidos em sindicatos, intensificaram este medo (Wood, 2009).

Importa também referir o desenvolvimento da vigilância na década de 90. Este foi profundamente marcado pelas câmaras de vigilância e pela disponibilização da internet ao público. Os desenvolvimentos que decorreram nesta década estão fundamentalmente ligados ao Reino Unido e à sua utilização em massa de câmaras de vigilância em espaço aberto, que tornaram o Reino Unido o arquétipo da "sociedade da vigilância". Os principais motivos para o financiamento desta tecnologia de vigilância foram: os atos de terrorismo por parte do Exército Republicano Irlandês (mais conhecido por IRA); o hooliganismo no futebol e alguns crimes com forte cobertura mediática contra crianças (Wood, 2009). De acordo com Germain, Dumoulin e Douillet (2013), a difusão das câmaras de vigilância resultou também da intenção de vários partidos políticos anunciarem preocupações com a segurança da população, de interesses governamentais em fortalecer parcerias público-privadas (caso do Reino Unido), do crescimento do mercado das tecnologias de segurança, entre outros. A falta de regulamentação sobre as câmaras de vigilância em locais públicos na região e a falta de estudos que comprovassem a sua capacidade para combater o crime, levaram a população a criticar o seu uso (Germain, Dumoulin e Douillet, 2013).

Outra tecnologia que passou a estar ao alcance do público nesta década foi a internet, tecnologia que iria ter uma influência decisiva no desenvolvimento da vigilância eletrónica. A partir da sua disponibilização, as capacidades para diversos agentes exercerem vigilância aumentaram exponencialmente. O papel global da internet como fornecedor de informações, ideias, imagens e dados aumentou significativamente as possibilidades de vigilância. A partir do seu surgimento, houve também mudanças ao nível do papel dos consumidores na vigilância. As compras disponibilizadas online significaram que imensos dados pessoais circulavam numa escala massiva. Quem tinha acesso e quem poderia assegurar e proteger estes dados tornou-se uma questão central (Lyon, 2007).

Ainda que o aparecimento da internet tenha aumentado a capacidade para se exercer vigilância, houve um evento que mudou a forma como a vigilância eletrónica passou a ser vista, os ataques terroristas no dia 11 de setembro de 2001. De acordo com Lyon (2003), os eventos do 11 de setembro podem ser vistos como revelantes e como constituindo uma mudança social significativa. Os ataques tornaram evidentes uma série de tendências da vigilância que se estavam a desenvolver despercebidas. O autor afirma que o estabelecimento de sociedades da vigilância já estava em curso muito antes destes eventos que chocaram o mundo. Até àquela data, as tecnologias de *data-mining* já estavam disponíveis. Antes dos ataques, as empresas de tecnologia incitavam a utilização de sistemas integrados para identificar e revistar pessoas em larga escala em locais como os aeroportos e fronteiras, porém, não parecia haver motivos plausíveis para que se aplicasse este tipo de tecnologias cuja implementação iria implicar custos elevados (Lyon, 2003). Após o 11 de setembro iniciou-se uma tendência a que Marx (2015) denominou de tentativas para a criação do mito da vigilância, estas são tentativas de gerar medos que justifiquem a necessidade para o aumento dos processos de vigilância, sendo que as alegações que estes são mais eficazes do que realmente são também fazem parte das referidas tentativas. Estas prolongaram-se no tempo, por exemplo, num contexto mais recente, em 2013, a administração de Barack Obama afirmou que as invasões de privacidade provocadas pelo programa de vigilância "PRISM" valeram a pena. Apesar da relação entre maiores níveis de segurança e maior número de dispositivos de vigilância ainda não ter sido comprovada cientificamente (Marx, 2015; Hong, 2017).

Voltando à discussão sobre a importância do 11 de setembro para a história da vigilância, verificou-se que após o evento, financiar projetos de tecnologias de vigilância foi entendido, por alguns setores, como a resposta mais adequada. Começou-se a dirigir fundos públicos para esse fim, algo que provocou um incremento significativo no desenvolvimento dessas tecnologias (Lyon, 2003; Gandy, 2007). Uma panóplia de dispositivos que incluem as câmaras de vigilância com reconhecimento facial, e o desenvolvimento de dados biométricos, os cartões de identificação eletrónicos, entre outros, começou a ser produzida e utilizada globalmente, sendo a sua utilização justificada pela alegada prevenção de novos ataques terroristas (Lyon, 2003).

Outras reações aos eventos envolveram duas tendências importantes, por um lado, a convergência ou integração de diferentes sistemas de vigilância e, por outro, a sua globalização, possibilitada, em grande medida, pela utilização de métodos similares pela maioria dos países ocidentais. Alguns exemplos indicativos da convergência e integração dos sistemas de vigilância, de uma forma globalizada, incluem a recolha, a partir desse momento obrigatória, de dados pessoais dos passageiros aéreos e o aumento no número de comunicações via internet. A aplicação, globalizada, destes sistemas de vigilância gerou, também, um aumento significativo dos dados recolhidos por entidades governamentais (Lyon, 2003).

Neste período ocorreu uma mudança na balança entre vigilância policial e os direitos de privacidade dos cidadãos. As novas tecnologias de vigilância que surgiram após o 11 de setembro contribuíram para que os agentes de vigilância pudessem agora exercer processos de vigilância eletrónica numa escala global, com um grau de intrusão física muito menor (Bloss, 2007). Os indivíduos têm menos noção das formas de vigilância que não envolvem contacto ou observação direta. No controlo de segurança de um aeroporto são visíveis e fáceis de identificar vários mecanismos de vigilância, enquanto que, por exemplo, na utilização de cartões de fidelização ou de aplicações móveis, a sua identificação não é tão fácil, a presença deste tipo de vigilância, não visível diretamente, e escapa mais facilmente à perceção dos utilizadores (Lyon, 2009). Algo que está diretamente relacionado com a tendência recente de "amolecimento" ou "suavização" da vigilância, uma vez que a coerção direta tradicional, é substituída por processos de vigilância com graus de manipulação e persuasão mais reduzidos e menos invasivos (Marx, 2015). As agências governamentais e as empresas começaram a adotar uma estratégia na qual recolhem informação pessoal pedindo autorização aos cidadãos ou oferecendo-lhes determinados benefícios, ao invés da lógica tradicional de coerção direta (Marx, 2006).

Mais recentemente ocorreu um outro evento que viria marcar a história da vigilância eletrónica, as revelações do *whistleblower* Edward Snowden. As revelações de Snowden sobre a *National Security Agency* (NSA), em junho de 2013, tiveram um enorme impacto nos processos de vigilância. Snowden era funcionário da NSA na altura que considerou que os processos de vigilância exercidos pela instituição estavam a violar aspetos fundamentais do direito à privacidade dos cidadãos. Snowden revelou que as agências e departamentos governamentais não estavam só a direcionar os processos de vigilância a alvos suspeitos ou considerados importantes, os alvos eram todos os cidadãos americanos e ainda alguns estrangeiros (Dijck, 2014; Harding, 2014).

As agências ou serviços secretos pareciam ter perdido o controlo, facto que se pode atribuir, em grande medida, ao pânico político que se seguiu aos eventos de 11 de setembro (Harding, 2014). As revelações de Snowden tornaram o conceito de *Big Data* num aspeto fundamental dos estudos da vigilância. As suas revelações demostraram que os governos podem monitorizar os seus cidadãos de forma mais sofisticada através da utilização do *Big Data,* não se limitando à quantidade de dados que são recolhidos pelos próprios governos. Desvendou-se que agências governamentais podiam e obtinham dados através de empresas privadas e de fornecedores de

internet ou telecomunicações. Estes dados, frequentemente gerados pelos utilizadores, incluem por exemplo, *log-ins*, cookies, dados produzidos nos telemóveis, localizações geográficas, entre outros. Uma das maiores questões relacionadas com este acontecimento, foi a recolha e análise destes dados sem que os utilizadores estivessem cientes dessa possibilidade. Um tipo de vigilância massificado e "sem suspeição" foi revelado para o grande público (Lyon, 2014, 2015, 2018).

Após as revelações chocantes do ex-funcionário da NSA, pode-se identificar uma série de eventos que foram, em boa medida, causados por aquelas. O facto de a produção de artefactos de vigilância constituir uma indústria, também ficou claro perante o envolvimento de empresas multinacionais, frequentemente com ligações aos governos, nos processos de vigilância. Estas ligações dissiparam quaisquer dúvidas que ainda prevalecessem sobre essa associação. O choque inicial prendeu-se com o facto de uma agência governamental (NSA) ter acesso a dados provenientes de empresas de telecomunicações. Descobriu-se que empresas multinacionais de software e serviços online como a Apple, Google, Microsoft, Amazon e Facebook, não só recolhiam dados, em grande escala, dos seus utilizadores como também partilhavam esses dados com agências governamentais (Lyon, 2018).

As revelações motivaram, também, debates sobre questões relacionadas com os direitos digitais e a sua relação com empresas e departamentos/agências governamentais. Quem tem a responsabilidade pelos fluxos de dados que ultrapassam fronteiras que têm consequências nas oportunidades de vida e liberdades dos cidadãos? Talvez o maior aspeto a reter das revelações de Snowden, foi que os dados que estavam implicados nestas revelações haviam sido criados principalmente por utilizadores comuns da internet através dos seus telemóveis e outros dispositivos integrados no nosso quotidiano. Tornou-se claro que o quotidiano do cidadão comum se encontrava sob um escrutínio que constituía uma situação de invasão de privacidade (Lyon, 2018).

O pós-revelações de Snowden, é também marcado pelo facto de os cidadãos começarem a adotar diversas medidas para se protegerem da vigilância. Os resultados de um relatório, elaborado por Rainie e Madden (2015) sobre as estratégias de privacidade dos Americanos após as referidas revelações, apontaram para uma percentagem significativa (25%) de Americanos, conscientes de programas de vigilância, que adotaram diversas estratégias para protegerem a sua privacidade, especialmente na utilização de telemóveis, de *email*, e dos motores de busca online. Nas conclusões do relatório, identificou-se uma relação entre o conhecimento obtido sobre a vigilância eletrónica e o comportamento dos utilizadores da internet, sendo que os que tinham mais conhecimento sobre a vigilância, eram os que mais facilmente adotam estratégias para proteger a sua privacidade.

O grande público passou a estar informado que o que acontece nas redes sociais está aberto ao escrutínio por parte de empresas e governos. A crença que se podia confiar nas grandes

empresas para que protegessem os nossos dados pessoais sofreu um enorme golpe, algo que teve impacto significativo no comportamento de muitos cidadãos.

Outro aspeto que é fundamental referir é a resposta do público, que além dos primeiros sinais de alteração do comportamento mencionado, apoiou de forma massiva Snowden. O objetivo dele foi sempre claro, não se tratava de um ato de espionagem ou de uma intenção de ameaçar as atividades da NSA, Snowden queria apenas gerar um debate sobre a forma como os dados pessoais dos cidadãos comuns circulavam (Harding, 2014; Lyon, 2018).

As revelações de Snowden atingiram uma dimensão raramente vista neste tipo de denúncias. Algo que se pode atribuir ao seu conhecimento técnico dos processos de vigilância e também à estratégia utilizada para a divulgação das suas revelações. A sua colaboração com jornalistas ao invés de simplesmente expor os factos sozinho, maximizou o alcance das suas revelações (Lyon, 2018). Este acontecimento causou um forte abanão na discussão em torno da vigilância e das suas potencialidades. No pós-revelações de Snowden alguns autores referência no estudo da vigilância, como por exemplo Dijck (2014) e Lyon (2014), refletiram aprofundadamente sobre algumas tendências que estavam a ocorrer na vigilância eletrónica.

Dijck (2014), chamou a atenção para a "dataficação" do comportamento social, esta refere-se à proliferação de aspetos da vida social que se tornaram quantificáveis. As amizades, interesses, pesquisas de informação online, entre muitas outras sociabilidades são facilmente quantificáveis através de plataformas da Web 2.0. A utilização de algoritmos por parte das principais redes sociais, tornam atividades sociais como "gostar" de algo ou criar amizades em algo quantificável, tornando também possível a sua análise por algoritmos. A capacidade para aceder, compreender e monitorizar o comportamento dos indivíduos através da dataficação é cada vez mais vista como legítima. Devido a esta crescente quantificação, as empresas e governos podem realizar processos de monitorização em tempo real e realizar análises previsionais cada vez mais complexas.

Lyon (2014), relacionando a dataficação com a emergência de bases de dados cada vez maiores de dados pessoais, salientou a importância do *Big Data* e das tendências, a ele associadas, de automação e antecipação. Em relação à automação, o autor afirma que utilização do *Big Data* envolve um uso amplificado de algoritmos para fins analíticos, uma maior confiança em software e na chamada relação humano-algorítmica; aspetos que ajudam a moldar as formas como os sujeitos da vigilância são tratados pelos sistemas de vigilância. Com o crescente desenvolvimento de software e a acessibilidade do seu preço, é previsível que a automação seja algo cada vez mais comum na vigilância com consequências, por enquanto, imprevisíveis. No entanto, parece óbvio, na perspetiva do autor, que a(s) entidade(s) que decidam sobre os algoritmos e as bases de dados terão uma grande importância nesta fase emergente da automação, visto que terão o poder de ditar o nível de automação dos processos de vigilância tal como a sua configuração, algo que poderá ter implicações éticas e nas dinâmicas de poder (Lyon, 2014). A automação também levanta questões em relação à fiabilidade das análises

feitas a partir de *metadata* e de algoritmos. Apesar da crença que os *metadata*, recolhidos através de diversas plataformas refletem o comportamento humano como ele é, os algoritmos utilizados pela Google, Twitter e outros sites, são intrinsecamente seletivos e manipulativos, tanto os utilizadores como os responsáveis pelas plataformas podem adulterar os dados. Por vezes, não se reflete sobre a possibilidade, por exemplo, de os utilizadores adulterarem os dados com determinadas intenções (Dijck, 2014; Lyon, 2014).

Segundo Lyon (2014), desde o final dos anos 90 que as técnicas de gestão de risco tendem a concentrar-se em tentativas de prever acontecimentos futuros. Trata-se de uma abordagem de antecipação analítica, onde o objetivo da recolha de dados é a identificação de "pessoas de interesse", mesmo que só o possam vir a ser no futuro (Dijck, 2014; Lyon, 2014; Topak, 2017). No entanto esta antecipação analítica baseia-se fortemente em processos de *social sorting*, portanto não é infalível. A antecipação analítica pode, por exemplo, envolver a identificação errónea de determinados ativistas como violentos, quando não o são, ou podem ser identificados indivíduos como sendo pobres merecedores de ação social, quando na verdade não cumprem os critérios para que recebam apoio da ação social. Esta tendência aliada à desumanização dos dados recolhidos, falhas e potenciais consequências, levanta questões ao nível do seu impacto na reprodução de desigualdades sociais como as de classe, género e etnicidade (Lyon, 2014).

1.3 – Os Aspetos Positivos e Negativos da Vigilância Eletrónica

Os investigadores da vigilância têm-se dividido em relação aos aspetos positivos e negativos que podem advir da vigilância. Alguns autores defendem que a vigilância só tem aspetos negativos enquanto outros autores afirmam que existem aspetos positivos e negativos na vigilância. É importante esclarecer, que quando se afirma que determinado desenvolvimento tecnológico pode ter simultaneamente aspetos positivos e negativos, não se está a afirmar que estamos perante uma tecnologia neutra (Lyon e Bauman, 2013). As tecnologias não são ferramentas neutras cuja orientação moral é revelada apenas na sua utilização, todo o desenvolvimento tecnológico é um produto de relações culturais, sociais e políticas que envolvem relações de poder, para o bem e para o mal. Citando Lyon, "a vigilância em si não é boa ou má, mas também nunca é neutra" (Lyon, 2018, pp.16).

As abordagens que vêm a vigilância como sendo, globalmente, negativa tendem a defini-la como uma recolha de dados sobre indivíduos ou grupos, que podem ser utilizados para controlar e disciplinar comportamentos. Alguns dos autores internacionalmente reconhecidos que adotaram uma abordagem similar foram: Ogura (2006), Foucault (1995) e Fuchs (2011). A vigilância é vista, nesta abordagem, como uma expressão de carater instrumental por estar baseada na ideia de que se monitoriza indivíduos e se recolhe dados sobre os seus comportamentos, ideias, entre outros aspetos da sua vida, para que se possa posteriormente

controlá-los e discipliná-los. A vigilância, segundo esta abordagem, opera através de ameaças e do medo, sendo uma forma de violência psicológica e estrutural que se pode tornar em violência física (Fuchs, 2011).

Para Fuchs (2011), a vigilância é sempre negativa, porque é sempre baseada numa lógica de competição. De acordo com o autor os processos de vigilância são utilizados para revelar ou prevenir determinados comportamentos de grupos ou indivíduos através da recolha, armazenamento, processamento, difusão, avaliação e utilização de dados de forma a que violência (potencial ou não) física, ideológica ou estrutural possa ser dirigida a humanos para influenciar o seu comportamento. A posição do autor é visível se atentarmos no seguinte excerto, no qual o autor comenta a forma como a vigilância influencia o comportamento dos cidadãos: "Esta influência é realizada através de meios coercivos e traz benefícios a certos grupos à custa de outros. A vigilância é na minha visão, portanto, nunca cooperativa ou solidária – nunca beneficia todos" (Fuchs, 2011:128). Apesar desta visão negativa da vigilância, o autor reconhece que é possível que determinadas recolhas de informação beneficiem todos os envolvidos, porém, na opinião do autor, esta recolha não deve ser considerada como vigilância uma vez que se verificam lógicas cooperativas e solidárias. Fuchs (2011) refere-se a processamentos de informação que envolvem assistência, solidariedade, ajuda e cooperação. Para o autor tais processamentos não fazem parte de os processos de vigilância visto que não envolvem violência sistemática, competição, dominação e tentam beneficiar todos. Alguns exemplos utilizados pelo autor para se referir a estes processos são: observação, por parte dos pais, do seu bebé com uma câmara para ver se ele precisa de ajuda, ou o sismógrafo para detetar terramotos atempadamente.

Por outro lado, há também visões que reconhecem que os processos de vigilância podem ter consequências positivas e negativas (Fuchs, 2011). Entre os autores que utilizam estes tipos de definições encontram-se cientistas reconhecidos nos estudos da vigilância como, Haggerty (2006), Zureik (2007), Marx (2016) e Lyon (2018). Estes conceitos da vigilância implicam, geralmente, que a vigilância é um fenómeno universal que se encontra em todas as sociedades. Alguns autores, chamam à atenção para a existência de abordagens demasiado concentradas na crítica da vigilância, afirmando que vários investigadores da vigilância têm dificuldade em reconhecer aspetos positivos da vigilância como, por exemplo, os seus contributos para controlar doenças infeciosas e para auxiliar no cuidado parental (Haggerty, 2006; Hong, 2017).

Segundo Lyon, a vigilância é quase sempre ambígua, os "processos que nos parecem restringir simultaneamente também nos permitem participar na sociedade" (Lyon, 1994, pp. ix) aludindo a processos de vigilância que nos permitem aceder ao Estado Social, mas que simultaneamente nos monitorizam. O autor já exemplificou que a vigilância pode ter aspetos positivos e negativos em diversos casos, vejamos por exemplo o caso de um paciente, com problemas de coração, que é alvo de monitorização remota na qual um dispositivo pode recolher dados sobre o quotidiano do paciente com grande facilidade, algo que possibilita uma vigilância intrusiva com alguns aspetos negativos, mas simultaneamente, oferece benefícios de saúde ao indivíduo. Mais

recentemente o autor também reconheceu que a monitorização exercida pelo comércio online pode ser benéfica, contudo alerta que apenas alguns consumidores conseguem reconhecer e aproveitar alguns dos benefícios oferecidos por esta nova economia (Lyon, 2006). Alguns contributos benéficos e positivos também incluem, na opinião de Lyon, os novos níveis de eficiência, produtividade, conveniência e conforto frequentemente permitidos por dispositivos de vigilância (Lyon, 2006). Também James Rule (2007) adota uma postura semelhante, afirmando que a vigilância varia entre o benigno e o repressivo, podendo auxiliar na saúde ou no combate ao terrorismo.

No âmbito desta dissertação, optou-se por seguir uma visão teórica que reconhece tanto os aspetos positivos como os negativos da vigilância eletrónica.

1.4 - As Três Principais Conceções Metafóricas da Vigilância

A vigilância tem estado associada a diversas metáforas. A metáfora distópica do *Big Brother*, foi inspirada pela obra *Nineteen Eighty-Four* de George Orwell publicada em 1949, foi uma das primeiras. O *Big Brother* representava o que poderia ser um governo com processos de vigilância massificados e omnipresentes (Lyon, 2018). A metáfora foi de tal forma popularizada, que se incorporou na linguagem do quotidiano. O adjetivo "orwelliano" começou a ser utilizado para representar um medo cultural de uma sociedade de vigilância total. Com a evolução da vigilância e das tecnologias que a facilitam, o cenário distópico orwelliano parecia agora ser passível de concretização. Surgiram várias análises políticas e sociológicas, sobre tendências totalitárias de Estados burocráticos, tal como a sua relação com as novas tecnologias, denotando-se a influência do estado de vigilância total que havia sido descrito do *Nineteen Eighty Four* (Lyon, 1994, 2006; Haggerty, 2006). No entanto, ainda nos anos 90, Lyon concluiu que o mundo estava a salvo deste cenário, visto que seria extremamente improvável que uma entidade concentrasse todos os dados provenientes da vigilância (Lyon, 1994).

O impacto da obra de Orwell, na opinião de Gary Marx (2012), deixou uma imagem ameaçadora, de um Estado todo poderoso e repressivo na mente coletiva de inúmeras pessoas. A sua importância e impacto não são ignorados na análise à vigilância dos últimos anos. No entanto, a metáfora do *Big Brother* limita a análise da vigilância ao concentrar-se num agente de vigilância tirano que ameaça os indivíduos com métodos de tortura e repressão acentuados. Alguns processos de vigilância podem-se assemelhar aos presentes no *Big Brother*, mas representam apenas uma pequena parte do que é, atualmente, a vigilância (Lyon, 2018).

Outra das metáforas mais famosas associadas à vigilância foi a do panótico, elaborada por Michel Foucault na sua obra *Surveiller et Punir* em 1975. Foucault elaborou a sua metáfora, ao aprofundar as ideias que Jeremy Bentham havia proposto, no século XVIII, com a estrutura arquitetónica a que denominou de panótico. Esta estrutura, desenvolvida para se aplicar em

prisões, era um edifício circular com uma torre de observação no centro e com celas ao seu redor. Este design utilizava um jogo de luzes para que fosse impossível, para os encarcerados identificar se estavam ou não a ser alvos de vigilância, enquanto, por outro lado, os funcionários da prisão poderiam facilmente identificá-los através da torre. Devido a esta incerteza, previa-se que os presos adotassem um comportamento menos problemático. A sua concretização significava algo que era central na teoria de Foucault, a imposição de disciplina de forma passiva. Foucault acreditava que era possível controlar populações humanas através de processos ou forças subtis e invisíveis (Foucault, 1995).

Com os desenvolvimentos tecnológicos mais recentes, depressa os investigadores da vigilância, relacionaram as ideias de Foucault com as novas possibilidades de vigilância. O panótico é frequentemente visto como um modelo que aprimorou em relação à visão Orwelliana a análise à vigilância. A capacidade que Foucault teve para situar a vigilância num contexto das teorias de poder foi um dos seus maiores contributos (Haggerty, 2006; Caluya, 2010). O "panoticismo" desenvolvido através da metáfora do panótico teve uma influência tão intensa, que David Lyon, afirmou figurativamente, que apesar do número elevado de críticas a que é sujeito, o panótico "recusa" desaparecer do debate da vigilância (Lyon, 2007; Henderson, Harmon e Houser, 2010; Elmer, 2012).

O panótico e as inúmeras variantes que baseou, como o superpanótico, panótico eletrónico, oligótico, panótico urbano, sinóptico, entre muitos outros marcaram uma era nos estudos da vigilância. No entanto, nenhuma destas alternativas parecia captar a realidade da sociedade nas últimas décadas, algo que motivou Haggerty (2006) a abandonar o modelo do panótico de uma vez, devia-se, na sua opinião, derrubar as paredes do panótico, afirmou metaforicamente (Haggerty, 2006). Lyon (2007) argumenta que apesar do conceito do panótico ser extremamente rico e multifacetado, há uma clara necessidade para que os estudos da vigilância ambicionem ir para além dos seus contributos.

Uma série de críticas ao panótico de Foucault, deixaram clara a incapacidade do panótico para captar a realidade dos últimos anos. Destacam-se, nesta secção, algumas das principais críticas proferidas por Haggerty (2006), Bauman e Lyon (2013) e Lyon (2014, 2018).

Em primeiro lugar, as alterações nos propósitos da vigilância ultrapassam as funções do panótico. As visões de Foucault relativamente aos usos da vigilância panótica concentravam-se em funções relacionadas com a educação, tratamento médico e punição. No entanto, assiste-se a uma expansão enorme nos seus propósitos que ultrapassam em muito os mencionados por Foucault. Os contextos nos quais a vigilância é utilizada incluem o consumo, o entretenimento, a promoção de saúde, a governança, o uso militar, entre outros. Afirmar que a vigilância serve apenas o propósito de controlo social é erróneo (Haggerty, 2006).

Em segundo lugar, a falha em reconhecer aspetos positivos da vigilância. A vigilância também pode resultar em projetos apreciáveis, observar outros ou expor-se pode ser considerado agradável e constituir uma parte da formação da identidade de indivíduos. A exposição em

blogs, redes sociais e a ascensão dos *reality shows* são um bom exemplo. A possibilidade de a vigilância ser apreciável ou libertadora não é captada pelo modelo do panótico (Haggerty, 2006; Lyon, 2018). A visão distópica de Foucault na qual todos os desenvolvimentos tecnológicos na vigilância são vistos como negativos é, agora, insuficiente. Capta apenas uma parte dos processos de vigilância.

Em terceiro lugar, o panótico não capta as alterações nas hierarquias de visibilidade. No modelo do panótico os alvos da vigilância são tipicamente pessoas que se encontram em posições mais baixas na hierarquia social. Os guardas que observam os prisioneiros e os médicos psiquiatras que o fazem com os seus pacientes são um exemplo da visão hierarquizada da vigilância panótica (Haggerty, 2006). Ainda que esta hierarquia se mantenha visível com o facto de instituições poderosas vigiarem grupos menos poderosos, as dinâmicas alteraram-se significativamente e reconfiguraram-se. A vigilância não é só direcionada aos menos poderosos, agora está presente em todos os segmentos da hierarquia social. Assiste-se a um contexto no qual o aumento da visibilidade dos mais poderosos contribui para que estes também sejam alvo de escrutínio. Apesar da vigilância continuar a ter um papel importante no estabelecimento e reforço de desigualdades sociais, os grupos mais poderosos podem agora ser alvo de um escrutínio maior quando comparados a outros grupos ou indivíduos menos poderosos (Haggerty, 2006). As novas tecnologias facilitaram o escrutínio dos mais poderosos, os *mass media* desempenham um papel vital nesta nova forma de escrutínio a que alguns autores chamam de sinótico, "onde os muitos são capazes de observar os poucos" invertendo a lógica sugerida pelo modelo do panótico (Bauman e Lyon, 2013:62).

Em quarto lugar, o panótico não abarca as alterações nas relações de poder. As alterações nas hierarquias de visibilidade estão intimamente ligadas às relações de poder nos processos de vigilância. As teorizações inspiradas no *Big Brother* ou no panótico pressupõem noções de um poder centralizado nas entidades vigilantes governamentais e nas grandes empresas, sendo o cenário atual algo diferente (Lyon, 2018). Lyon (2009), sem negar que a balança de poder está claramente inclinada para as instituições de maior dimensão, afirma que é importante atentar que a vigilância é um processo interativo. O que os sociólogos, especializados no estudo da tecnologia, chamam de co-construção aplica-se ao mundo da vigilância. Como referido anteriormente, os contextos nos quais acontecem processos de vigilância são fundamentais para a análise da vigilância. Se atentarmos em diferentes contextos, a forma como vemos e se exerce a vigilância muda significativamente. No contexto do cuidado parental, os agentes da vigilância (como os pais) podem sentir uma obrigação moral e responsabilidade legal de invadir a privacidade dos seus filhos para garantir o seu bem-estar (Marx, 2015), algo que, por exemplo, a série televisiva *Black Mirror* captou na perfeição no episódio "Arkangel" da sua quarta temporada (Brooker, 2017). No contexto dos contratos de trabalho, a vigilância fornece meios para os trabalhadores identificarem condições de trabalho injustas e pode ser decisiva na reivindicação contra as mesmas, ainda que, por outro lado, também possa servir para despedir trabalhadores ou excluí-los das entrevistas de trabalho (Guzik, 2017).

As dinâmicas de poder dos processos de vigilância podem-se alterar de inúmeras formas. Ao contrário do que o modelo do panótico sugere, as relações de poder na vigilância podem mudar com o decorrer do tempo. Marx (2016) dá um exemplo, no contexto do cuidado parental, no qual uma criança passa de sujeito da vigilância a agente de vigilância. A criança antes de se tornar adulta, é alvo de inúmeros processos de vigilância com o intuito de garantir o seu bem-estar. Porém, quando esta chega à idade adulta e forma o seu próprio lar, os processos de vigilância dos quais era alvo (postos em prática pelos seus pais) decrescem abruptamente. Com o decorrer do tempo a dinâmica de poder inicial até se pode reverter, se a criança (agora adulta) ficar com o papel de cuidadora dos seus pais idosos.

Os "Escândalos" como o das revelações de Snowden também são bons exemplos de como se pode assistir a alterações das dinâmicas de poder. Este escândalo levou a alterações nas leis de proteção de dados com a intenção de limitar a expansão dos processos de vigilância (Hong, 2017). Outros acontecimentos ou ações podem limitar a vigilância, por exemplo a *sousveillance* trouxe mudanças significativas nas dinâmicas de poder, também as medidas ou estratégias como as de neutralização da vigilância (exploradas no Capítulo 2) podem anular atividades de monitorização, ou pelo menos aumentar drasticamente o custo da vigilância, e, consequentemente, limitar o uso de determinados processos de vigilância. Alguns protestos contra determinados processos de vigilância podem ser facilitados através da disseminação da Web 2.0, como por exemplo, os *Cyber-Protest*. Os cidadãos, hoje, não estão só sujeitos à vigilância são, simultaneamente, agentes vigilantes (Mann, 2003; Guzik, 2017; Lyon, 2018).

A assunção que os processos de vigilância irão sempre aumentar, concentrar-se e tornar-se cada vez mais poderosos poderá ser falaciosa. As dinâmicas de poder envolvidas na vigilância eletrónica podem sofrer alterações no sentido de tornar a vigilância menos abrangente e poderosa (Marx, 2015; Guzik, 2017).

Em quinto lugar, prosseguindo a crítica de alguns autores ao modelo do panótico, este concentrava-se apenas no estudo da vigilância exercida por e sobre humanos. No entanto, existe um volume significativo de processos de vigilância que não são direcionados a humanos. Muitos destes processos estão relacionados com a monitorização de doenças, animais, entre outros. Por outro lado, no modelo do panótico a presença humana, como agente de vigilância, era necessária, mas com os novos desenvolvimentos tecnológicos já não se verifica esta necessidade. O rácio entre os recursos humanos e dispositivos de vigilância mudou drasticamente, diversos aparelhos de vigilância tornaram-se economicamente rentáveis, influenciando a sua primazia sobre a utilização de recursos humanos que requerem formação e pesam mais nos orçamentos (Haggerty, 2006).

Em sexto lugar, na sua obra mais influente sobre vigilância, Foucault via os alvos da vigilância como sendo, em grande medida, passivos. Atualmente são possíveis de identificar inúmeras formas de resistência como a defesa dos direitos à privacidade, dos direitos civis e da autonomia. Casos de desobediência civil como os cometidos pelos denominados *whistleblowers*,

são um bom exemplo de como os alvos de vigilância nem sempre são alvos passivos e que podem lutar contra os excessos na vigilância (Haggerty, 2006; Lyon, 2014; Simões e Jerónimo, 2018).

Após a grande quantidade de críticas que visaram o modelo de panótico, parece estar a desenvolver-se a tendência no sentido de abandonar o panótico de Foucault. David Lyon (2006) e outros autores defendem o abandono definitivo do panótico. Esta abordagem foi denominada de pós-panoticismo e assinala uma mudança (na forma analítica) da sociedade da disciplina de Foucault para uma sociedade do controlo, onde a produção da vida social é governada por relações globais nas quais as práticas da vigilância se integram na mobilidade geográfica, na produção económica e no consumo (Zureik, 2007).

Atualmente, a procura de uma metáfora mais adequada da vigilância continua. A *Surveillant Assemblage* de Haggerty e Ericsson (2000, 2006) é uma das tentativas mais discutidas dos últimos anos. Os autores inspirando-se nos trabalhos de Deleuze e Guattari, exploraram a utilização da infinidade de tecnologias de vigilância baseadas em sistemas combinados que analisam dados pessoais, tornando-os mais rentáveis para fins comerciais, administrativos, entre outros. A então resultante *Surveillant Assemblage* tem a potencialidade de retratar as nossas vidas numa série de fluxos de dados, estes dados podem ser reagrupados em localizações diferentes sob a forma de *data doubles,* estes podem ser escrutinados e selecionados para algum tipo de intervenção específica que poderá ter diversos propósitos.

A noção de *Surveillant Assemblage* vê o envolvimento dos sujeitos de vigilância como resultado dos seus próprios desejos, principalmente os relacionados com o consumo, a autoexpressão e o entretenimento voyeurístico (Haggerty e Ericson, 2000, 2006; Jansson, 2012). Desta forma a *Surveillance Assemblage* pode ser vista como uma das primeiras noções teóricas da vigilância que reconhece a necessidade da incorporação dos contextos da vigilância na sua análise (Galič, Timan e Koops, 2017).

No entanto, a noção de *Surveillant* Assemblage não é, atualmente, a mais adequada para se compreender as perceções e ações dos indivíduos perante a vigilância. Esta conceção, apesar de reconhecer alguns aspetos do envolvimento voluntário ou forçado dos sujeitos com a vigilância, não é capaz de capturar todo o espetro da vigilância na atualidade. Nomeadamente os papeis ativos dos alvos da vigilância. Por essa razão, optou-se por seguir os contributos da "Cultura da Vigilância" elaborados por David Lyon (2018).

1.5 - A Cultura da Vigilância: Observar como Modo de Vida

O termo cultura da vigilância já havia sido utilizado anteriormente por Staples (1997, *cit in* Lyon, 2018) e por Monahan (2011). Staples (1997) explorou os desenvolvimentos pós-modernos na vigilância, enquanto Monahan (2011) dissertou sobre a vigilância como "prática cultural", esta conceção é semelhante à visão da cultura da vigilância de David Lyon em dois aspetos

importantes: o relevo dado à inclusão de elementos como a cultura popular, média, arte e narrativa na discussão da vigilância; e também a importância de tentar entender a negociação da vigilância dos indivíduos nos seus próprios termos (Monahan, 2011; Lyon, 2018).

Lyon (2018) defende que atualmente deve-se captar a vigilância como cultura. A vigilância nunca havia estado integrada nas atividades do quotidiano como atualmente, os cidadãos participam ativamente nos processos de vigilância negociando-a e exercendo-a sobre outros. As antigas noções de vigilância, ainda que sejam pertinentes, parecem ser desadequadas para captar todo o espetro da vigilância na atualidade. De acordo com Lyon (2018), há uma clara necessidade de um conceito que capte os papeis ativos dos "alvos" da vigilância. Diferentemente do que o autor havia descrito quando escreveu sobre "a sociedade da vigilância", o foco principal (ou quase único) na vigilância organizacional já não é adequado, apesar de sua importância não poder ser subestimada. Na cultura da vigilância tem que se ir além desta, deve-se agora analisar como as pessoas participam e contribuem ativamente para a vigilância. O autor vai ainda mais longe quando afirma que as nossas vidas não são apenas gravadas, monitorizadas e rastreadas como nunca haviam sido. Na cultura da vigilância, as rotinas do quotidiano adquirem um papel importante na constituição da vigilância através da vigilância gerada pelo utilizador.

A vigilância tornou-se numa forma de ver e de ser no mundo, parece ser uma dimensão importante do nosso modo de vida. Apesar das diferenças ao nível do poder nos processos de vigilância, já não são só as empresas, que vigiam para persuadir cidadãos a comprar os seus produtos, ou os governos, para decidir que cidadãos têm direito a apoios estatais ou para monitorizar potenciais criminosos. Agora qualquer utilizador da internet o pode fazer facilmente, pode vigiar outros cidadãos ou organizações (públicas e privadas) e automonitorizar-se. A vigilância já não é meramente algo externo que se impinge nas nossas vidas. É algo que todos os cidadãos consentem, e/ou negoceiam, e/ou tentam resistir, e se envolvem de formas diferentes, podendo iniciar e até desejar alguns processos de vigilância. A cultura da vigilância reporta para um maior envolvimento das pessoas com meios de monitorização. Algumas pessoas utilizam as redes sociais para monitorizarem o outro, outras expõem-se deliberadamente nas redes sociais através de *tweets,* publicações, fotografias, histórias, entre outras formas. Os utilizadores podem atuar de forma vigilante em relação a outros, seja através de critérios avaliativos como "gostos" ou "recomendações" ou de publicações de protesto em relação a determinado assunto. É importante atentarmos na definição de conteúdo gerado por utilizador, proveniente dos estudos da Web 2.0. Através desta podemos observar que as mesmas capacidades tecnológicas, que permitem que os utilizadores contribuam com conteúdos, possibilitam simultaneamente novas formas de vigilância. O aumento drástico da utilização das redes sociais levou a um incremento significativo e não intencional da quantidade de dados fornecidos às organizações da vigilância organizacional (Simões e Jerónimo, 2018). Enquanto os utilizadores vão explorando os benefícios da Web 2.0,

assiste-se a diversos esforços, por parte de diversas organizações, para lucrar com a recolha de dados pessoais (Simões e Jerónimo, 2018; Lyon, 2018).

Ao interpretarmos a vigilância como cultura, temos um enquadramento que nos permite captar melhor as razões que levam a determinadas reações em relação à vigilância. Vejamos, por exemplo, as diversas reações às revelações de Snowden. Alguns reagiram com indignação e mobilizaram-se politicamente, outros sentiram um alívio por saberem que os governos estavam a esforçar-se no combate ao crime e ao terrorismo, outros simplesmente seguem a sua vida normal como consumidores despreocupados com a vigilância e contentes pela conveniência que lhe está associada. A vigilância não é apenas um aspeto institucional da modernidade ou uma forma tecnologicamente aumentada de disciplina/controlo social, atualmente, ela informa os pensamentos do quotidiano e o reportório das práticas quotidianas (Lyon, 2018).

O autor desenvolveu duas distinções analíticas que facilitam a interpretação da vigilância como cultura, os imaginários e as práticas em relação à vigilância. Os imaginários da vigilância, de uma forma sintética, são o que as pessoas pensam sobre a vigilância. Uma série de interrogações poderão estar presentes nos imaginários da vigilância dos cidadãos, como por exemplo: (i) o que constitui vigilância? (ii) Como e por quem ela é efetuada? (iii) Ou quais são os seus objetivos? Os imaginários da vigilância estão relacionados com entendimentos partilhados de certos aspetos da visibilidade no quotidiano, nas relações sociais, expectativas e compromissos normativos. Eles providenciam a capacidade para agir, engajar ou legitimar as práticas em relação à vigilância. São construídos através do envolvimento quotidiano com a vigilância, as notícias, a internet, a arte (principalmente através de filmes, música e livros), entre outros. Os imaginários da vigilância são subjetivos e complexos. Uma série de assunções podem fazer parte dos imaginários da vigilância, desde noções que acreditam que a vigilância é fundamental para garantir a segurança às que questionam a sua eficácia e apelam a uma maior proteção da privacidade, até às que reconhecem a sua conveniência, onde, por exemplo, se considera que trocar privacidade por benefícios é compensador. Apenas se apresentou alguns exemplos, a heterogeneidade dos imaginários da vigilância é imensa e dificilmente captada na íntegra. Não obstante, podem-se encontrar assunções, nos imaginários da vigilância, que são mais frequentes ou até unânimes (Lyon, 2018).

As práticas em relação à vigilância são as ações que nós fazemos face à vigilância. Estas não só incluem as resistências às relações de poder expressas pela vigilância, como também, qualquer atividade que surja como resposta à vigilância. Por exemplo alguns passageiros aéreos, com características percetíveis que os possam identificar como pertencentes ao "mundo do Médio Oriente", adotam comportamentos específicos de redução de risco. Por vezes, evitam dialogar em árabe perto dos controlos de segurança porque estão cientes que podem ser mais facilmente identificados como suspeitos. As alterações comportamentais em resposta à vigilância, como a presente no exemplo referido, também fazem parte das práticas da vigilância, tal como os comportamentos que iniciam processos de vigilância. Alguns exemplos práticos de atividades como resposta à vigilância incluem a adoção de estratégias de neutralização da vigilância, como

a instalação de alguma forma de proteção encriptada, ou o cobrir a webcam do computador pessoal. Os comportamentos que iniciam processos de vigilância, poderão verificar-se, por exemplo, na utilização das redes sociais para averiguar dados pessoas de outros ou na iniciação de comportamentos de automonitorização (Lyon, 2018).

De acordo com Lyon (2018) explorar a cultura da vigilância, através destes conceitos, permite-nos analisar a vigilância através de uma abordagem diferenciada. O autor argumenta que esta abordagem permite explorar um panorama cultural mais complexo do que os conceitos de "estado de vigilância" ou "sociedade da vigilância" (mas não os substitui), e ultrapassa alguns dualismos simples como poder-participação, visibilidade-invisibilidade, privacidade-exposição, ou o enganador "nós e eles" que constitui uma boa parte da retórica da vigilância. Por último, importa esclarecer que nesta nova forma de analisar a vigilância, apesar de se reconhecer que o papel ativo dos utilizadores na vigilância é fundamental, em nenhum momento se depreende que todos os cidadãos estão envolvidos ou implicados da mesma forma. A cultura da vigilância é multifacetada, complicada e imprevisível.

1.6 - Os Principais Tipos de Vigilância Eletrónica

Optou-se por dividir a vigilância eletrónica em quatro tipos: a governamental; a comercial; a lateral e, ainda, a *sousveillance*.

A vigilância governamental refere-se aos processos de vigilância nos quais determinado governo é o agente de vigilância. Este foi o primeiro tipo de vigilância a ser estudado e discutido nos estudos de vigilância, sendo o seu estudo, numa fase inicial, largamente influenciado por duas metáforas globalmente conhecidas e referidas anteriormente: o *Big Brother* de Orwell e o Panótico de Foucault (Lyon, 1994, 2003, 2006, 2018; Haggerty, 2006; Essen, 2008; Bauman e Lyon, 2013). A vigilância governamental foi desenvolvida por necessidade, desenvolveram-se diversos métodos de recolha de informação centralizados para aprimorar a capacidade de resposta a diversos aspetos que a governação, cada vez mais complexificada, implicava (Weller, 2012).

Desde os finais do século XVIII, uma série de processos e acontecimentos aprofundaram essa necessidade. A industrialização teve um impacto enorme na necessidade para uma recolha de informação centralizada, também a migração para as novas áreas urbanas, as revoluções nos transportes e comunicações e o crescimento de todo o aparelho eleitoral exigiram uma capacidade de resposta e responsabilidade maior por parte dos governos somente possibilitada através da vigilância (Giddens, 1990; Weller, 2012). A vigilância governamental engloba as atividades exercidas pelos diversos departamentos de determinado governo, por serviços secretos governamentais, pela polícia ou até por departamentos ligados aos Estados-Providência. Através da recolha de dados como os registos bancários, os governos podem deliberar se o indivíduo tem direito a aceder à assistência social ou não. Estes são apenas alguns

exemplos que não captam a totalidade dos processos de vigilância que os governos podem exercer (Lyon, 2018).

Como já foi referido, a vigilância governamental mais recente foi significativamente influenciada por dois acontecimentos marcantes: o 11 de setembro e as revelações de Snowden. Bruce Schneier (2015), criptógrafo e especialista em segurança computacional, afirmou que atualmente a vigilância governamental monitoriza todos os alvos possíveis. Não se concentra em apenas líderes governamentais ou em alegados espiões, uma das maiores preocupações prende-se com o terrorismo cujos membros podem estar em qualquer lugar no mundo. Desta forma a vigilância governamental monitoriza toda gente, sejam cidadãos domésticos ou internacionais. Após a recolha de dados generalizada é possível, através de processos de *social sorting* criar perfis de "pessoas de interesse" como por exemplo potenciais criminosos ou terroristas, por outro lado, este tipo de vigilância pode ajudar na decisão de quem tem direito à ação social (Lyon, 2005,2014).

Schneier (2015) argumenta que é difícil analisar em profundidade a capacidade deste tipo de vigilância, visto que é quase sempre realizado por serviços secretos que podem quebrar as leis dos seus Estados. O autor afirma que, só porque não tenha havido grandes fugas de informação sobre o funcionamento da vigilância governamental em outros países, não se deve de forma alguma deduzir que tal não aconteça. O autor defende que, provavelmente, qualquer país com orçamento suficiente para ter serviços secretos exerce, ou pelo menos possuí a capacidade para exercer processos de vigilância poderosos sobre a sua população. Estes processos podem, inclusive, desrespeitar as leis nacionais.

Além da recolha de dados generalizada, atualmente os governos que pretendam monitorizar alvos específicos, podem exercer os seus processos através de *hacks*. Existem fabricantes de armas eletrónicas como a "Hacking Team", que produzem ferramentas capazes de invadir os sistemas operativos de computadores e *smartphones*. Em 2015, ficou claro, através de um vazamento de dados, que diversos governos compravam as suas ferramentas. As suas capacidades incluem tirar capturas de ecrãs e fotos, gravar áudio, monitorizar chamadas e monitorizar os GPS's dos telemóveis (Schneier, 2015). De acordo com Schneier (2015) a maioria dos países têm estas capacidades de *hacking*. Quando é que as utilizam, contra quem e quais as regras legais que devem obedecer varia de país para país.

Deve-se destacar, também, as parcerias de vigilância formadas entre governos. Estas incluem os famosos "Cinco Olhos" constituídos pelos EUA, Reino Unido, Canadá, Austrália e Nova Zelândia, e outras parcerias menos abordadas como os "9 Olhos" e ainda os "14 Olhos" que apesar de não incluírem Portugal, abarcam outros países da União Europeia como a França e Alemanha. Surpreendentemente, algumas parcerias já foram formadas entre inimigos históricos como a Rússia e os EUA para colaborar na segurança de algum evento. A Rússia forneceu informações aos EUA sobre o perpetrador que realizou o atentado na maratona de Boston. Os EUA colaboraram na garantia de vigilância dos Jogos Olímpicos de Inverno, realizados na Rússia,

em Sochi. Estas parcerias podem levantar questões relacionadas com uma espécie de monopolização da vigilância, no entanto, esta parece estar sempre condicionada por aspetos de relações internacionais (Schneier, 2015).

Por último, importa advertir, que apesar de algumas práticas comuns em todos governos do mundo Ocidental, existem diferenças significativas entre governos; principalmente ao nível do acesso à informação pessoal. Estas diferenças alteram o que os governos podem saber sobre os seus cidadãos a diversos níveis, como a situação familiar, nível de riqueza, inclinações políticas e as suas localizações e condicionam as capacidades deste tipo de vigilância (Rule, 2007).

Outro dos tipos de vigilância mais estudados é o da vigilância comercial. A interação da vigilância eletrónica com o mercado, era já explorada por Oscar Gandy em 1989. O autor dissertava, entre outras temáticas, sobre o controlo do consumo em massa através de informação recolhida dos consumidores. Esta informação incluía dados pessoais e índices de como as pessoas respondiam a certas mensagens persuasivas. Através da análise de dados, as organizações procediam a uma classificação, com base nos interesses individuais, nas necessidades e orientações, dos indivíduos em determinados grupos (Gandy, 1989). Neste artigo parecem ter ficado alicerçadas as bases para a identificação do processo, hoje, denominado de *social sorting,* aprofundado no Capítulo 1.

A implementação da vigilância, baseada em *social sorting,* no mercado teve vários motivos: (i) a eficiência que este tipo de vigilância promove ao facilitar a adoção de políticas de redução de custos; (ii) a conveniência que o marketing baseado em dados pessoais fornece e (iii) o aumento das capacidades de persuasão, por parte das empresas, sobre as opções de consumo dos cidadãos (Pridmore, 2012; Lyon, 2015).

A recolha de dados sobre os consumidores provou ser valiosa, os denominados *data doubles* reforçaram as oportunidades para as organizações se aproximarem dos seus clientes, personalizando a sua oferta e possibilitando a criação de estratégias de marketing direcionadas (Ball, 2016). Atualmente, as empresas estão cada vez mais dependentes da recolha e análise de dados sobre os desejos (ou a sua fomentação) e necessidades dos consumidores. As decisões de marketing e negócios empresariais são previstas com a ajuda destes dados desde: os serviços que as empresas escolhem providenciar, às localizações onde vão operar e como criar relações proveitosas com os consumidores, entre outros. Além dessa relevância, importa salientar que os processos de recolha, armazenamento e análise destes dados tornaram-se muito mais fáceis e menos dispendiosos. A vigilância é o alicerce que permite a compreensão otimizada digitalmente dos hábitos de consumo e dos próprios consumidores. Ela também oferece formas de participação e envolvimento visto que são os consumidores que fornecem os dados (Pridmore, 2012; Ball, 2016).

Em suma a vigilância comercial, na sua forma mais desenvolvida, é utilizada para influenciar, controlar e monitorizar as escolhas dos consumidores, por um lado guiando certos consumidores para produtos e práticas que são valiosos para as empresas, e por outro lado desviando a sua

atenção de consumidores que não geram grandes ganhos (Pridmore, 2012). Apesar de ter como objetivo influenciar e de levantar problemas de desigualdade entre consumidores, deve-se questionar as noções que defendem que ela constitui uma orquestração mal-intencionada desenvolvida para os oprimir. A vigilância do consumidor, também tem aspetos positivos como a sua maior participação e conveniência que este tipo de vigilância lhes pode oferecer. A vigilância comercial deve ser vista como uma parte integral da vida económica moderna, sendo analisada tendo em conta um elevado grau de complexidade (Ball, 2016).

A vigilância lateral refere-se à panóplia de processos de vigilância sem uma hierarquia clara do tipo *top-down*. Trata-se de uma vigilância realizada horizontalmente por pessoas (e entre elas) de forma frequentemente recíproca (Andrejeikavic, 2004; 2005; Marwick, 2012).

A vigilância lateral foi um conceito elaborado por Mark Andrejeikavic (2004; 2005). Não se pode afirmar que, este tipo de vigilância, seja uma novidade plena, na Alemanha Nazi e na Rússia Estalinista este tipo de vigilância era de tal forma intenso que nos relembra noções Orwellianas (Weller, 2012). No entanto, foi Andrejeikavic que dissertou sobre a ascensão deste tipo de vigilância relacionando-a com as novas tecnologias que permitem papeis mais participativos na vigilância por parte dos cidadãos. Este tipo de vigilância inclui ferramentas que monitorizam outras pessoas, de forma horizontal, fundamentalmente (mas não só) em três categorias: interesses românticos, família ou amigos e conhecidos. Pode ser composta por diversas formas de observação/monitorização, alguns exemplos incluem a utilização do motor de busca da Google, instalação de câmaras de vigilância, utilização de máquinas fotográficas dos telemóveis, ou um escrutínio da atividade de outros cidadãos nas redes sociais, entre outros (Andrejeikavic, 2005).

As redes sociais são, porventura, a plataforma online onde este tipo de vigilância mais se manifesta atualmente. Importa notar que a atividade dos cidadãos nas redes sociais, é profundamente influenciada pela audiência a que o utilizador se está a expor. Os utilizadores estão a observar outros, mas também estão cientes que eles próprios estão a ser observados, algo que influencia o seu comportamento nas redes sociais. O potencial de estar a ser monitorizado pode contextualizar uma autovigilância. Curiosamente, a atividade dos utilizadores é mais influenciada pela presença dos seus conhecidos na audiência, principalmente pais e patrões, do que com a monitorização efetuada pelos governos ou empresas (Marwick e Boyd, 2010; Marwick, 2012).

Por último, apresenta-se a *sousveillance*. Steve Mann foi o responsável pela formulação do conceito de *sousveillance*, a designação *Sousveillance* foi elaborada através da junção e analogia de duas palavras francesas, *sous* (de baixo) e *veiller* de observar. Contrastando com a vigilância organizacional, este tipo de vigilância permite observar a partir debaixo, isto é, observar poderosos a partir de uma posição de menor poder e autoridade (Mann, 2003; Ganascia, 2010). Para Mann e Ferenbok (2013) a proliferação de aparelhos capazes de gravar e

transmitir vídeos provocaram um aumento exponencial na frequência e eficácia das práticas de *sousveillance*.

Para Mann (1998, 2003) este tipo de vigilância é uma forma de reflecionismo. O reflecionismo refere-se à apropriação de mecanismos de um determinado opressor, e consequente utilização direta dessa metodologia contra ele. O reflecionismo manifesta-se na vigilância através da disponibilização de ferramentas ou dispositivos de vigilância para o cidadão comum, que permitem gravar e difundir determinados acontecimentos. Outrora estas tecnologias só estavam ao alcance de instituições poderosas como Estados ou empresas com elevados orçamentos, enquanto atualmente a maior parte dos cidadãos também as possuem, algo que lhes permite observarem as entidades de maior autoridade e poder. Através da *sousveillance* os indivíduos têm a oportunidade, em certa medida, de fazer frente à monitorização organizacional. Atualmente as ferramentas, mais frequentemente utilizadas, neste âmbito, são as capazes de gravação audiovisual e/ou as capazes de difundir conteúdos na internet (Mann, 2003; Ganascia, 2010; Lyon, 2018).

A incorporação da *sousveillance* no quotidiano pode, de certo modo, alterar as relações de poder da vigilância ao restaurar, em certa medida, um maior equilíbrio entre cidadão e a vigilância organizacional. Atualmente, muitos cidadãos têm alguma noção do poder da *sousveillance*. Lyon (2018) oferece-nos o exemplo do incentivo ao uso de dispositivos de filmagem, por parte de um grupo defensor dos direitos humanos Israelita, para que a população palestiniana filmasse determinadas situações de forma a possibilitar a partilha com quem não esteve presente. Em Portugal, a recente polémica em torno dos acontecimentos no "Bairro da Jamaica" (Cardoso, 2019) ilustra perfeitamente as alterações nas dinâmicas de poder da vigilância que podem ser causadas pela s*ousveillance*. A utilização de dispositivos de vigilância, neste caso telemóveis com câmara de filmar permitiu o registo e divulgação de uma atuação polémica da Polícia de Segurança Pública que resultou na abertura de um inquérito aos incidentes por parte do Ministério Público (Lusa, 2019).

Apesar de distintas, os quatro grandes tipos de vigilância, identificados nesta dissertação, interrelacionam-se entre si. A forma como se relacionam é importante e tem consequências ao nível das capacidades da vigilância (Ball, 2012, 2013; Espanha e Estêvão, 2017; Lyon, 2014, 2018).

A interação entre vigilância comercial e a lateral é facilmente identificada no domínio das redes sociais. As redes sociais expõem os consumidores aos regimes de vigilância vertical e lateral. Através da incorporação e uso crescente dos smartphones no quotidiano, a quantidade de dados produzida aumentou, tornando visível dados relacionados com os estilos de vida e relações interpessoais, tanto entre "pares", como para as agências governamentais e plataformas de marketing (Simões e Jerónimo, 2018). São recolhidas, através dos dados disponibilizados nas redes sociais, informações sobre as atividades, práticas e comportamentos de indivíduos e grupos, sendo estas posteriormente transmitidas, através de infraestruturas

tecnológicas de grande escala a organizações de negócios. O entusiasmo pelo aumento das capacidades do *Big Data* é, também, partilhado com as entidades governamentais que se envolvem na segurança dos seus cidadãos. Os dados recolhidos pelas organizações comerciais podem, dentro dos limites legais, ser analisados, combinados e correlacionadas, posteriormente, por entidades com responsabilidades ao nível da segurança. Algo que amplia as capacidades da vigilância governamental (Ball, 2012, 2013; Lyon, 2014).

Recentemente, Rita Espanha e Tiago Estêvão (2017) dissertaram sobre a relação entre vigilância lateral e governamental. Para a exemplificarem, utilizaram o atentado à maratona de Boston em 2013 e os tumultos em Vancouver no ano de 2011. Nestes dois acontecimentos, as forças de segurança obtiveram uma ajuda importante na identificação dos perpetuadores através da disseminação das suas fotos em redes sociais. A importância da participação dos cidadãos com dispositivos móveis com ligação á internet foi decisiva, esta participação parece estar a adquirir uma importância cada vez maior. Algo que está de acordo com o "ver de forma vigilante" que Lyon (2018:31) referiu.

No fundo, a *sousveillance* pode ser entendida como uma forma de pactuar com a vigilância, uma vez que os cidadãos a utilizam para se beneficiar, no próximo capítulo exploram-se as formas como os cidadãos podem pactuar ou resistir à vigilância.

Capítulo 2 – Vigilância Eletrónica: da Pactuação à Resistência

As reações e as respostas à vigilância são variadas. Alguns indivíduos podem adotar ações para bloquear ou limitar processos de vigilância, outros, mesmo que estejam conscientes da vigilância, apenas continuam com a sua vida sem lhe atribuir grande importância (Augusto e Simões, 2017), outros sentem que têm de aceitar a vigilância, não encontrando alternativa. Por outras palavras, goste-se ou não, toda gente tem mais aspetos da sua vida influenciados pela vigilância do que anteriormente (Lyon, 2018).

Contudo, David Lyon argumenta que é errado assumir que os indivíduos são passivos e que seguem voluntariamente as regras estabelecidas da vigilância. O autor defende que se deve explorar as práticas do quotidiano para se explorar as formas como as pessoas lidam com as estratégias de poder no seio da vigilância. A pactuação com a vigilância ou a tentativa de lhe resistir, por parte dos indivíduos, pode ser influenciada por vários fatores, como a sua nacionalidade, género, experiências anteriores e etnicidade (Lyon, 2018).

As três próximas secções abordam diversos contextos nos quais os cidadãos pactuam com a vigilância. De acordo com Steeves (2009), os cidadãos podem desejar negociar o seu grau de privacidade, estipulando em que situações fornecem (ou não) os seus dados, expor os seus dados por confiarem nas entidades, ou fornecê-los em troca de benefícios.

As últimas duas secções deste capítulo abordam algumas das formas como os cidadãos podem tentar resistir à vigilância. As ações de resistência à vigilância são mais difíceis de executar. A manifestação, por vezes, escassa de formas e ferramentas de resistência à vigilância pode estar relacionada com dois problemas assimétricos importantes. Por um lado, a assimetria de poder existente entre os cidadãos em relação a entidades vigilantes mais poderosas. Os cidadãos raramente podem escolher como ou quando são monitorizados, o que acontece à informação que lhes foi recolhida e quais as consequências que poderão advir dessa recolha. Por outro lado, o problema relacionado com a assimetria ao nível do conhecimento, visto que muitas vezes nem estamos conscientes ou totalmente conscientes da monitorização e da forma como esta funciona. Estas duas assimetrias podem reforçar a falta de resistência visto que estamos a tentar resistir a algo que não compreendemos, de que temos pouca informação e que dificilmente conseguimos influenciar (Galič, Timan e Koops, 2017).

Contudo, os indivíduos podem, pelo menos até certa medida, resistir e recusar a vigilância através das formas como utilizam a tecnologia e de algumas limitações inerentes à arquitetura de sistemas de vigilância. O desenvolvimento das tecnologias e as estratégias de vigilância tem muitas vezes vulnerabilidades que se podem explorar (Marx, 2016; Galič, Timan e Koops, 2017). Marx (2016) argumenta que os limites logísticos e económicos da monitorização total, como por

exemplo, a diversidade de valores, a natureza interpretativa e contextual de muitas situações humanas, a vulnerabilidade dos agentes vigilantes e outros fatores, possibilitam a resistência à vigilância.

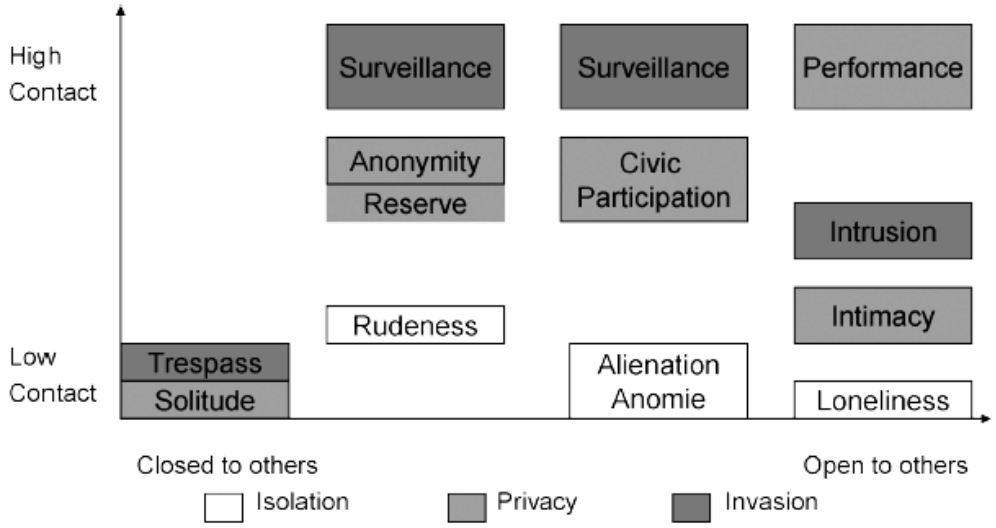
2.1 – Privacidade e Exposição

A relação entre privacidade e vigilância é óbvia. A privacidade é geralmente definida como o direito de o indivíduo ter a sua informação pessoal protegida de outros autores sociais sejam eles o governo, as instituições ou os seus pares. O acesso à informação pessoal só não invade a privacidade quando é consentido voluntariamente pelo indivíduo (Steeves, 2009).

De entre as muitas questões que podem ser exploradas, Steeves (2009) aponta para a ameaça que a vigilância pode representar ao quebrar as fronteiras entre os diversos papéis sociais que um individuo pode desempenhar. Seguindo os contributos de Goffman, Steeves (2009) destaca a importância da separação entre o que é público e privado sobre o indivíduo. A privacidade é essencial porque permite essa separação. A autora defende uma conceptualização da privacidade como construção social, ao fazê-lo possibilita uma teorização sobre as formas como determinados estados de privacidade são negociados nas interações sociais. Cada interação social é contextualizada por um acordo social no que diz respeito à disposição para se expor ao outro, seja ele um indivíduo ou uma organização. Este acordo é ameaçado pela vigilância quando esta não é aceite (Steeves, 2009).

Através da conceptualização de diversos níveis de privacidade, é possível teorizar sobre um modelo para compreender a negociação social da privacidade. Steeves (2009), elaborou um esquema no qual separa o que pode ser considerado isolamento, privacidade e invasão. O esquema é baseado em dois eixos, o vertical refere-se ao contacto com outros atores sociais e o horizontal à abertura para com os outros atores sociais. O esquema (Figura 1), pretende demonstrar como a vigilância ameaça severamente a negociação da privacidade.

Figura 1 - Esquema de Privacidade de Steeves



Fonte: Steeves, 2009, pp. 208

A invasão da privacidade ocorre quando o indivíduo não consegue negociar o estado de privacidade que pretende. Já o isolamento manifesta-se na incapacidade de um individuo obter interações íntimas, em sentimentos de solidão ou na incapacidade de obter o nível de privacidade que deseja na sua participação cívica (Steeves, 2009).

A intimidade pressupõe, neste esquema, que o indivíduo confia noutro ator social e revela-lhe determinadas informações. Por outro lado, a obtenção dessas informações sem consentimento pressupõe uma situação de intrusão da privacidade. Além das relações interpessoais do quotidiano, o esquema capta a questão da participação cívica. Ela surge no domínio da privacidade, porém quando um indivíduo é confrontado com a impossibilidade de garantir o grau de privacidade que deseja, pode sentir-se isolado e com sentimentos de alienação e anomia. O anonimato é conseguido quando outros atores sociais concordam em respeitar o desejo do indivíduo em não ser identificado, se esse desejo não for respeitado está-se perante uma situação de vigilância invasiva. A intimidade também só é possível porque os outros reconhecem o espaço para a interação íntima, podemos observar este reconhecimento quando alguém desvia o olhar ao ver um casal a beijar-se de forma romântica (Steeves, 2009)

Como Goffman (1956) havia afirmado, os indivíduos apenas podem manter determinado papel durante um tempo limitado, nenhum indivíduo pode representar infindavelmente, sem descanso, a variedade de papéis que a vida exige. Os momentos de "bastidores", onde o cidadão pode ser ele próprio, são essenciais na vida humana e podem ser ameaçados pelos processos de vigilância (Steeves, 2009).

2.1.1 A Automonitorização, a Exposição Voluntária nas Redes Sociais e o Paradoxo da Privacidade

Os processos de vigilância, do ponto de vista dos indivíduos, podem ser bem-vindos e integrados no seu quotidiano com o objetivo de melhoria da sua vida. O sentimento de risco e a necessidade para o reduzir é evidente no nosso quotidiano. A automonitorização da saúde, do dinheiro e do tempo é frequentemente vista como uma prática capaz de reduzir riscos. Esta pode ser efetuada através de diversos dispositivos de vigilância (Lyon, 2018). Os mais comuns são, porventura, a utilização de aplicações que monitorizam a atividade física como o *Google Fit* e os chamados dispositivos "vestíveis" como os *smartwatches*. A importância e uso cada vez mais comum destes dispositivos, que quantificam aspetos da nossa vida, tem levado à discussão sobre o conceito de *self* quantificado (Schneier, 2015; Lyon, 2018).

De acordo com a teorização deste conceito, o *self* quantificado implica que o indivíduo inicie qualquer atividade de automonitorização, seja ela biológica, física, comportamental ou ambiental. Os participantes têm uma postura proativa na obtenção destas informações e reagem consoante os dados que recolhem, procurando melhorar determinado aspeto da sua vida. No entanto, os utilizadores veem apenas o seu fragmento dos dados, a grande maioria dos dados acaba nas bases de dados das empresas que fornecem as tecnologias. As lógicas da vigilância comercial aplicam-se neste processo, os utilizadores são persuadidos por uma forte retórica de participação e inclusão, mas enfrentam uma grande falta de transparência sobre a forma como os seus dados são agregados, analisados e vendidos (Crawford, Lingel e Karppi, 2015).

Quanto à exposição voluntária, o mundo onde, anteriormente, só celebridades conseguiam ter uma exposição relevante, fez com que o ser visto fosse considerado um desejo ou privilégio. Hoje, com a emergência das redes sociais a possibilidade de exposição voluntária é facilmente alcançável. Esta exposição também pode ser vista como um modo de reinvenção pessoal, onde as pessoas tentam expor as suas vidas da forma mais favorável possível perante o olhar do outro (Lyon, 2018). Lyon faz também referência à junção de dois desejos, o desejo de descoberta e o de exposição, que podem contribuir para uma legitimação e naturalização da vigilância (Lyon, 2018). Esta tendência pode ser o resultado da procura individual para a participação e interação social, mas não é necessariamente uma decisão coletiva para invadir a privacidade dos outros. Assim, o indivíduo vive num processo pessoal contínuo, no qual procura privacidade em determinados momentos e exposição ou companheirismo noutros (Steeves, 2009).

Porém, estes comportamentos nos quais a vigilância pode ser bem-vinda, contrastam com as preocupações subjetivas de privacidade que muitos cidadãos referem ter, algo que tem sido apelidado de paradoxo da privacidade. O paradoxo da privacidade refere-se a uma disparidade entre a intenção inicial para a cedência de dados e o fornecimento, na prática, de dados

pessoais. Os cidadãos afirmam, frequentemente, não ter a intenção de fornecer dados pessoais, porém, quando são confrontados com situações práticas onde a cedência de dados é pedida, acabam por fornecê-los (Norgberg, Horne e Horne, 2007.) Vários autores tentaram explicar o paradoxo da privacidade, Baek (2014), por exemplo, defendeu que uma das razões para a existência do paradoxo, é o facto de os cidadãos raramente experienciarem violações de privacidade diretamente em contexto *online*.

2.2 – Dataísmo e Confiança nas Instituições

Diversos autores notaram a relação entre aceitação da vigilância e a confiança nas instituições envolvidas. Esta dimensão é vista como um facto fundamental na moldagem das reações e perceções sobre a vigilância (Steeves, 2009; Pavone e Esposti, 2010; Jansson, 2012; Dijck, 2014; Lyon, 2018).

As grandes empresas possuidoras de uma grande quantidade de dados pessoais, tal como as agências governamentais e investigadores, realçam a importância da confiança dos utilizadores nas plataformas online. O Estado é, geralmente, visto como o responsável por ditar as regras enquanto as plataformas têm de obedecer às regras ditadas por este. As revelações de Snowden deixaram claro que as pessoas confiavam nas instituições para gerirem os seus dados pessoais, agindo com base na crença que estas seguiam as regras legalmente impostas. A ideologia do Dataísmo, crença que o processamento de dados e o fluxo de informação são valores supremos, está relacionada com a confiança que as pessoas depositam nas instituições. No entanto, os desenvolvimentos e debates após as revelações de Snowden, vieram abalar a confiança e credibilidade de todo o "ecossistema" da gestão de dados online (Dijck, 2014). Esta desconfiança, nas entidades possuidoras de grandes quantidades de dados pessoais, adquiriu uma importância significativa na atualidade, basta atentar nas polémicas relacionadas com proteção de dados de empresas como o *Facebook* nos últimos anos. Em notícias recentes, observam-se tentativas, por parte de diversos Estados, de proteger a privacidade dos seus cidadãos através de multas e sanções em diversos contextos nos quais as suas leis de privacidade foram violadas. Mas assiste-se também a esforços, por empresas como o *Facebook*, de alterar e corrigir aspetos na sua plataforma para garantir uma maior proteção de dados aos seus utilizadores (Agência Lusa, 2018; Gebel, 2019).

2.3 – Dados Pessoais como Moeda de Troca para a Obtenção de Benefícios

Atualmente os dados pessoais têm indubitavelmente um valor comercial, autores como Acquisti, Taylor e Wagman (2016) têm vindo a apelar para que se investigue a forma como os cidadãos podem (ou não) reconhecer o valor que os seus dados têm. Neste subcapítulo

exploram-se algumas formas como acabamos por trocar os nossos dados pessoais pela, por vezes alegada, obtenção de benefícios de diversas naturezas.

A maior parte dos indivíduos, provavelmente, desconhece os diversos fatores que podem afetar a sua privacidade, como por exemplo as formas como os seus dados pessoais são recolhidos e utilizados, uma vez que as entidades que recolhem informação atuam de uma forma sofisticada (Acquisti, Brandimarte, Loewenstein, 2015). As entidades vigilantes apresentam aos cidadãos alguns argumentos para os persuadirem a ceder os seus dados. As entidades governamentais, por vezes, justificam o aumento da vigilância alegando que ela contribui para um aumento na segurança nas suas sociedades (Hong, 2017). Na lógica da vigilância comercial, as entidades oferecem benefícios comerciais em troca dos nossos dados pessoais, ou podem também tentar tornar a aceitação da monitorização numa questão de conveniência ao adicionar certos impedimentos a quem não aceite fornecer os seus dados (Zurawski, 2011; Wottrich, Reijmersdal, e Smit, 2018).

Em suma são propostas diversas trocas aos cidadãos que implicam a cedência de dados pessoais para a obtenção de benefícios, neste subcapítulo, destacam-se 3 situações onde a referida troca decorre: (i) a troca de privacidade por segurança; (ii) a troca de dados pessoais por benefícios comerciais e (iii) a troca de dados pessoais por conveniência.

2.3.1 – A troca de privacidade por segurança

A relação entre privacidade e segurança tem sido amplamente discutida (Chandler, 2009; Pavone e Esposti, 2010; Solove, 2011; Augusto e Simões, 2017; Hong, 2017; Simões e Jerónimo, 2018), numa fase inicial analisou-se esta relação como se ela se tratasse de uma troca de custo-benefício. Os aumentos na segurança, através da implementação de dispositivos de vigilância, diminuem o nível de privacidade gozada pelos cidadãos, porém, esta diminuição é por vezes justificada ou aceite devido aos alegados ganhos na segurança. A troca de privacidade por segurança também pode funcionar como uma retórica que diminui a oposição pública à vigilância; veja-se o caso de diversas administrações dos EUA. Esta retórica reforçou-se no contexto social recente: a imprevisibilidade, espacial e temporal das diversas ações criminosas e as suas repercussões globais contribuíram para a substituição de uma racionalidade de meios/fins para uma de gestão do risco. A partir desta perspetiva, o objetivo de uma sociedade mais segura é tentado através da implementação de políticas de segurança que muitas vezes pressupõem o uso de dispositivos de vigilância que limitam a privacidade do cidadão comum. Ainda que não tenham surgido dados que demonstrem os incrementos na segurança provocados devido ao aumento da vigilância (Pavone e Esposti, 2010; Hong, 2017).

As reações à implementação de dispositivos de vigilância são geralmente duas, algumas pessoas duvidam da eficácia da utilização de novos dispositivos de vigilância como forma de garantir uma maior segurança, enquanto outros sugerem a limitação da utilização destes dispositivos, apelando ao uso destes dispositivos apenas em contextos específicos e sempre sob garantias

legais e institucionais. Aqueles que consideram os riscos e benefícios dos dispositivos de vigilância tendem a ter uma abordagem de troca. As pessoas que acreditam que os dispositivos de vigilância violam a privacidade e não aumentam a segurança adotam uma atitude preocupada, porque enfrentam uma situação de perda-perda. Já outras pessoas avaliam a situação de forma oposta, desenvolvendo uma atitude de confiança nas instituições. Nestas últimas duas perspetivas, verificou-se que a troca privacidade-segurança não se aplica (Pavone e Esposti, 2010).

A tese da troca de privacidade por segurança acaba por ser tendenciosa (Chandler, 2009; Solove, 2011) ou até falaciosa (Pavone e Esposti, 2010; Augusto e Simões, 2017; Simões e Jerónimo, 2018). Chandler (2009) argumenta que a troca da privacidade por segurança parece ser tendenciosa a favor da segurança, particularmente em tempos de insegurança pública. A autora acredita que nós estamos a sacrificar direitos e liberdades demasiado facilmente. Chandler também se questiona sobre a adequabilidade da análise desta troca, defendendo que a segurança e a privacidade são conceitos complexos e de difícil comensurabilidade. A autora sugere uma alteração na análise desta troca, integrando valores mais comensuráveis na sua análise. Pavone e Esposti (2010) defendem que a análise desta troca é errada, pois a troca privacidade-segurança implica que estas sejam bens trocáveis, no entanto, a confiança e a preocupação são atitudes políticas, que podem mudar ao longo do tempo dependendo de diversos fatores, por essa razão não podem ser trocadas como se fossem bens económicos. Além disso, o enfâse no equilíbrio abstrato entre privacidade e segurança, encobre uma série de implicações éticas, sociais e políticas associadas às novas formas de vigilância. Estas implicações podem ter impacto na forma como os cidadãos vêm os dispositivos de vigilância: como uma solução para um problema de segurança, ou como uma ameaça à privacidade.

Apesar da existência da troca privacidade-segurança ser discutível, a sua presença nas perceções dos cidadãos, tal como a primazia dada à segurança, é frequente (Chandler, 2009; Pavone e Esposti, 2010; Solove, 2011; Augusto e Simões, 2017).

A falácia da troca acima referida, também pode ser demonstrada pelos acontecimentos recentes na Turquia. De acordo com Topak (2017), após uma tentativa falhada de golpe de Estado e consequente declaração de Estado de Emergência, o Partido da Justiça e do Desenvolvimento, liderado pelo presidente Turco Recep Erdoğan, instrumentalizou o Estado de Emergência para ultrapassar o parlamento e avançar com uma série de medidas que limitaram diversos direitos e liberdades do povo turco. De entre estas medidas, encontram-se as que aumentaram e intensificaram os processos de vigilância governamental na Turquia e que não resultou em incrementos de segurança. O dispositivo de vigilância governamental, deixou rapidamente de se concentrar e criminalizar apenas os alvos suspeitos de conspirarem no golpe para abranger também dissidentes, incluindo membros Curdos do parlamento, jornalistas e académicos que se opunham ao governo liderado por Erdoğan. Além do escrutínio do que poderiam ser consideradas, na perspetiva do Governo Turco, "pessoas de interesse", a vigilância tornou-se massificada, a procura de opositores por parte do Governo resultou na

detenção de mais de 100 mil pessoas, no despedimento de cerca de 130 mil empregados públicos (incluindo 7000 académicos) e ainda no encerramento de mais de 70000 contas em redes sociais. A alteração dos dados recolhidos para que parecessem mais incriminatórios, tornou esta utilização intensificada de vigilância ainda mais ameaçadora para a liberdade individual na Turquia (Topak, 2017).

2.3.2- A troca de dados pessoais por benefícios comerciais

Muitos cidadãos trocam os seus dados pessoais, conscientemente ou não, por benefícios comerciais. Esta troca pode ser realizada de inúmeras formas, nesta secção exploramos apenas duas das práticas que consideramos mais relevantes neste contexto, a troca de dados pessoais por benefícios comerciais na utilização de cartões de fidelização, e na transferência e instalação de aplicações.

Quanto à troca no contexto das aplicações móveis, destaca-se o crescimento exponencial, nos últimos anos deste mercado. No ano de 2015 estima-se que ocorreram cerca de 179 bilhões de transferências de aplicações (Gu *et al.*, 2017). Este crescimento relaciona-se com a monetarização dos dados pessoais, os dados pessoais tornaram-se na moeda com a qual os utilizadores "pagam" as aplicações móveis. Ao invés de pagarem com dinheiro "real", estes utilizadores recompensam, muitas vezes sem terem consciência, os criadores das aplicações ao aceitar os pedidos para que a aplicação aceda a informações pessoais armazenadas no seu dispositivo. Essas informações incluem normalmente o ID do dispositivo, o registo de chamadas e os contactos, algo que pode ter impacto ao nível da privacidade dos utilizadores (Wottrich, Reijmersdal, e Smit, 2018). Muitas aplicações móveis oferecem serviços personalizados disponíveis a qualquer altura e em qualquer lugar, alguns destes serviços incluem navegação a tempo real, acesso às redes sociais, serviços bancários, entre outros. Apesar da atratividade destas aplicações, o acesso sem precedentes aos dados pessoais dos seus utilizadores levanta novas questões. Especialmente em relação à invasão, frequentemente desnecessária, da privacidade dos indivíduos através dos seus aparelhos móveis. Considera-se invasão de privacidade desnecessária quando as aplicações recolhem informações desnecessárias para a funcionalidade da aplicação, ou quando determinada organização utiliza ou transmite os dados para outros propósitos sem autorização (Gu *et al.*, 2017). Discernir que aplicações invadem a privacidade não é uma tarefa fácil. Podem ser necessárias ferramentas técnicas, conhecimento e precauções por parte dos utilizadores.

Gu *et al.* (2017), argumentam que os indivíduos fazem uma análise de custo-benefício antes de efetuarem a instalação de determinadas aplicações. Os indivíduos que se preocupam mais com a sua privacidade tendem a instalar menos aplicações. A influência de uma série de variáveis na instalação de aplicações foi identificada: por um lado, a popularidade das aplicações foi um elemento importante, e, por outro lado, a idade dos utilizadores também demonstrou ser um fator que influência a facilidade com que se fornece dados pessoais a organizações. Midha (2012) identificou diferenças ao nível das questões de género, as mulheres tendem a preocupar-

se mais com a sua privacidade nas suas práticas de consumo *online*. A experiência na utilização da internet e aplicações móveis também alteram a preocupação com a privacidade, sendo que quanto mais experiência os utilizadores adquirem, menos preocupação demonstram com a privacidade (Gu *et al.*, 2017). Outras consequências da aceitação em partilhar informações pessoais prendem-se com a discriminação de alguns consumidores, a receção de publicidade não solicitada e ainda a possibilidade de roubo de identidade. Desta forma, a decisão de instalar uma aplicação gratuita pode ser arriscada e merece consideração, dado que implica uma relação de custo-benefício (Wottrich, Reijmersdal, e Smit, 2018).

Zurawski (2011) remete-nos para a integração e normalização dos cartões de fidelização nas nossas compras do quotidiano. Apesar destes cartões não serem necessários para realizarmos compras nem de substituírem o dinheiro, eles representam uma parte específica das nossas compras. Estes cartões prometem recompensas aos consumidores leais a uma loja, cadeia ou marca. Em contrapartida das recompensas oferecidas aos consumidores que utilizam os cartões de fidelização, as organizações recolhem os seus dados pessoais. Estes dados são posteriormente integrados nas lógicas da economia da informação pessoal (Boyne, 2000; Lyon, 2009, 2015; Zurawski, 2011; Ball, 2017). Zurawski (2011) argumenta que os cartões de fidelização representam a ligação entre as práticas locais e os fluxos de dados a nível global. Neste sentido, os cartões de fidelização constituem a interface entre as práticas locais de consumo, por um lado integram o ato mundano de promover descontos e recompensas aos clientes leais e, por outro, estabelecem a ligação ao que tem sido denominado de economia da informação pessoal.

Os indivíduos lidam com os cartões de fidelização de diversas formas, de acordo com Zurawski (2011), os quatro fatores que mais motivam a adesão dos indivíduos aos cartões de fidelidade são os bónus/pontos, os possíveis lucros na utilização, a confiança que depositam na organização em questão e os hábitos de compra. Apesar de um tipo de racionalismo económico estar claramente presente na escolha da adesão, ele não constitui de forma alguma o único argumento para a adesão. As questões dos hábitos de compra e da confiança estão fortemente relacionadas, os consumidores aderem aos cartões de fidelização de determinadas organizações, porque compram mais frequentemente ou porque confiam nelas. Pode-se analisar a adesão a um cartão de fidelização, como uma forma de reconhecimento de uma prática de consumo frequente. Desta forma, parece haver um fluxo de confiança entre o consumidor e a empresa no qual se assiste a uma relação social de compromisso mútuo.

Ao nível das preocupações demonstradas pelos aderentes aos cartões de fidelização, no estudo de Zurawski (2011) os indivíduos demonstraram que não são influenciados pela sua preocupação ou pela consciência que os seus dados estão a ser recolhidos. Um dos únicos fatores que preocuparam os entrevistados deste estudo em relação à recolha de dados através dos cartões, foi a receção de publicidade indesejada. Outro aspeto importante da investigação do autor, foi a abordagem, por parte dos entrevistados, feita à recolha de dados como se ela constituísse algo muito abstrato e pouco claro.

A vigilância comercial constitui uma parte mercantilizada do consumo, inquestionavelmente manifestada nas trocas de dados por benefícios comerciais presentes na utilização de cartões de fidelidade e das aplicações móveis. Porém, importa destacar que estas duas práticas não representam de forma alguma a totalidade dos contextos onde a troca se manifesta. Foram apresentados apenas dois exemplos significativos, onde esta troca já foi identificada e estudada (Zurawski, 2011).

2.3.3 – A troca de dados pessoais por conveniência

Atualmente a troca de dados pessoais por conveniência é bastante frequente. Park, Shung e Shin (2018) argumentam que o processo cognitivo para que uma pessoa se aperceba do custo (potencial), para a sua privacidade ao utilizar plataformas que recolhem dados, é de uma exigência cognitiva elevada. Sendo assim, os autores defendem que as decisões dos indivíduos tendem a centrar-se mais nos benefícios imediatos e na conveniência que lhes é oferecida por estas plataformas.

Enquanto muitos indivíduos não estão preocupados ou conscientes da recolha dos seus dados e do respetivo impacto ao nível da sua privacidade, as entidades, cuja prosperidade depende do *Big Data*, adotam uma postura muito mais sofisticada. Estas entidades utilizam frequentemente técnicas, baseadas em conhecimento altamente especializado ao nível do comportamento humano, para persuadirem à cedência de dados pessoais (Acquisti, Brandimarte e Loewenstein, 2015). Estas técnicas jogam com a maleabilidade das preferências de privacidade, um termo desenvolvido por Acquisti, Brandimarte e Loewenstein (2015) para se referirem a vários fatores, às vezes subtis, que podem ser utilizados para ativar ou suprimir preocupações com a privacidade.

A maleabilidade e a conveniência têm interações percetíveis e significativas. As definições predefinidas desempenham um papel importante, dado que através delas as entidades conseguem afetar os comportamentos de privacidade dos indivíduos. Não alterar as definições predefinidas é conveniente, e os indivíduos interpretam frequentemente as predefinições como recomendações implícitas (Acquisti, Brandimarte e Loewenstein, 2015). Um exemplo prático das implicações que as definições predefinidas podem ter no comportamento foi apontado por Calo (2014), o autor argumenta que se os consumidores não precisarem de manifestar a sua recusa para a recolha dos seus dados, mais dados acabarão por ser recolhidos. No entanto, se a predefinição funcionar de forma antónima, ou seja, se for necessário o consumidor aceitar a recolha de dados, ele estará mais ciente e porventura mais preocupado com a invasão da sua privacidade.

À parte das definições predefinidas, os websites utilizam outras funcionalidades que podem frustrar ou confundir utilizadores (Acquisti, Brandimarte e Loewenstein, 2015). Segundo Hull (2015), as noções de autogestão da privacidade dependem de duas assunções, a primeira é que os indivíduos se comportam racionalmente quando expressam as suas preferências de

privacidade, a segunda é a que essas preferências são reveladas adequadamente através dos seus comportamentos. O autor argumenta que, infelizmente, nenhuma destas assunções está correta, afirmando que existem três tipos de razões para que a autogestão da privacidade não proteja a privacidade: (i) os utilizadores não sabem nem podem saber exatamente ao que estão a consentir; (ii) é difícil configurar as preferências de privacidade; (iii) recusar participar em websites que invadem a privacidade é cada vez mais difícil (Hull, 2015). Algo visível com a recente resposta de inúmeros websites à nova regulamentação de proteção de dados na União Europeia, que implica o consentimento do utilizador para que os seus dados sejam recolhidos. Como resposta a esta nova regulamentação, diversos websites decidiram tornar este consentimento como o requisito para visitar a sua página, barrando o acesso a todos os utilizadores que não consintam a recolha de dados pessoais.

2.4 – Estratégias de Neutralização da Vigilância

Os sujeitos da vigilância, como se tem vindo a referir ao longo da dissertação, quase nunca são meramente passivos. Existem inclusive, várias associações profissionais, movimentos sociais e políticos que podem apoiar a resistência à vigilância. Existe literatura sobre como resistir à vigilância. Por exemplo, uma pesquisa no *Google* sobre métodos para resistir à vigilância apresenta-nos inúmeros *websites* com conteúdo sobre as diversas formas de como o podemos fazer (Marx, 2016).

Apesar dos sistemas de vigilância terem quase sempre contradições, ambiguidades, falhas, ou limitações, estruturais ou culturais, que podem ser exploradas pelos cidadãos (Marx, 2016), a assimetria de poder entre os sujeitos e os agentes da vigilância é clara. Diversas entidades têm a capacidade de ultrapassar as diversas estratégias de neutralização da vigilância; têm, por exemplo, sistemas de recolha de dados com capacidade para eliminar dados adulterados ou ultrapassar ferramentas que tentam garantir o anonimato (Howe, 2015). No entanto, essa capacidade requer uma quantidade significativa de recursos que se multiplica consoante o número de indivíduos a adotarem estratégias para contrariar a vigilância (Acquisti, Brandimarte e Loewenstein, 2015). Por conseguinte, a adoção de estratégias de neutralização pode tornar a recolha de dados mais ambígua, confusa, mais dificilmente utilizada e, consequentemente, menos valiosa para as entidades. Algo que demonstra que os utilizadores da internet podem colocar entraves e dificultar a recolha massificada de dados (Howe, 2015).

O reportório de estratégias de neutralização é limitado e muda consoante as sociedades, sendo a natureza, estrutura, recursos e contextos da vigilância fatores importantes na sua constituição. Marx (2016, pp. 145) construiu uma tabela, baseada indutivamente em entrevistas e observação feitas pelo autor, onde definiu 12 tipos de ações de neutralização da vigilância. A Tabela 1, foi elaborada com base nos contributos do autor e apresenta resumidamente as estratégias consideradas nesta dissertação.

Tabela 1 - Estratégias de Neutralização da Vigilância

Técnica de Neutralização	*Acão*
Descoberta	Descobrir se a vigilância está presente, e se estiver, onde, por quem e como
Evitamento	Optar por localizações, intervalos de tempo, e meios que não estão sujeitos a vigilância
Troca	Transferir um resultado autêntico para alguém ou para algo a que a informação não se aplica
Distorção	Alterar os dados que fornecemos de forma a que sejam tecnicamente válidos, mas a inferência dos dados seja inválida
Bloqueamento	Eliminar ou tornar os dados inacessíveis
Disfarce	Bloquear, mas adicionando dados enganosos
Inviabilização	Tornar determinado dispositivo de vigilância inoperável
Recusa	Ignorar a vigilância e o que é suposto ela deter
Explicação	Justificar um resultado desfavorável através de uma reformulação do resultado para que se torne aceitável, ou através do fornecimento de dados alternativos e reivindicações de direitos civis
Conluio	Efetuar ações em conluio com os agentes (vigilantes)
Inversão da Vigilância	Inverter os papeis, de forma a que os sujeitos apliquem as táticas dos agentes, tomando vantagem do potencial das ferramentas de vigilância

Fonte: elaborado a partir de Marx (2016, pp.145)

De um modo geral, as ações que o autor apresentou permitem identificar alguns aspetos comuns de resistência à vigilância. As ações que um indivíduo adota na tentativa de resistir à vigilância são frequentemente encobertas para maximizar a sua eficácia, evitar a suspeição e as potenciais sanções. Além disso, o objetivo passa, na maior parte das vezes, por combater uma determinada aplicação da vigilância, e não por aboli-la. Cada estratégia pode ser vista como apenas uma parte de um conjunto de resistência e de não-conformidade (Marx, 2016). De seguida apresentam-se, de forma mais aprofundada, todas as estratégias de neutralização consideradas nesta investigação.

A estratégia de recusa, aprofundada mais abaixo, na sua forma extrema envolve dizer literalmente não. Mas a maior parte das estratégias envolvem uma recusa mais subtil e parcial. Cada estratégia refere-se a um elemento empírico distinto, mas não são mutualmente exclusivos e podem ser relacionados sistematicamente. As estratégias também podem ser ligadas lógica e temporalmente: a descoberta que estamos a ser observados em determinado local leva-nos a evitá-lo posteriormente. A neutralização pode ser direta ou indireta, os sujeitos podem tentar afetar os dados que oferecem, ou que lhes são recolhidos, escondendo ou alterando, pelo menos até certo ponto, a sua identificação, localização e/ou as condições nas quais a recolha de dados ocorre (Marx, 2016).

A estratégia de descoberta está relacionada com a consciencialização sobre a vigilância. As ações associadas a esta estratégia podem ser identificadas como detetoras da vigilância, tendo

o sujeito como objetivo descobrir se a vigilância está a ocorrer em determinado contexto, e se sim, onde, por quem e como (Marx, 2016).

Já a estratégia de evitamento e as ações subsequentes podem seguir-se à descoberta de que a vigilância está presente. Geralmente, os sujeitos assumem que o evitamento é uma resposta prudente perante a possibilidade de a vigilância estar presente. As ações de evitamento são passivas e envolvem uma certa seletividade. Quando um sujeito utiliza a estratégia de evitamento, não tenta confrontar diretamente a vigilância. Pode-se argumentar que quando a descoberta da vigilância leva a ações autorreguladas de evitamento de comportamentos, o objetivo de dissuasão da vigilância foi concretizado. No entanto, se atentarmos no quotidiano, podemos verificar que a dissuasão causada pela vigilância tem, frequentemente, uma duração breve. O condutor que reduz a velocidade devido aos avisos de radar, com o tempo, irá adotar comportamentos de deslocamento para tempos, espaços ou meios onde presume que a vigilância não está presente ou é irrelevante (Marx, 2016). Esta estratégia também é visível nas redes sociais, onde se pode adotar estratégias como o uso superficial destas plataformas, mudar as definições de privacidade e reduzir a quantidade de informação publicada na plataforma (Dal Bello, 2011; Augusto e Simões, 2017). No âmbito desta investigação decidiu-se englobar nas estratégias de evitamento o uso seletivo de redes Wi-Fi, como por exemplo um indivíduo evitar ao máximo conectar-se a redes de Wi-Fi públicas.

Por outro lado, a estratégia de troca envolve a verificação, a certificação e a validação: um sujeito pode transferir um resultado autêntico para alguém, ou algo, ao qual ele não se aplica. Enquanto o sistema de vigilância deteta o acesso como legítimo, preciso e válido, falha ao detetar a identidade do individuo que utilizou o meio de acesso. Um exemplo comum da utilização desta estratégia é a transferência de certificação: um sujeito consegue aceder a determinado serviço\local ao utilizar um bilhete, cartão de acesso, licença ou palavra-chave pertencente a outro indivíduo (Marx, 2016).

As próximas três estratégias de neutralização (distorção, bloqueamento e disfarce), abaixo apresentadas, são agrupadas por alguns autores, como por exemplo, Howe (2015), Acquisti, Brandimarte e Loewenstein (2015), como pertencendo a um tipo de estratégia mais geral, a de ofuscação. Na definição desta estratégia verificam-se elementos das estratégias acima referidas, no entanto, optou-se por seguir as denominações e características apontadas por Gary Marx (2016) devido à sua análise mais pormenorizada das estratégias de neutralização da vigilância.

Passando agora para a definição das estratégias de distorção, estas são ações que manipulam a recolha de dados de forma a que os resultados da recolha e análise sejam tecnicamente válidos, mas as inferências retiradas a partir da recolha sobre o desempenho, o comportamento ou os atributos sejam inválidas. As ações de distorção contrastam com as de troca, enquanto as ações de troca implicam uma inferência errada em relação à identidade dos indivíduos, as de distorção apenas afetam as inferências em relação aos dados recolhidos, não escondendo

necessariamente a identidade do sujeito (Marx, 2016). No contexto online, esta estratégia pode manifestar-se na criação de um perfil falso em determinada plataforma. No contexto de criação de perfis falsos, o utilizador fornece dados que são considerados como legítimos pelos sistemas de vigilância, ao mesmo tempo que impossibilita que a sua identidade seja desvendada através desses dados. Esta estratégia é também visível quando o utilizador opta por adulterar determinadas informações pessoais que fornece a uma plataforma (Dal Bello, 2011). Ou através da utilização de extensões de browser como a "I Like What I See", que aciona automaticamente todos os botões de "gosto" que aparecem no Facebook dos utilizadores escondendo os verdadeiros interesses dos indivíduos (Howe, 2015).

As estratégias de disfarce tal como as de bloqueamento chamam à atenção para os aspetos comunicativos da vigilância. Através das estratégias de bloqueamento mesmo que os agentes da vigilância pretendam ler sinais oferecidos pelos sujeitos, o bloqueamento elimina ou torna inacessível o que é de interesse para os agentes. Se os sujeitos não conseguirem impedir, fisicamente ou de outra forma, que os agentes acedam às suas informações, podem tentar tornar um determinado dispositivo, ou aspetos que ele possa recolher como a identidade, aparência, localização, ou comportamento do cidadão, inutilizáveis. A encriptação das comunicações é um exemplo, já que permite que o intercetor saiba que algo está a ser comunicado, mas o seu conteúdo é inacessível sem a sua decriptação (Marx, 2016).

As estratégias de disfarce são uma forma de bloqueamento, mas que adiciona dados enganadores no que respeita à identidade, estatuto e/ou localização do sujeito da vigilância. Resumidamente, a maior diferença entre esta estratégia e a de bloqueamento é a adição de informação enganosa intencionalmente utilizada para iludir os agentes vigilantes. Bloquear sem disfarce pode, facilmente, chamar à atenção. (Marx, 2016). Se atentarmos no mundo da Internet, pode-se considerar que a arquitetura da própria Internet, que depende de múltiplas comunicações entre aparelhos, possibilita a utilização de ferramentas computacionais como o navegador de internet "TOR", ou outras ferramentas que atuam de forma semelhante para neutralizar a vigilância. O TOR permite anonimato ao utilizador através da sua ligação a uma "rede de confiança", constituída por vários aparelhos, antes de o utilizador aceder a partes potencialmente vigiadas da internet. A anonimidade surge dos percursos complexos que os dados percorrem ao entrar e sair da rede de confiança encriptada, dificultando enormemente a identificação dos dados recolhidos a um determinado aparelho (Marx, 2016).

As estratégias de inviabilização têm como objetivo tornar determinado dispositivo de vigilância inoperável. No entanto, à semelhança das ações de bloqueamento, os agentes (vigilantes) irão provavelmente descobri-las a determinado ponto. Alguns exemplos de ações desta estratégia incluem desligar linhas de telefone ou de eletricidade, tapar uma câmara com fita cola ou com post-its (Marx, 2016).

Enquanto as outras estratégias mencionadas se referem mais à recusa de cooperação com os agentes (vigilantes), as estratégias de recusa, aqui aprofundadas, envolvem uma recusa mais

direta que pode passar por ignorar a vigilância ou tentar invertê-la: recusar fornecer informações ou até destruir aparelhos de vigilância são exemplos de ações desta estratégia. Um outro exemplo, significativamente diferente dos mencionados, envolve a performance teatral em determinada ação, podendo iludir o agente através da mesma (Marx, 2016; Lyon, 2018). Nesta investigação considerou-se a rejeição para a partilha de cookies recolhidos por determinada plataforma, como uma estratégia de recusa.

As estratégias de explicação envolvem um esclarecimento sobre determinado resultado desfavorável na tentativa de o tornar aceitável. O indivíduo pode fornecer explicações alternativas às informações que foram recolhidas oficialmente. Podem utilizar uma retórica de reformulação ou alegar que, apesar do teste ser preciso e válido, desconheciam que determinado comportamento podia resultar num resultado desfavorável (Marx, 2016).

Quanto à estratégia conluio, como o nome indica, envolve o conluio entre sujeito e agente de vigilância. Esta é uma estratégia regularmente presente em crimes de colarinho branco. Tendo os criminosos controlo sobre os sistemas e agentes de vigilância através do conhecimento obtido através do conluio. Outro exemplo prático ocorre quando alguém, devido à posição de poder que ocupa, simplesmente apaga um determinado registo (Marx, 2016).

Por último, as ações que pretendem inverter a vigilância são normalmente postas em prática através da utilização de ferramentas de vigilância baratas e fáceis de utilizar que se tornaram acessíveis. Estas tecnologias são frequentemente utilizadas de várias formas e muitas vezes transcendem os usos pretendidos. Estas utilizações incluem o redireccionamento destas tecnologias: os sujeitos utilizam as mesmas ferramentas que os agentes (vigilantes) para registar o comportamento destes e as suas interações com os sujeitos da vigilância (Marx, 2016). Nesta estratégia os papéis invertem-se, trata-se da vigilância do tipo *sousveillance* anteriormente referida (Galič, Timan e Koops, 2017).

Segundo Marx (2016), é também possível categorizar os cidadãos consoante as suas respostas ao nível da sua atitude e comportamento em relação à vigilância, veja-se a Tabela 2.

Tabela 2 – Atitudes e comportamentos face à vigilância

Conformistas Verdadeiros	Pessoas que têm uma atitude de aceitação perante a vigilância e que, consequentemente, não adotam qualquer tipo de comportamento para a contrariar.
Conformistas Intimidados (ou que não têm os recursos ou capacidades contrariar a vigilância)	Pessoas que têm uma atitude de rejeição à vigilância, mas que, nas suas ações, acabam por a aceitar.
Rebeldes Relutantes	Pessoas que têm uma atitude de aceitação perante a vigilância, mas nos seus comportamentos tentam rejeitá-la, por exemplo sob a pressão de pares.
Rebeldes	a) Verdadeiros Rebeldes: têm uma atitude de rejeição à vigilância e tentam neutralizá-la abertamente b) Rebeldes de "Armário": têm uma atitude de rejeição à vigilância, mas tentam neutralizá-la de uma forma discreta.

Fonte: Marx, 2016, pp.170

Marx (2016) ao considerar as conexões entre as estratégias individuais e as formas de protesto cujo objetivo é marcar uma posição, reflete sobre a sua relação. Terão as estratégias individuais de neutralização um sentido mais alargado de protesto político, ou serão, por outro lado, apenas formas de reduzir a influência da vigilância nas suas vidas sem que haja um interesse em modificar as políticas?

Na próxima secção explora-se como o ativismo pode constituir uma estratégia com a ambição de alterar as políticas relacionadas com a vigilância.

2.5 – Ativismo como Estratégia para Contrariar a Vigilância

Na última década, também devido às revelações de Snowden, a (im)possibilidade de se tentar resistir à vigilância eletrónica tem suscitado um debate substancial, ainda que seja realizado maioritariamente em círculos de ativistas e académicos. Tem-se discutido a dificuldade que os utilizadores têm em resistir aos processos de vigilância. Enquanto diversos autores elaboram investigações críticas de alguns processos de vigilância, outros defendem a importância do fortalecimento da alfabetização digital do cidadão, particularmente ao nível de compreensão da privacidade e segurança em relação aos dados pessoais, para contrariar a vigilância (Dijck, 2014).

Têm surgido diversos atos corajosos de ativismo contra a vigilância nos últimos anos. Desde manifestações individuais de *whistleblowers* até atos de cidadãos severamente prejudicados por processos de vigilância como aconteceu recentemente na Turquia. Topak (2017) afirmou que mais de metade da população turca recusou consentir a vigilância, recentemente, imposta pela Partido da Justiça e Desenvolvimento. O autor afirma que contra todas as probabilidades, diversos indivíduos continuam a envolver-se em atos corajosos de resistência direta. Como exemplo, o autor oferece-nos o caso de dois professores dispensados pelo regime que decidiram entrar numa greve de fome como forma de protesto à máquina de vigilância do Partido no poder na Turquia.

Também já decorreram ondas de protesto contra a vigilância em solo europeu. Desde o outono de 2008 uma nova onda de protestos emergiu na Alemanha, tendo como objetivo protestar contra a vigilância governamental. Esta onda de protestos inclui demonstrações anuais sob o *slogan* "*freedom not fear*", e foi bem-sucedida ao aumentar a sensibilização do público para a vigilância e proteção de dados. Esta onda de protestos foi desencadeada pela decisão do Governo Alemão em implementar medidas de retenção de dados. A retificação de uma série de políticas relacionadas com a recolha, processamento, armazenamento de dados pessoais, bloqueamento de sites e, acima de tudo, a permissão para armazenar dados sobre as comunicações de internet e telecomunicações sem uma justificação específica, foi a principal razão para o surgimento desta onda de protestos (Daphi, Lê e Ullrich, 2013).

II - Das Orientações Metodológicas à Interpretação e Análise dos Resultados

Capítulo 3 – Procedimento Metodológico

Neste capítulo apresentam-se os objetivos da investigação, tal como todo o processo metodológico utilizado. Começa-se por apresentar os objetivos e o modelo de análise, posteriormente apresenta-se o cariz da metodologia escolhida, assim como a técnica utilizada. Por último caracteriza-se os dados sociodemográficos dos respondentes.

Partindo dos conceitos de imaginários e práticas em relação à vigilância, elaborados por Lyon (2018), e explorados no Capítulo 1, esta dissertação tem como objetivo geral analisar: por um lado, o modo como os respondentes percecionam e experienciam a vigilância eletrónica; e por outro as suas práticas perante a vigilância. De forma a aprofundar o objetivo geral, formulou-se sete objetivos mais específicos:

i) Analisar a consciencialização que os indivíduos têm sobre a vigilância eletrónica;
ii) Perceber em que situações cedem (ou não) os seus dados pessoais;
iii) Analisar que mecanismos de recolha conhecem, assim como os modos do seu funcionamento;
iv) Captar os aspetos considerados positivos e negativos da vigilância;
v) Analisar as perceções em relação aos diferentes tipos de vigilância: lateral; governamental e comercial;
vi) Mapear as ações de negociação da vigilância e as razões para a sua utilização;
vii) Averiguar que consequências, da vigilância eletrónica, são identificadas pelos respondentes.

Para responder aos objetivos acima referidos, elaborou-se um modelo de análise composto por oito dimensões de análise: (i) consciencialização dos processos de vigilância; (ii) cedência de dados pessoais; (iii) mecanismos de recolha; (iv) vigilância lateral; (v) vigilância governamental; (vi) vigilância comercial; (vii) ações de negociação da vigilância e, por último, (viii) a perceção sobre as consequências da vigilância.

Quanto aos indicadores de cada dimensão de análise, optou-se por apresentá-los na Tabela 3 de forma a simplificar a sua apresentação.

Tabela 3 - Modelo de Análise

Dimensões de análise	Indicadores
I - Consciencialização dos processos de vigilância	Existência de processos de vigilância
	Identificação de entidades/plataformas vigilantes
	Perceção sobre os objetivos da vigilância
	Preocupação com os processos de vigilância
II - Cedência de dados pessoais	Facilidade no fornecimento de dados pessoais
	Importância do consentimento informado
	Perceção sobre a venda de dados pessoais
	Possibilidade de *social sorting*
III - Mecanismos de recolha	Identificação de mecanismos de recolha de dados
	Conhecimento e opinião sobre a forma como os mecanismos funcionam
IV - Vigilância lateral	Exposição voluntária nas redes sociais
	Tendência voyeurística nas redes sociais
	Condicionamentos no comportamento
V - Vigilância governamental	Identificação da informação recolhida por agências governamentais
	Propósitos e aceitação
	Perceção sobre a classificação e categorização dos cidadãos
	Desencadeamento ou aprofundamento das desigualdades sociais
VI - Vigilância comercial	Noção sobre a recolha de dados
	Reconhecimento de vantagens e desvantagens da cedência de dados
	Opinião sobre o *social sorting* comercial
VII - Ações de negociação da vigilância	Valorização subjetiva da privacidade online
	Condicionamento da atividade devido à vigilância
	Incómodo causado pela vigilância
	Estratégias de neutralização da vigilância
VIII - Perceção sobre as consequências da vigilância	Potenciais consequências
	Consequências atuais
	Consequências ao nível pessoal

3.1 – A Metodologia Qualitativa

Com base nos objetivos desta dissertação no que respeita à necessidade de, além de captar as perceções, analisar o papel que os cidadãos têm na negociação da vigilância, a adoção de uma metodologia de cariz compreensivo é fundamental.

Seguindo os contributos Guerra (2006), esta investigação segue a postura analítica e de reconstrução do sentido. Nesta, a pesquisa sociológica procura produzir metodicamente sentido

social a partir da exploração de entrevistas de pesquisa. O sujeito é visto como uma síntese ativa do todo social, a realização de uma análise de conteúdo pretende interpretar a relação entre o sentido subjetivo da ação, o ato objetivo e o contexto social no qual decorrem as práticas em análise. O centro de análise passa, fundamentalmente, pela categorização social acionada por uma narração que permite ao sujeito estruturar o sentido do mundo social e o seu lugar nesse mundo, tornando possível a sua interpretação através de um processo de interpretação metódico. O processo de interpretação deve produzir categorias e proposições (ou hipóteses explicativas), que são indispensáveis no entendimento dos fenómenos através de um processo indutivo e com origem na narração (Guerra, 2006).

A metodologia qualitativa enquadra-se na postura teórico-epistemológica acima referenciada, ela envolve uma abordagem interpretativa onde se visa compreender os significados que as pessoas atribuem a determinado fenómeno, tal como as ações, decisões, crenças e valores dos participantes tendo em conta os seus mundos sociais (Richie, 2003; Flick, 2009). Algo que dado os objetivos e a perspetiva teórica escolhida da vigilância como cultura, se reforça nesta investigação. Este enfoque nos significados que as pessoas dão aos fenómenos sociais, também vai ao encontro da importância de entender a negociação da vigilância dos indivíduos nos seus próprios termos, sugerida por Monahan (2011) e Lyon (2018). Ademais, Green e Zurawski (2015) defendem a necessidade de uma maior integração de metodologias de carater qualitativo nos estudos da vigilância. Os autores defendem que estes estudos iriam beneficiar de uma abordagem mais etnográfica, que fosse capaz de capturar a vigilância como uma atividade situada no nosso quotidiano. A metodologia qualitativa é também, para Lyon (2018), adequada para explorar a variedade de perceções dos indivíduos sobre a vigilância.

A escolha pela metodologia qualitativa está, por outro lado, relacionada com o grau de profundidade pretendido (Ragin, 2011). Nos resultados de investigações qualitativas tenta-se, frequentemente, responder a questões como “o que é?”, “como?” e “porquê”, que devem ser selecionadas com base em critérios salientes e devidamente justificados. Os métodos de recolha de dados envolvem, frequentemente, contacto próximo entre o investigador e os participantes na investigação, o que permite a exploração de determinadas temáticas de forma interativa e construtiva (Richie e Lewis e Elam 2003).

Após a apresentação do cariz da metodologia utilizada, importa referir a técnica que se optou por utilizar nesta investigação, a entrevista semiestruturada.

3.2 – A Entrevista Semiestruturada

A entrevista é uma técnica frequentemente utilizada nas ciências sociais, esta implica uma conversa, em forma de entrevista, na qual uma pessoa tem o papel de investigador. As entrevistas podem fornecer dados sobre perceções, opiniões, formas de experienciar acontecimentos, entre outros (Arksey e Knight, 1999).

As entrevistas podem ser categorizadas consoante o seu grau de estruturação, podendo ser consideradas estruturadas, semiestruturadas ou não-estruturadas (Gray, 2004; Ragin, 2011; Roulston e Choi, 2018). Numa entrevista estruturada, o investigador irá seguir as questões presentes no guião de entrevista de forma estruturada e metódica. Enquanto na entrevista não-estruturada as questões presentes no guião, podem servir apenas como um auxiliar de memória para relembrar o investigador das principais questões que precisa de explorar. Ao passo que nas entrevistas semiestruturadas utiliza-se um guião com as questões, podendo, no entanto, o entrevistador incluir novas questões de aprofundamento quando as considerar pertinentes (Gray, 2004).

Nesta investigação optou-se pela utilização de entrevistas semiestruturadas, embora se tenha recorrido a algumas (poucas) questões de resposta direta relacionadas com as práticas face à vigilância.

Nesta técnica, os sujeitos adquirem o estatuto de informadores privilegiados. Os defensores das metodologias compreensivas argumentam que a intenção deste tipo de pesquisa é articular as várias dimensões da vida social ao mesmo tempo que se recusa a rutura entre o "sujeito da ciência" e o seu "objeto", o sujeito real dito de outra forma. Pretendem-se novas reconciliações ente teoria e prática, entre a "ciência do geral" e os "saberes particulares", entre o individuo e a sociedade. Do ponto de vista do entrevistado, o momento da entrevista exige-lhe um processo de totalização através do qual procurará dar consistência às suas racionalidades, seja em forma de ação ou pensamento. Frequentemente, a racionalidade para momentos que pareciam ser espontâneos, pode ser encontrada no momento da entrevista (Guerra, 2006). O grau de maleabilidade da aplicação desta técnica, tal como o grau de liberdade dado ao entrevistado, é de grande importância visto que as entrevistas servem para encontrar pistas de reflexão, ideias, entre outros assuntos e não para verificar hipóteses pré-estabelecidas (Arksey e Knight, 1999; Quivy e Campenhoudt, 2008).

Nas entrevistas semiestruturadas, como se referiu, a formulação de um guião de entrevista é fundamental, este deve ser constituído por questões geradas através da literatura científica da temática que se vai investigar (Gray, 2004). Importa salientar que as entrevistas são complementares e que se enriquecem mutuamente. A composição dos guiões de entrevista pode mudar ao longo de uma investigação, podendo alterar-se devido: às características específicas dos entrevistados\as; a novas questões que surjam através de outras entrevistas (Quivy e Campenhoudt, 2008); da consulta de nova literatura ou de ideias retiradas de novas conferências a que o investigador tenha assistido (Rapley, 2007).

Em suma, os motivos para a utilização desta técnica no âmbito da presente investigação são vários: (i) o objetivo da investigação é largamente exploratório, e envolve a necessidade de recolher e analisar dados como as crenças e perspetivas dos indivíduos (Gray, 2004; Guerra, 2006; Flick, 2009; Roulston e Choi, 2018); (ii) a possibilidade de aprofundar determinado tema através de questões que possam não estar inicialmente contempladas no guião das entrevistas,

é fundamental para enriquecer a futura análise e interpretação dos dados recolhidos, algo importante para responder aos objetivos da investigação e (iii) a pertinência da utilização de entrevistas nos estudos da vigilância, especialmente quando estes se concentram no modo como os indivíduos experienciam e captam a vigilância (Green e Zurawski, 2015).

3.3 – Considerações Éticas

Qualquer investigação deve-se preocupar com princípios éticos. É necessário proteger os interesses dos indivíduos que estão a ser estudados, especialmente se estes se encontrarem em posições vulneráveis, ou em ocasiões onde é possível identificar os indivíduos através das suas contribuições para o estudo (Flick, 2009). Geralmente os códigos de ética requerem que a investigação seja baseada no consentimento informado (ver Anexo 1). Este deve ser um pré-requisito para a participação na investigação, ele tem de ser dado por alguém competente para o fazer, a pessoa que dá o consentimento deve ser adequadamente informada e o consentimento deve ser dado de forma completamente voluntária (Flick, 2009). Nas investigações qualitativas, que utilizam a entrevista como técnica, deve-se adotar uma postura especialmente sensível às questões éticas da investigação, uma vez que a recolha de informação envolve, frequentemente, um contacto próximo com o quotidiano e vida pessoal dos participantes (Mertens, 2018).

Também se deve garantir que a investigação não prejudica os respondentes, algo que inclui respeitar a privacidade destes, tal como uma comunicação honesta dos objetivos da investigação. Alguns autores apontam para uma teoria da ética, ligada a quatro características: (i) a não-maleficência - os investigadores devem evitar prejudicar os participantes; (ii) a beneficência - a investigação deve produzir algum tipo de benefício identificável; (iii) a autonomia e a autodeterminação - os valores e decisões dos participantes na investigação devem ser respeitados; e por último (iv) a justiça - todos os indivíduos devem ser tratados de igual forma (Flick, 2009).

A dignidade e os direitos dos participantes têm de ser garantidos. Caso, por exemplo, o investigador note que o indivíduo, que participa na sua investigação, está claramente desconfortável ou emocionalmente instável, deve considerar parar imediatamente com a recolha de informação, e perguntar ao participante se quer fazer um intervalo, mudar o tópico que estavam a abordar ou terminar a entrevista naquele momento (Rapley, 2007).

3.4 - Seleção e Caracterização dos Entrevistados

Em investigações de cariz metodológico qualitativo, que utilizam a entrevista como técnica, existem vários fatores a que se deve atentar para se definir a população entrevistada. O tamanho da população-alvo é um dos que suscita mais debate; os estudos qualitativos costumam conter poucos casos (Lee, 2014; Roulston e Choi, 2018; Schreier, 2018). O número de entrevistas ou observações que se devem efetuar depende das questões que o investigador

colocou no âmbito da sua investigação (Roulston e Choi, 2018; Schreier, 2018). A análise aprofundada, fundamental nesta metodologia, impede, na maior parte dos casos, que se contemple uma amostra mais numerosa, devido a limitações temporais e/ou de recursos financeiros (Richie, Lewis e Elam, 2003; Flick, 2009). Alguns autores defendem que, ao contrário do que sucede na investigação quantitativa, o tamanho da amostra na investigação qualitativa não é relevante, ou é no mínimo uma preocupação secundária (Schreier, 2018). O critério da saturação da informação recolhida é o melhor indicador de que se chegou ao número limite necessário de entrevistas. Como Flick (2009) afirma, quando se atinge um ponto no qual não estão a surgir novas perspetivas nas entrevistas, não se justifica continuar a alargar o número. Para que seja possível aferir se os dados atingiram um grau de saturação elevado, é necessário estudar e analisar os dados à medida que o investigador os vai recolhendo. Deve-se então atentar mais na qualidade dos dados recolhidos do que no tamanho da população estudada (Lee, 2014).

É igualmente importante definir e explicar a estratégia de recrutamento utilizada para compor a população entrevistada, tal como as suas especificidades e limitações (Lee, 2014). Nesta investigação utilizou-se como estratégia de recrutamento, o pedido, junto de pessoas conhecidas, para a realização de entrevistas. Posteriormente pediu-se aos entrevistados, sugestões sobre pessoas que pudessem estar dispostas a participar no estudo. Além dos aspetos acima referidos, só se entrevistaram cidadãos que utilizassem, com frequência, pelo menos um dispositivo tecnológico com conexão à internet.

Nesta dissertação realizaram-se 16 entrevistas semiestruturadas, estas tiveram uma duração que variou entre os quarenta e os noventa e cinco minutos, e foram direcionadas a indivíduos com perfis sociodemográficos heterogéneos ao nível de: idade; género; escolaridade e conhecimento informático. A caracterização sociodemográfica da população entrevistada é apresentada detalhadamente na Tabela 4.

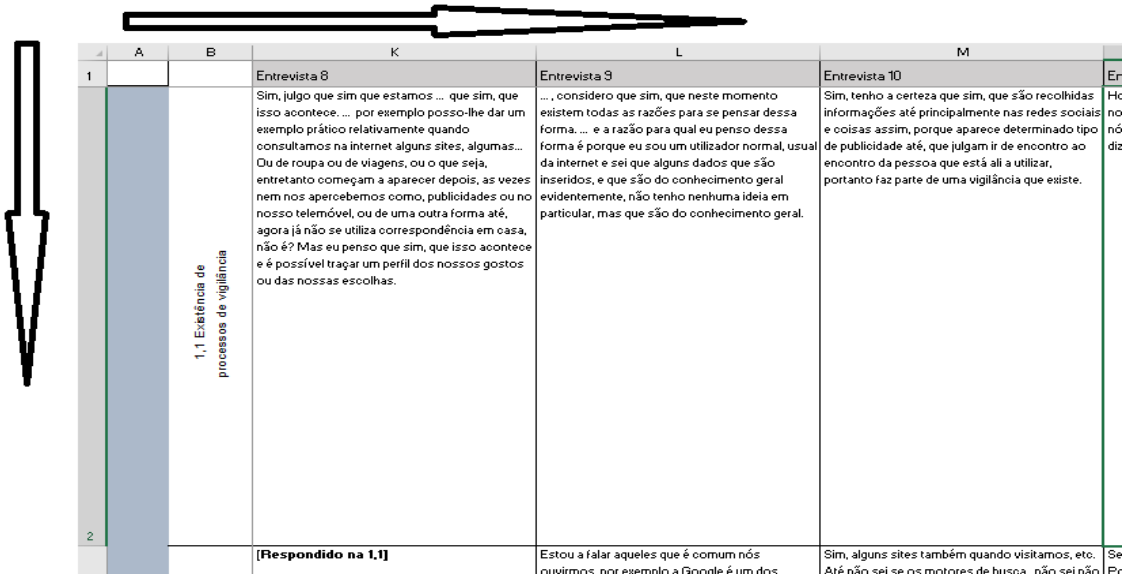
Tabela 4 - Caracterização sociodemográfica da população-Alvo

Entrevistados	Sexo	Idade	Habilitações Literárias	Área Profissional/Formação	Distrito de Residência
Entrevistado 1	F	35	12º Ano	Assistente Operacional	Açores
Entrevistado 2	F	40	12º Ano	Escriturária	Açores
Entrevistado 3	M	35	12º Ano + Curso Técnico Nível IV	Taxista\ Técnico de Informática	Açores
Entrevistado 4	M	25	10º Ano	Empregado de Mesa e Bar	Açores
Entrevistado 5	F	23	Licenciatura	Estudante\Ciência Política	Porto
Entrevistado 6	M	47	12º Ano	Gerente\Comerciante	Lisboa
Entrevistado 7	M	20	12º Ano (Frequenta o E.S)	Estudante\Medicina	Braga
Entrevistado 8	F	50	Mestrado	Técnica Superior\Sociologia	Castelo Branco
Entrevistado 9	M	57	12º Ano	Assistente Operacional	Castelo Branco
Entrevistado 10	F	52	Doutoramento	Ensino Secundário\ Educação	Braga
Entrevistado 11	F	55	12º Ano	Assistente de Contacto\Técnica de Controlo de Qualidade	Porto
Entrevistado 12	M	25	Licenciatura	Investigador\ Informática Web	Santarém
Entrevistado 13	M	24	12º Ano - Profissional	Segurança\ Técnico de Sistemas Solares Fotovoltaicos	Castelo Branco
Entrevistado 14	F	40	Doutoramento	Especialista Informática\ Tecnologias da Informação	Castelo Branco
Entrevistado 15	M	22	Licenciatura	Estudante\Relações Internacionais	Covilhã/Castelo Branco
Entrevistado 16	F	42	Doutoramento	Professora Universitária\Psicologia	Viseu

Capítulo 4 – Procedimento da Análise e Interpretação dos Resultados

Neste capítulo são analisados e interpretados os resultados das entrevistas numa reflexão baseada no modelo de análise previamente apresentado na Tabela 3. Optou-se por apresentar a análise e interpretação dos resultados em torno de 8 dimensões de análise, atribuindo uma secção para cada uma.

Após a realização e transcrição das entrevistas, procedeu-se a uma seleção dos conteúdos que se consideraram mais relevantes para o estudo. Posteriormente construiu-se uma tabela, utilizando o *software* Microsoft Excel, contendo as dimensões de análise, e respetivos indicadores preenchidos com os testemunhos selecionados dos 16 entrevistados. Optou-se pela utilização deste software devido às vantagens que oferece quando se deseja comparar testemunhos relativos a determinada dimensão de análise, a dimensão das folhas de cálculo do Excel permite a colocação de todos testemunhos numa só tabela (ver Figura 2). Recorrendo a este *software*, pode-se realizar, mais facilmente, uma comparação entre os testemunhos dos entrevistados (seta horizontal), ao mesmo tempo que o seguimento de uma só entrevista (seta vertical) é também facilitado.



	A	B	K	L	M
1			Entrevista 8	Entrevista 9	Entrevista 10
2		1.1 Existência de processos de vigilância	Sim, julgo que sim que estamos ... que sim, que isso acontece. ... por exemplo posso-lhe dar um exemplo prático relativamente quando consultamos na internet alguns sites, algumas... Ou de roupa ou de viagens, ou o que seja, entretanto começam a aparecer depois, as vezes nem nos apercebemos como, publicidades ou no nosso telemóvel, ou de uma outra forma até, agora já não se utiliza correspondência em casa, não é? Mas eu penso que sim, que isso acontece e é possível traçar um perfil dos nossos gostos ou das nossas escolhas.	... , considero que sim, que neste momento existem todas as razões para se pensar dessa forma. ... e a razão para qual eu penso dessa forma é porque eu sou um utilizador normal, usual da internet e sei que alguns dados que são inseridos, e que são do conhecimento geral evidentemente, não tenho nenhuma ideia em particular, mas que são do conhecimento geral.	Sim, tenho a certeza que sim, que são recolhidas informações até principalmente nas redes sociais e coisas assim, porque aparece determinado tipo de publicidade até, que julgam ir de encontro ao encontro da pessoa que está ali a utilizar, portanto faz parte de uma vigilância que existe.
			[Respondido na 1.1]	Estou a falar aqueles que é comum nós ouvirmos, por exemplo a Google é um dos	Sim, alguns sites também quando visitamos, etc. Até não sei se os motores de busca, não sei não

Figura 2 – Exemplo do modelo de análise preenchido com testemunhos por entrevistado

Tendo-se esclarecido o procedimento da análise e interpretação dos resultados, segue a sua apresentação.

4.1 – Consciencialização sobre os Processos de Vigilância

Tiveram-se em conta quatro indicadores de análise: (i) a existência de processos da vigilância; (ii) a identificação de entidades/plataformas vigilantes; (iii) a perceção sobre os objetivos da vigilância e, por último, (iv) a preocupação com os processos de vigilância. Importa realçar que as questões colocadas aos entrevistados, nesta primeira fase, nunca incluíram qualquer tipo de pista ou indicação sobre a existência, os tipos ou os propósitos da vigilância. Também importa realçar que nas três primeiras dimensões de análise, optou-se por seguir a recomendação de Lyon (2018) que implica permitir que os respondentes falem sobre a vigilância nos seus próprios termos. Não se utilizou, propositadamente, termos ligados especificamente a algum tipo de vigilância, nem se mencionou o conceito de privacidade.

Existência de processos de vigilância

Atualmente serão muito raros os casos nos quais os cidadãos não se apercebem dos processos de vigilância eletrónica no mundo Ocidental (Lyon, 2018). No estudo em questão, um número significativo de respondentes, afirmou com grande convicção que a atividade na internet era de alguma forma controlada, independentemente dos seus perfis sociodemográficos ao nível de: escolaridade; conhecimento informático e género.

> "(…) considero que sim, que neste momento existem todas as razões para se pensar dessa forma. Porque eu sou um utilizador normal, usual da internet e sei que alguns dados que são inseridos, e que são do conhecimento geral evidentemente… Não tenho nenhuma ideia em particular, mas que são do conhecimento geral." (E9, masculino, 57 anos, 12º ano, assistente operacional, Covilhã).

> "Sim, tenho a certeza que sim, que são recolhidas informações até principalmente nas redes sociais e coisas assim, porque aparece determinado tipo de publicidade até, que julgam ir de encontro ao encontro da pessoa que está ali a utilizar, portanto faz parte de uma vigilância que existe." (E10, feminino, 52 anos, Doutoramento, Docente no Ensino Secundário, Braga).

O "conhecimento geral" referido pelo E9, ou a reflexão sobre determinados aspetos da navegação na internet, como por exemplo, as publicidades personalizadas, assim como a cobertura mediática dos escândalos relacionados com falhas na proteção de dados pessoais, parecem contribuir para uma maior consciencialização sobre a vigilância.

> "Sim, sinceramente sim, tipo… como aconteceu no Facebook, eles conseguem…eles conseguem entrar nos computadores das pessoas, eles sabem tudo basicamente. (…), é a principal, e é a que a maioria das pessoas utiliza." (E13, masculino, 24 anos, 12º ano, segurança, Covilhã).

Por outro lado, verificou-se que uma participante (E1) tem uma perceção contrastante, a entrevistada acredita que a sua navegação na internet é apenas controlada através de processos de vigilância no seu local de trabalho.

> "A nível de serviço sim, a nível pessoal…acho que não." (E1, feminino, 35 anos, 12º ano, assistente operacional, Açores).

Neste caso a participante não tomou consciência por si própria que era alvo de vigilância, mas por informação fornecida diretamente pelo seu empregador. Tal situação poderá remeter, de acordo com Bloss (2007), Lyon (2009) e Marx (2015), para o facto de o grau de intrusão muito menor, possível nos processos de vigilância atuais, algo que facilita a sua utilização sem que alguns indivíduos se apercebam.

Atendendo ao facto que todos respondentes enfrentam processos de vigilância com graus de intrusão reduzidos, poder-se-á levantar questões em relação à influência de variáveis como o capital cultural na consciencialização sobre a vigilância. A comunicação direta sobre a existência de processos de vigilância, poderá ser uma das únicas formas de alertar e captar a atenção de alguns cidadãos, podendo ser especialmente importante para os cidadãos com capital cultural mais reduzido. Outros tipos de mecanismos, menos diretos, como as notificações de recolha de cookies ou consentimentos informados para a cedência de dados, nem sempre são interpretados espontaneamente, pelos respondentes, como sinais que comprovam a existência da vigilância na internet.

Identificação de entidades/plataformas vigilantes

Os respondentes identificaram várias plataformas vigilantes pertencentes a diversas entidades: plataformas de entidades empregadoras; redes sociais; serviços de e-mail; motores de busca; qualquer site de vendas; portais e serviços públicos.

Relativamente às menções aos motores de busca, serviços de e-mail e às redes sociais, para alguns entrevistados justificação é encontrada no conhecimento sobre a forma como multinacionais como, por exemplo, a Google ou o Facebook recolhem dados pessoais. Também o conhecimento sobre a apelidada economia dos dados contribui para que se identifique algumas entidades vigilantes. Veja-se os seguintes testemunhos:

> "Uma das entidades que o faz é a Google como você deve saber. A Google enquanto motor de busca é uma entidade tão grande a nível mundial, e tão acessível a todos, porque armazena informação no próprio computador de cada pessoa. Ou seja, se guarda informação no computador de cada utilizador da rede, indubitavelmente irá estar a recolher informação desse mesmo utilizador. (…) Qualquer tipo de rede social é usada e monopolizada para outros fins que não aqueles que os utilizadores inicialmente subscreveram." (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

> "(…) um exemplo prático relativamente quando consultamos na internet alguns sites, algumas… Ou de roupa ou de viagens, ou o que seja, entretanto começam a aparecer depois, as vezes nem nos apercebemos como, publicidades ou no nosso telemóvel, ou de uma outra forma até (…)." (E8, feminino, 50 anos, mestrado, técnica superior, Covilhã).

Importa salientar que alguns respondentes que mencionaram as redes sociais, referiram-se principalmente ao Facebook, mencionando apenas recolha de dados que a empresa efetua. No entanto, não mencionaram os aspetos relacionados com a vigilância lateral que as redes sociais potenciam.

Se atentarmos aos tipos de vigilância que as plataformas identificadas praticam, nota-se que grande parte dos entrevistados (E2; E3; E4; E5; E6; E7; E8; E9; E10; E11; E12; E13; E14; E15; E16), apesar da diversidade de perfis sociodemográficos, mencionou espontaneamente uma série de procedimentos ligados a entidades que participam, seja através da venda ou utilização dos dados em proveito próprio, na vigilância comercial. Sendo as entidades ligadas à vigilância no trabalho (E1; E11) e à vigilância governamental (E15) pouco referidas.

Como Augusto e Simões (2017) apontaram nas conclusões do seu estudo, sobre as perceções da vigilância lateral nas redes sociais, alguns tipos de vigilância podem estar mais presentes nas perceções dos cidadãos em comparação com outros. No presente estudo, os cidadãos parecem ser mais sensíveis aos tipos de vigilância que lhes são mais próximos: o tipo de vigilância que mais referiram nas suas respostas foi o comercial. A maior proximidade da vigilância comercial nas perceções dos respondentes, poderá estar associada ao contacto frequente com o marketing baseado na recolha, análise e compra/venda de dados.

Importa realçar que nesta primeira parte das entrevistas, utilizou-se o termo entidades nas questões colocadas aos entrevistados, o que poderá ter dificultado as menções a aspetos da vigilância lateral. Como refere Marx (2015), o próprio termo "vigilância" parece ainda estar mais associado a atividades praticadas por entidades mais poderosas como as grandes empresas, algo que também poderá ter impedido alguns respondentes de refletirem sobre possíveis formas de vigilância que não pressuponham, necessariamente, uma assimetria de poder.

Perceção sobre os objetivos da vigilância

Neste indicador pareceu haver, novamente, uma maior sensibilidade para os aspetos comerciais da vigilância. A maioria dos respondentes, independentemente dos seus perfis sociodemográficos, referiu objetivos relacionados com a vigilância comercial (E4; E5; E7; E8; E9; E10; E11; E12; E14; E15; E16), associando-os a lógicas de marketing e de maximização de lucros por parte das empresas. Os entrevistados E8, E9, E15 e E16 demonstraram algum incómodo e, por vezes, desconfiança em relação a estes objetivos, como está explícito nestes dois testemunhos:

> "(...) alguns dados são de facto utilizados para outros fins que não aqueles que nós estamos a preencher. Nomeadamente quando nos pedem… alguns dados mais pessoais, como a idade, o local onde vivemos e tudo isso, são utilizados para fazer outro tipo de estudos… Muitas vezes nem têm a ver com o carater que estamos de facto a presenciar." (E9, masculino, 57 anos, 12º ano, assistente operacional, Covilhã).

> "Lá está, acho que grande parte dos objetivos passam por ser objetivos de marketing, que por um lado até ajudam, mas por outro, é um grande entrave à privacidade das pessoas." (E15, masculino, 22 anos, licenciatura, mestrando em ciência política, Guarda).

Parece também haver alguma incerteza em relação ao tratamento dos dados. Os sentimentos demonstrados pelos respondentes não são surpreendentes, dada a dificuldade de interpretação das informações prestadas pelas entidades. A própria arquitetura da Web reforça a incerteza sobre o futuro tratamento e utilização dos dados, após a entrada de dados pessoais na Web, aferir a quantidade de vezes que se reproduzem cópias dos dados, rastreá-los ou eliminá-los são tarefas de difícil concretização (Schneier, 2015).

Os três respondentes que associaram os objetivos da vigilância a atividades ilícitas (E1; E2; E13), pareceram relacionar a vigilância ao cibercrime de forma bastante clara, observe-se:

> "Nesse caso de… bancos ou assim poderá ser ter as minhas passwords para conseguir assim aceder à minha conta." (E1, feminino, 35 anos, 12º ano, assistente operacional, Açores).

> "Exatamente, roubar dados. Por exemplo através do Paypal roubar dados bancários". (E2, feminino, 40 anos, 12º ano, escriturária, Açores).

> "(…) para tentar descobrir a vida das pessoas…de alguma forma tentar depois…tentar depois encostá-los à parede para depois tentar extorquir dinheiro ou assim, não faço ideia." (E13, masculino, 24 anos, 12º ano, segurança, Covilhã).

Estes entrevistados têm algumas semelhanças ao nível de sociodemográfico, nenhum frequentou o ensino superior nem trabalha em empregos qualificados, as suas idades variam entre os 22 e os 40 anos. Ao longo da entrevista pareceram ter um conhecimento muito reduzido sobre as práticas da vigilância eletrónica.

Declarações como as citadas acima, sugerem que a vigilância pode ser confundida com o (ciber)crime, especialmente quando os entrevistados têm um conhecimento algo reduzido sobre os procedimentos da vigilância.

Já os entrevistados que mencionaram aspetos de manipulação de massas (E7; E16) revelaram estar cientes da possibilidade, algo distópica nas palavras da E16, de se poder manipular consumos e eleições políticas através da utilização estratégia dos processos de vigilância.

> "Como foi o caso do Donald Trump nas eleições, que utilizaram as redes sociais inclusive o Facebook para monopolizar o pensamento dos Americanos e influenciar o voto." (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

> "(…) divulgação de informação, publicidade, criar aqui necessidades (…), de alguma forma até, em última análise, numa lógica mais distópica, controlar as pessoas, não é?" (E16, feminino, 42 anos, doutoramento, docente universitária, Viseu).

As perceções aparentam resultar de uma reflexão sobre o potencial, mais ao nível estrutural, sobre os objetivos da vigilância. A menção espontânea a aspetos mais estruturais exige uma reflexão informada e aprofundada, que poderá estar intimamente ligada a níveis elevados de consciencialização sobre a vigilância. No entanto, alguns respondentes com níveis elevados de consciencialização da vigilância, por exemplo os que têm formação em informática, não refletiram sobre objetivos com um impacto mais estrutural, referindo apenas e prontamente objetivos relacionados com a venda e publicitação de produtos. Seria pertinente, em futuras investigações, explorar a razão para que tal tenha acontecido.

Apenas uma entrevistada (E8) mencionou objetivos relacionados com a vigilância governamental, nomeadamente ao nível de controlo fiscal. O número reduzido de menções à vigilância governamental pode indicar que este tipo de vigilância é tido como algo distante dos respondentes.

De forma algo contrastante com as outras perspetivas, o E6 não identificou qualquer objetivo específico da vigilância para além da recolha de dados, não emitindo a sua opinião sobre os propósitos da recolha.

A preocupação com os processos de vigilância

De forma geral os respondentes afirmaram preocupar-se com a vigilância de que são alvos. Um número significativo de respondentes abordou questões relacionadas com a sua privacidade (E3; E4; E6; E7; E9; E10; E12; E14; E15; E16), emergiram discursos em que transparece o incómodo pela perda de privacidade de que são alvos em contexto online, e também pelo desconhecimento sobre a sua utilização e tratamento. Os resultados deste indicador vão de acordo ao que Lyon (2015) afirmou: as reações mais comuns, fora do mundo académico, à vigilância são as preocupações com a violação da privacidade.

> "Privacidade da própria pessoa, e a utilização desses dados. Não sabemos onde esses dados vão parar, quem os gere e para que é que podem servir." (E6, masculino, 47 anos, 12º ano, empresário, Lisboa).

> "E, portanto, quando nós naquilo que fazemos estamos a ser, no fundo, vigiados isso acaba por condicionar a nossa…diminuir a nossa privacidade, não é? Isso é preocupante para mim pelo menos, para mim é. Se calhar os mais jovens não ligam muito para isso,

> mas para mim ainda é um valor muito importante." (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

> "É a privacidade…está a ser recolhida muitas vezes… supostamente com o nosso próprio consentimento muitas vezes através dos cookies, dos sites que principalmente, ultimamente, eles simplesmente metem têm que aceitar os cookies, está aqui o eu aceito, está aqui para ver mais, mas resumidamente e muitas vezes quase que impõe que aceitemos os cookies. Mesmo antes de ler, e muitas das vezes isso acontece." (E4, masculino, 25 anos, 10º ano, Empregado de Mesa\bar, Açores).

Por outro lado, em linha com o que tinham referido anteriormente, os entrevistados que afirmaram que os objetivos da vigilância se prendiam com o cibercrime demonstraram a sua preocupação com o mesmo.

> "Eu tenho sempre receio em colocar alguns códigos na internet, com receio que alguém possa utilizar (…)." (E1, feminino, 35 anos, 12º ano, assistente operacional, Açores).

> "Tento prestar atenção nisso, para já quando se clica, quando vem esses emails se a gente põe só o cursor em cima do email já se vê de quem é que é o email." (E2, feminino, 40 anos, 12º ano, escriturária, Açores).

> "Preocupa-me, (…) porque conseguem entrar nos computadores das pessoas e eu conheço pessoas que fazem isso, e epá, é muito mau, é muito mau não haver segurança…os hackers e assim conseguem-te descobrir isso tudo, e isso é mau." (E13, masculino, 24 anos, 12º ano, segurança, Covilhã).

Estes entrevistados, numa primeira fase, pareceram estar preocupados apenas com possíveis consequências diretas que os pudessem afetar, não refletindo sobre possíveis consequências indiretas. De acordo com Lyon (2018), geralmente os cidadãos têm alguma noção da vigilância, porém raramente têm conhecimento sobre as formas como os dados são recolhidos, comparados e utilizados, desconhecendo também os propósitos e consequências do tratamento de dados. Este parece ser o caso de uma boa parte dos entrevistados, sendo que os entrevistados menos informados parecem desconhecer até mesmo as noções mais básicas de como a vigilância funciona.

No entanto, vários respondentes demonstraram estar a par de alguns processos da vigilância que ultrapassam preocupações mais individuais. A preocupação com a manipulação comercial foi algo frequente (E5; E9; E10; E12; E14; E15; E16), denotando-se uma preocupação mais elevada em alguns discursos como o da E5.

> "É uma questão só de vender e comprar produtos, e é só aqueles… ou o que nós vemos… Ou seja, passamos a estar restringidos de tudo o resto que se está a passar, de alguma forma." (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

Contudo, também surgiram discursos de entrevistados (E12; E14), que apesar terem conhecimento das lógicas do *social sorting* por exemplo, mostraram alguma indiferença em relação às tentativas de manipulação comercial.

> "(…) já não é espanto nenhum para mim que isso aconteça, simplesmente se eu vir eu vou…Epá ok está mais barato aqui, deixa ver, vamos ver quando é que…se é um produto que eu realmente quero, é uma forma de eu poder procurar e procurar mais rápido aquilo que eu quero." (E12, masculino, 25 anos, licenciatura, mestrando e investigador em engenharia informática, Santarém).

> "Se eu me preocupo? É assim, eu tenho consciência que a partir do momento em que uso a internet seja para o que for, a toda, estou de certa forma, a colocar os meus dados ou a dar a conhecer às empresas os meus gostos, onde viajo, etc." (E14, feminino, 40 anos, doutoramento em informática, especialista em tecnologias de informação, Covilhã).

Os entrevistados que adotaram estes discursos pareceram ter, além do conhecimento informático proporcionado pelas suas formações\ocupações, um conhecimento elevado sobre a vigilância eletrónica, o que poderá contribuir para uma postura que atua racionalmente para tirar proveito das potenciais vantagens oferecidas pela vigilância, enquanto sabem como evitar os aspetos potencialmente prejudiciais para os próprios. Esta postura informada e racional vai de acordo ao que Turow, Feldman e Meltzer (2005), haviam sugerido na sua investigação em relação às formas como as pessoas mais informadas sobre a vigilância comercial lidam com ela.

Por outro lado, os entrevistados 3 e 4 parecem associar uma preocupação acentuada em relação à vigilância, a um sentimento de paranoia.

> "Epá não naquela base de que já te disse, eu não sou muito paranoico, (…) epá tenho algum cuidado se calhar com câmaras." (E3, masculino, 35 anos, 12º ano + curso técnico (IV) em informática, taxista, Açores).

> "(…) Paranoicas provavelmente, ou têm alguma coisa a esconder (risos) Só se seria alguma coisa muito, muito secreta." (E4, masculino, 25 anos, 10º ano, empregado de mesa\bar, Açores).

A associação da vigilância a sentimentos de paranoia é referida por diversos autores, como Staples (2000) e Giroux (2015), que apontam o sensacionalismo jornalístico como causa para esta associação. Lyon (2019) reconhece que esta associação é algo comum no imaginário das pessoas, enquanto Holm (2009) chama a atenção para a sua utilidade nos estudos da vigilância, o autor já havia notado que ao adotar-se determinados comportamentos relacionados com a vigilância, um individuo pode facilmente ser catalogado como tendo uma fobia patológica e injustificada. Analisando os discursos dos entrevistados percebe-se que, nas suas opiniões, um condicionamento forte da atividade online, por motivos de privacidade, é facilmente associado a paranoia. O discurso do entrevistado 4, contém também elementos de um discurso

amplamente explorado nos estudos da vigilância, o argumento "Não tenho nada a esconder" explorado por Solove (2011), Augusto e Simões (2017) e Simões e Jerónimo (2018) por exemplo. No entanto, este discurso pode gerar diversas interpretações: por um lado a associação de paranoia a uma forte vontade de proteger a privacidade, pode significar que o entrevistado pensa que o contexto atual da vigilância eletrónica não justifica a adoção de medidas tão avançadas para proteger a nossa privacidade; ou por outro lado, o participante poderá ser apologista, por exemplo, de uma sociedade com graus de transparência mais elevados.

4.2 – Cedência de Dados Pessoais

Considerou-se quatro indicadores de análise. Em primeiro lugar, a facilidade no fornecimento de dados pessoais, onde se procurou aferir em que circunstâncias os entrevistados fornecem, ou não, os seus dados pessoais, e também explorar a existência de diferenças em termos das entidades a quem aceitam fornecer os seus dados pessoais, como por exemplo entidades públicas *versus* privadas, e ainda a modalidade do fornecimento dos dados (online vs. offline). Em segundo lugar, a importância do consentimento informado, onde se procurou aprofundar até que ponto os consentimentos informados são importantes para os entrevistados. Em terceiro lugar, a perceção sobre a venda de dados pessoais, para se saber que opinião têm desta venda. E por fim, a possibilidade de *social sorting*, no qual se explora se os respondentes consideram possível efetuar o processo atualmente e também as perceções sobre as suas consequências; e ainda se tentou aferir se o *social sorting* é entendido como sendo potencialmente discriminatório.

Facilidade no fornecimento de dados pessoais

Vários respondentes (E5; E6; E8; E9, E10; E13; E14; E16), referiram só dar os seus dados pessoais em situações nas quais a sua cedência é obrigatória. De entre os discursos que mencionam a obrigatoriedade da cedência encontram-se sinais evidentes de uma aceitação "semiforçada", algo que parece suscitar diversas reações, como por exemplo, o fornecimento de dados falsos para contornar a obrigatoriedade, o evitamento dos websites cuja cedência é obrigatória, e uma cedência relutante.

> "Tal como tinha dito, normalmente não dou. Portanto não existe o fator de eu dar em alguns aspetos e noutros não, eu na internet normalmente eu não dou. E quando de repente me pedem eu normalmente minto, não ponho os dados verdadeiros." (E9, masculino, 57 anos, 12º ano, assistente operacional, Covilhã).

> "Não dou com muita facilidade embora às vezes tenha que dar (risos) Mas, não, não dou com muita facilidade e nunca…quando me ponho em coisas que tenho de aceitar os cookies e não sei quê eu digo logo que não, e prefiro não ver." (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

> "Olhe, eu dou com relutância (…). Mas dou com, ao início até evitava alguns serviços, agora julgo que criei um efeito de tolerância que não é bom, (…) Mas não fico confortável." (E16, feminino, 42 anos, doutoramento, docente universitária, Viseu).

Seguindo o modelo de privacidade, anteriormente apresentado, de Steeves (2009) esta cedência de dados semiforçada, uma vez que a sua recusa impede o acesso a serviços considerados fundamentais pelos respondentes, constitui uma invasão da privacidade devido à mencionada impossibilidade de rejeitar a cedência. A importância do acesso em alguns casos parece sobrepor-se às preocupações que os respondentes têm em relação à cedência de dados, enquanto noutros casos, os respondentes optam por tentar aceder ao conteúdo que desejavam através de uma alternativa que não implique essa cedência.

Porém, também sugiram discursos mais despreocupados em relação à cedência de dados como no caso do E7.

> "Sinceramente eu quase sempre dou os meus dados pessoais, porque não acredito que sejam assim tão relevantes quanto isso. Por isso a mim não me faz grande diferença." (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

No testemunho do E7, o argumento "não sou uma pessoa de interesse" pareceu ser responsável pela atitude despreocupada em relação à cedência de dados.

Relativamente às entidades a quem cedem os dados, uma boa parte dos entrevistados referiu que fornece mais facilmente a entidades públicas do que a privadas (E1; E5 E7; E8; E9, E10; E11; E13; E15). Foi possível identificar noções claras de uma maior responsabilidade das entidades públicas e, também, de uma maior confiança nos propósitos da recolha de dados.

> "A entidades públicas, pelos fins que… confio mais nos fins das entidades públicas e também porque têm mais responsabilização, porque se são públicas estão ligadas de alguma forma ao Estado (…)." (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

> "Públicas, porque há aquele sentido de *accountability* que eu espero que haja no público." (E15, masculino, 22, licenciatura, mestrando em relações internacionais, Guarda).

> "Entidades públicas, porque eles no fundo já têm os nossos dados. Quer tu queiras, quer não os teus dados estão todos no teu cartão de cidadão, por isso invariavelmente eles vão ter acesso aos teus dados. (…) Sim e porque os dados que damos às entidades públicas são por um bem maior, no caso da Saúde, no caso do cartão do cidadão, em qualquer caso é para um bem maior, não é propriamente para monopolizar as pessoas" (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

Os propósitos da recolha de dados parecem, novamente, adquirir uma grande importância na decisão dos respondentes em ceder os seus dados pessoais. Também surgiram discursos que

consideram que o fornecimento de dados a entidades públicas é indiferente, visto que, na opinião de alguns respondentes, as entidades públicas terão acesso aos seus dados de qualquer forma. Esta despreocupação de alguns entrevistados contrasta, de certa forma, com o relatório sobre cibersegurança em Portugal no qual cerca de 73% dos respondentes manifestou preocupações relacionadas com a incapacidade das entidades públicas garantirem a segurança dos seus dados (Comissão Europeia, 2014).

Enquanto que para alguns entrevistados (E2; E6; E12; E14) o tipo de entidade que lhes pede os dados pessoais, seja pública ou privada, é indiferente para a decisão de cedência dos dados pessoais, sendo para eles mais decisivos os contextos em que são solicitados os dados.

> "É-me completamente indiferente, vai depender mais da situação do que se é público ou privado, isso não me vai influenciar em nada." (E12, masculino, 25 anos, licenciatura, mestrando e investigador em engenharia informática, Santarém).

> "(…) eu aqui não faria assim uma grande distinção entre entidades públicas e privadas, é mais, vai mais ao encontro daquilo que eu preciso." (E14, feminino, 40 anos, doutoramento em informática, especialista em tecnologias de informação, Covilhã).

O discurso destes entrevistados parece ir de encontro ao que Marx (2015) afirmou, o autor salientou que os contextos nos quais acontecem processos de vigilância são decisivos na forma como se perceciona e age perante a vigilância. Como referiram Kennedy, Elgesem e Miguel (2015), a adequação dos dados solicitados em relação aos propósitos da sua recolha, também parecem desempenhar um papel importante na cedência de dados dos entrevistados. Há ocasiões, como o acesso a serviços públicos, nas quais os entrevistados compreendem que seja obrigatório o fornecimento de dados pessoais, consequentemente estão mais predispostos a fornecê-los nessas situações. Já nos casos de pedidos de informação que consideram inadequados, os entrevistados demonstram-se mais relutantes.

> "(…) a app da balança inteligente uma pessoa põe-se em cima da balança o que é cómico nessa app (…), é que obriga a ligar o GPS, porquê? Porque é que essa aplicação tem que saber onde é que eu estou para me pesar? É porque em diferentes pontos do mundo será que eu sou mais pesado ou mais leve? (...)." (E3, masculino, 35 anos, 12º ano + curso técnico (IV) em informática, taxista, Açores).

Estas situações são consideradas, por vários autores (Gu et al., 2017), como constituindo uma invasão de privacidade desnecessária. As aplicações incorrem nessas invasões sempre que recolhem informações desnecessárias para a funcionalidade da aplicação. A invasão de privacidade ocorre também, no contexto das aplicações móveis, quando determinada organização utiliza ou transmite os dados para outros propósitos sem que obtenha autorização para o fazer. Esta invasão de privacidade parece ser especialmente incomodativa nos casos em que é detetada pelos entrevistados.

Por último, em relação à modalidade de fornecimento de dados (*Online* vs. *Offline*) um número significativo de entrevistados (E4; E6; E7; E8; E9; E10; E12; E13; E14; E15; E16) disse ser indiferente. A noção de que mesmo os dados que são fornecidos de modo *offline*, serão posteriormente colocados nas bases de dados foi o motivo referido para não existirem diferenças significativas na modalidade de fornecimento.

Por outro lado, quatro respondentes (E1; E2; E3; E11) preocupam-se mais com a cedência online devido a preocupações relacionadas com o tratamento dos seus dados, já que nas suas perceções, os dados online são mais vulneráveis, por exemplo, a acessos ilícitos.

> "(…) online fico um bocadinho desconfiada…fico sempre na dúvida se mais alguém poderá ter acesso aos meus dados e haverá alguma fraude ou assim. Por isso nesse aspeto... mais offline do que online." (E1, feminino, 35 anos, 12º ano, assistente operacional, Açores).

A entrevistada E5 referiu que dava mais facilmente na internet simplesmente porque os pedidos de recolha de dados são muito mais frequentes no contexto online.

Importância do consentimento informado

Os respondentes declaram, unanimemente, que o consentimento informado era fundamental em todos os processos de recolha de dados. Realça-se o facto de uma série de entrevistados (E2; E5; E8; E9; E12; E14; E16) sentir que os consentimentos informados são geralmente pouco transparentes, de difícil leitura e que parecem ser orquestrados para persuadir a sua aceitação. As características que os respondentes atribuíram aos consentimentos informados, parecem estar ligadas à forma sofisticada de persuadir a cedência de dados mencionada por Acquisti, Brandimarte e Loewenstein (2015). Algo que de acordo com o E12, com formação em informática, é claramente intencional para persuadir a aceitação dos consentimentos.

> "(…) acho que se por exemplo em determinadas aplicações tinha que se ter a noção ou sermos avisados… de que estavam a utilizar os nossos dados para benefício próprio." (E2, feminino, 40 anos, 12º ano, escriturária, Açores).

> "Que revejam a forma como nos informam do que é que está a ser pedido e como é que isso vai ser usado, que normalmente (…) é um conjunto de informações que ninguém lê é impossível ler aquilo até ao fim, e eu acho que isso é intencional." (E16, feminino, 42 anos, doutoramento, docente universitária, Viseu).

> "(…) é escrito de uma forma muito extensa, muito complexa e para a qual as pessoas não têm tempo. Nós por exemplo quando vamos a criar uma página web, algo que eu aprendi na minha licenciatura, é que as pessoas estão dispostas, para chegar ao seu objetivo, estão dispostas apenas a dar três cliques, (…) se uma pessoa só quer dar três cliques para chegar ao objetivo, porque é que uma pessoa que está naquele site e quer ser rápido a encontrar uma coisa, se vai dar ao trabalho de estar a ler algo tão extenso,

> ninguém o faz porque não está dentro, não se enquadra nos conselhos, nas normas de utilização da internet." (E12, masculino, 25 anos, licenciatura, mestrando e investigador em engenharia informática, Santarém).

Os resultados aqui apresentados, podem levantar questões sobre a forma como os consentimentos informados devem ser colocados aos cidadãos. A obrigatoriedade do pedido de consentimento informado, resultou numa reação sofisticada por parte das entidades que recolhem os dados. Através das referidas estratégias, as entidades que recolhem os dados, acabam por obter frequentemente "consentimentos informados" que não são verdadeiramente informados, parecem surgir mais como cliques motivados pela conveniência. Vários respondentes referiram nunca ter lido os consentimentos informados, referindo que simplesmente clicavam no "aceito" ou na cruz da caixa de diálogo, para que o aviso parasse de os incomodar.

Perceção sobre a venda de dados

Diversos respondentes (E6; E7; E8; E9; E10; E11; E12; E14; E16) tem uma opinião negativa sobre a venda de dados pessoais. De entre estes respondentes, no geral, surgem discursos de desconfiança e/ou desconhecimento dos fins da recolha de dados, tal como novas menções à aceitação de consentimentos informados, apesar de não terem sido lidos.

> "Não, não acho que seja correto. Até porque maior parte dos utilizadores nem sabe disso porque isso faz parte daquelas letrinhas pequeninas dos termos e condições" (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

> "Ai, acho horrível isso (risos) Acho muito mal, porque eu… é vendida e depois a questão é o para quê?" (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

Apesar das recorrentes notícias relacionadas com a venda de dados, três entrevistados (E1; E5; E13) desconhecem que esta exista.

> "Por acaso confesso que nunca pensei nisso. Que era através daí…que eles… poderiam estar a angariar algum dinheiro." (E1, feminino, 35 anos, 12º ano, assistente operacional, Açores).

> "Eu não sei se isso é verdade. Se isso for verdade, não tenho uma opinião muito positiva sobre isso (…)". (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

O desconhecimento da prática de venda de dados pessoais poderá estar relacionado com o processo que Marx (2015) denominou de amolecimento\suavização da vigilância, onde os processos de vigilância atuam com menor visibilidade e aparentam ser menos invasivos, dificultando a tomada de conhecimento de alguns procedimentos da vigilância, neste caso

relacionadas com a vigilância comercial. As habilitações literárias de um nível mais baixo destes respondentes (E1; E13), poderão ser uma das causas para o desconhecimento demonstrado.

Em relação à E5, a linguagem utilizada nos consentimentos informados parece ter dificultado a sua interpretação, a própria participante afirmou que nos consentimentos não constava nada sobre a venda de dados.

Possibilidade de *Social Sorting*

Todos respondentes acreditam ser possível realizar processos de *social sorting*, relativamente às consequências que advêm do *social sorting*, os entrevistados dividem-se entre os que reconhecem que as consequências podem ter aspetos positivos e negativos, e os que apenas consideram os aspetos negativos.

De entre os respondentes que reconhecem aspetos positivos e negativos (E4; E5; E6; E7; E8; E10; E12; E15; E16), foram considerados positivos aspetos que permitam incrementos na conveniência da navegação\compra, tal como a possibilidade de se receber benefícios comerciais personalizados. Enquanto os aspetos negativos prendem-se, fundamentalmente, com a incerteza sobre a forma como os dados seriam preservados e tratados, tal como alguns aspetos relacionados com a privacidade e manipulação comercial.

> "Se calhar dá-te mais oportunidades por um lado porque te vai direcionar para coisas que estás mais interessado… (…) Mas é negativo porque tu tens uma série de dados expostos e não sabes de que forma é que estão salvaguardados." (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

> "(…) quando olhamos à partida achamos que é benéfico, ganhar um desconto para uma coisa que eu normalmente utilizo, mas às vezes não refletimos, (…) será que aquilo leva a que eu consuma mais do que seria necessário? (...). Eu acho que, de facto tem esse aspeto negativo." (E8, feminino, 50 anos, mestrado, técnica superior, Covilhã).

Relativamente aos entrevistados que apenas consideraram aspetos negativos (E9; E11; E13; E14), foram mencionados os mesmos aspetos negativos referidos anteriormente, sendo que uma entrevistada se mostrou especialmente preocupada com a sua vulnerabilidade perante os impulsos consumistas que diversas entidades comerciais exploram.

4.3 – Mecanismos de Recolha

A análise desta dimensão baseou-se em dois indicadores: (i) a identificação dos mecanismos de recolha de dados, e (ii) o conhecimento e opinião sobre a forma como estes mecanismos funcionam.

Identificação dos mecanismos de recolha de dados

A ideia de que a internet é um espaço onde, através de diversos mecanismos, podem ser recolhidos dados, foi a que mais surgiu nas respostas dos entrevistados (E3; E4; E7; E9; E10; E11; E12; E14; E15; E16).

> "Tudo, a partir do momento que fazes um clique na Internet tudo dá para recolher dados." (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

> "(…) todos os sites que te pedem autorização é por causa disso, é poder recolher os dados e tudo o que fazes os cookies e tudo para depois ao vender ou analisar para os seus próprios fins (…)." (E3, masculino, 35 anos, 12º ano + curso técnico (IV) em informática, taxista, Açores).

Contudo, dois entrevistados (E2; E13) apenas referiram mecanismos que podem ser utilizados em relação ao cibercrime, não mencionando qualquer mecanismo de recolha de dados ligado à vigilância eletrónica. A perceção de que a internet é um espaço perigoso e suscetível a atividade de cibercrime pareceu preocupar alguns entrevistados ao longo das entrevistas, especialmente os com menor conhecimento sobre as lógicas da vigilância.

Os mecanismos, especificamente identificados pelos entrevistados foram: recolha de cookies; armazenamento das pesquisas efetuadas em motores de busca; formulários de inscrição em websites de vendas; utilização não consentida de câmaras e microfones em aparelhos privados e, por último, as plataformas das redes sociais.

De forma geral, a maioria dos entrevistados parece ter noção dos principais mecanismos de recolha de dados online. Poder-se-á relacionar a obrigatoriedade de todos os websites apresentarem uma notificação a pedir o consentimento informado, com um grau acrescido de consciencialização para a existência dos mecanismos de recolha, apesar da maioria dos entrevistados, ter mencionado que nunca leem a totalidade de um consentimento informado. As lógicas sofisticadas que as entidades vigilantes podem utilizar para recolher dados, mencionadas por Acquisti, Brandimarte e Loewenstein (2015), tal como a suavização da vigilância referida por Marx (2015), são porventura, desafiadas pela obrigatoriedade de apresentação de um consentimento informado aos utilizadores da internet imposta pelo recente Regulamento Geral de Proteção de Dados de 25 de maio de 2018, que se aplica a toda União Europeia. Também outras situações de vigilância subtil e não consentida, vão sendo denunciadas através da comunicação social, como por exemplo a utilização não consentida de microfones e câmaras nos aparelhos privados dos cidadãos. Os entrevistados referiram ter ouvido notícias que relatavam a sua utilização. A comunicação social parece ter um impacto relevante em relação ao conhecimento sobre os mecanismos de recolha informação.

Conhecimento e opinião sobre a forma os mecanismos funcionam

Quanto ao modo como os mecanismos funcionam, a maioria dos entrevistados referiram que a base para o seu funcionamento era o histórico de pesquisas\compras (E5; E6; E7; E10; E13; E14; E15; E16). A forma de atuar dos algoritmos de preferência, foi considerada fácil de detetar devido à presença de sugestões claramente ligadas ao histórico de pesquisa\compra dos entrevistados.

> "Por exemplo, já aconteceu a todos, estarmos no Facebook e de repente aparecer-nos um anúncio de sofás, como nós estamos à procura de um sofá, que coincidência! (risos)." (E15, masculino, 22, licenciatura, mestrando em relações internacionais, Guarda).

> "(…) quando se põe lá o que é que queremos ver aparecem logo lá uns quantos também sobre o mesmo, ou que tenho a ver, tenham afinidade com…Por exemplo, estar a ver uma coisa de roupa, se eu vou ver de um determinado tipo de roupa, aparece-me algumas sugestões de tipos de roupa parecidos e tal, e portanto, isso é vigilância." (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

Apenas uma participante (E11) referiu não ter qualquer pista sobre o funcionamento dos mecanismos.

Alguns entrevistados manifestaram a sua opinião sobre os algoritmos, sendo que cinco entrevistados consideraram que têm aspetos positivos e negativos (E5; E7; E14; E15; 16). Estes entrevistados referiam que as recomendações os direcionavam de forma conveniente para os seus interesses, mas que, podiam de certa forma, limitar as suas capacidades de escolha. Relativamente aos que reconheceram apenas aspetos negativos (E10; E13), estes afirmaram que para o marketing empresarial era positivo, no entanto, para eles próprios era prejudicial porque viam a sua atividade registada em arquivos duradouros.

Os resultados apresentados neste indicador parecem estar relacionados com um aspeto referido por Lyon (2006), o autor referiu que a monitorização online pode ser benéfica, mas que apenas alguns utilizadores conseguem reconhecer e aproveitar os benefícios oferecidos por ela.

4.4 - Vigilância Lateral

Teve-se em conta 3 indicadores: (i) a exposição voluntária nas redes sociais; (ii) a tendência voyeurística nas redes sociais; e por último (iii) os condicionamentos no comportamento. Os elementos narcisísticos e voyeurísticos das redes sociais, são importantes para se analisar a vigilância lateral, uma vez que o desejo de exposição e de descoberta podem contribuir para uma legitimação e naturalização da vigilância (Lyon, 2018). Relativamente ao terceiro indicador, procurou ver-se até que ponto os comportamentos dos respondentes estão (ou não) condicionados pela perceção de que são sujeitos à vigilância lateral.

Exposição voluntária nas redes sociais

Grande parte dos respondentes (E1; E2; E3; E4; E5; E8; E9; E10; E11; E13; E14; E15; E16) consideram que as pessoas, no geral, expõem-se demasiado das suas vidas nas redes sociais, sendo que alguns manifestaram alguma preocupação com as consequências que a exposição nas redes sociais pode ter ao nível do crime. Os vários comunicados emitidos pelas autoridades portuguesas, nomeadamente a Polícia de Segurança Pública, sobre a precaução que se deve ter nas redes sociais foram mencionados por alguns respondentes. Outros respondentes abstiveram-se de emitir qualquer tipo de julgamento (E6; E12), afirmando simplesmente que cada individuo deve pensar de forma autónoma e agir de acordo com o seu pensamento. Alguns respondentes transmitiram a ideia de que apenas publicam coisas impessoais nas redes sociais (E2; E3; E7; E8; E12; E14), como publicações de algum vídeo que consideram interessante, ou para divulgar alguma ideia ou evento, parecendo utilizar uma estratégia de seleção de conteúdo nas publicações que partilha, para se proteger da vigilância lateral.

É possível identificar alguns aspetos de legitimação e naturalização da exposição voluntária nas redes sociais, tal como Lyon (2018) haveria sugerido, em declarações como as seguintes:

> "(…) percebe-se quando publicam alguma coisa mais importante, um pouco mais digamos pública por exemplo um anúncio, alguma coisa por exemplo um casamento, se uma pessoa se casa quer anunciar ao mundo, é normal querer publicar para as outras pessoas (…)." (E4, masculino, 25 anos, 10º ano, empregado de mesa\bar, Açores).

> "É assim, é positivo…mais ou menos, é moda, é moda. (…) Se for, em termos da sociedade, agora toda gente faz isso, vai comer à noite e tira uma fotografia, foi de viagem e tira uma fotografia e diz onde é que está (…)." (E13, masculino, 24 anos, 12º ano, segurança, Covilhã).

No entanto, de forma geral, parece haver uma noção de que uma exposição voluntária e não cuidada nas redes sociais, pode prejudicar os entrevistados.

Quanto aos aspetos positivos e negativos, uma boa parte dos respondentes considerou a existência de ambos (E1; E2; E3; E4; E5; E7; E10; E13; E14; E15). Como aspetos positivos os entrevistados referiram formas de promover um maior contacto entre cidadãos e/ou de possibilitar reencontros virtuais. Por outro lado, alguns entrevistados afirmaram que os aspetos eram maioritariamente negativos (E1; E2; E3; E10; E13; E14) devido à vulnerabilidade, tanto ao nível de privacidade como ao nível do crime, que pode advir da exposição. Fuchs (2010) concluiu que uma atitude crítica em relação às redes sociais pode ser ativada através da discussão pública, a série de notícias que têm surgido nos jornais nacionais e internacionais, sobre a falta de proteção de dados oferecida pelo Facebook e as suas possíveis consequências, tal como o grau cada vez maior de conhecimento sobre a plataforma, podem estar a aumentar a atitude crítica dos portugueses em relação às redes sociais, sendo o Facebook o principal visado das críticas. Também os comunicados, acima referidos, que as autoridades portuguesas

como a Polícia de Segurança Pública têm vindo a realizar podem contribuir para a formação desta atitude crítica nos entrevistados.

Tendência Voyeurística nas redes sociais

Vários entrevistados (E2; E5; E8; E10; E12; E13; E15) salientaram a importância que as redes sociais podem ter para se manter em contacto ou em estar informado das novidades dos seus contactos nas redes sociais.

> "(…) nas redes sociais eu tenho pessoas que são… Eu não tenho pessoas que não conheço e, portanto, tenho pessoas que de alguma forma estão relacionadas com algum dos meus interesses e eu quero estar atualizada sobre isso." (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

Segundo Andrejeikavic (2005), a utilização das redes sociais para este efeito é semelhante ao escrutínio, entre amigos e conhecidos, podendo corresponder frequentemente a interesses voyeurísticos direcionados à família, amigos e conhecidos. Através de uma análise do discurso de alguns entrevistados as redes sociais são, pouco surpreendentemente, o meio de eleição para exercer vigilância lateral e satisfazer as suas curiosidades sobre a vida pessoal dos seus contactos nas redes sociais.

Por outro lado, alguns entrevistados referiram que as potencialidades voyeurísticas oferecidas pelas redes sociais são aborrecidas ou pouco interessantes (E6; E7; E14).

> "Para mim já é aborrecido, já utilizo as redes sociais porque… olha até por uma questão de trabalho porque é um meio de chegar com facilidade às pessoas." (E6, masculino, 47 anos, 12º ano, empresário, Lisboa).

> "É assim, eu tenho vários amigos e se eles têm alguma coisa importante para me dizer, telefonam-me e dizem-me, ou falam comigo pessoalmente, acho que é a melhor forma." (E14, feminino, 40 anos, doutoramento em informática, especialista em tecnologias de informação, Covilhã).

No discurso de alguns entrevistados foi possível notar alguma saturação das referidas potencialidades das redes sociais. A opinião que seguir a vida de outros cidadãos, através do que publicam nas redes sociais, não é a forma mais adequada de manter o contacto com os seus amigos está, também, claramente presente nos discursos de alguns entrevistados.

Condicionamentos no comportamento

Relativamente a algum tipo de condicionamento nas redes sociais, os respondentes dividem-se entre os que se sentem condicionados (E4; E5; E6; E7; E8; E12; E15), e os que não se sentem condicionados (E1; E10; E13; E14). Os primeiros sentem-se condicionados devido a diversos motivos: alguns preocupam-se com a possibilidade de muitas pessoas poderem escrutinar o que publicam; outros por expor a sua vida e a de outros nas redes sociais; e por último, dois

entrevistados, evitam fazer determinadas publicações porque se preocupam com a possível descontextualização das mesmas.

> "Sim, ultimamente quase sempre penso duas vezes porque depois isso vai aparecer no *feed* das outras pessoas, toda gente sabe o que eu gosto e o que não gosto." (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

> "Basta que haja uma publicação que eu ache muito engraçada, mas que de certa forma, pode criar ali alguma suscetibilidade relativamente a outras pessoas, por exemplo, às vezes uma piada que até envolva…desigualdade de género por exemplo, há piadas que acabam por nunca deixar de ter piada, mas nós não vamos partilhar porque simplesmente não queremos ficar numa má posição." (E12, masculino, 25 anos, licenciatura, mestrando e investigador em engenharia informática, Santarém).

Por outro lado, os que não se sentem condicionados não consideram que a seleção dos conteúdos que escolhem publicar seja condicionada por fatores externos, argumentam que publicam o que desejam.

> "Não, quando tenho mesmo vontade partilho. Quando não tenho, não partilho." (E14, feminino, 40 anos, doutoramento em informática, especialista em tecnologias de informação, Covilhã).

> "Não, é mais uma coisa minha. Eu é que quero publicar (…) Por exemplo, normalmente o que eu publico é alguma foto minha porque estou num sítio qualquer, que eu tive num sítio qualquer. É espontâneo, se calhar não tem uma razão mesmo de ser (risos)" (E1, feminino, 35 anos, 12º ano, assistente operacional, Açores).

Importa referir que alguns entrevistados não se manifestaram sobre este indicador por não serem utilizadores de redes sociais (E9; E11; E16).

4.5 – Vigilância Governamental

Nesta dimensão de análise considerou-se 3 indicadores. Em primeiro lugar, a identificação da informação recolhida por agências governamentais, onde se procurou perceber que tipo de dados os entrevistados acreditam que estão a ser recolhidos por entidades governamentais. Em segundo lugar, os propósitos e aceitação, onde se pretendeu perceber até que ponto os cidadãos consentem e aprovam a vigilância governamental em Portugal; em terceiro lugar a perceção sobre a classificação e categorização dos cidadãos, onde se recolheram perceções sobre as consequências que o processo de *social sorting* poderá ter se for utilizado por entidades governamentais. Por último, o desencadeamento ou aprofundamento de desigualdades sociais onde se pretende captar as perceções sobre as potencialidades da vigilância governamental poderem contribuir para um desencadeamento ou aprofundamento de desigualdades sociais.

Identificação da informação recolhida por agências governamentais

Alguns dos entrevistados (E1; E5; E13) desconhecem que sejam recolhidas informações por entidades governamentais.

> "Eu não sabia, mas informação de…como assim? (…) Mas isso está comprovado?" (E13, masculino, 24 anos, 12º ano, segurança, Covilhã).

> "(…) mas não faço ideia que tipo de informações é que os governos acham oportuno recolher, isto no caso português." (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

Curiosamente, estes entrevistados, que desconheciam a vigilância governamental, coincidem com os que não estavam a par das práticas de venda de dados pessoais *online*. Seria importante, em futuras investigações, testar a existência de uma relação entre os níveis de consciencialização sobre a vigilância comercial e governamental, sendo que os cidadãos com níveis mais elevados consciencialização da vigilância comercial aparentam ter uma maior consciencialização da vigilância governamental.

A consciencialização da vigilância comercial aparenta ser mais facilmente obtida do que a governamental. Todos os entrevistados, independentemente do perfil sociodemográfico, parecem estar cientes de pelo menos algumas práticas da vigilância comercial. Porém, no que respeita à vigilância governamental, vários entrevistados declararam assertivamente que desconheciam por completo que tipo de dados é que as entidades governamentais podem recolher.

Outros entrevistados (E3; E4; E6; E7; E10; E12; E15; E16), mais informados sobre a vigilância governamental, referiram que as entidades governamentais recolhem dados pessoais principalmente através da navegação da internet e dos dados obtidos através dos serviços governamentais.

> "Como eu já tinha dito, o tipo de sites que uma pessoa recorre, e que atualmente recorre e que impacto é que aquela pessoa pode ter para a sociedade e o quão mau aquele site é. Isso nota-se atualmente perfeitamente na procura dentro da própria Europa por extremistas Islâmicos, que são muitas vezes reconhecidos por se reparar que visitam várias vezes os sites da Jihad." (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

> "Eu acho…há a questão policial, não é? Que há aqueles sites, e palavras, palavras que se põem, por exemplo, nos motores de busca, não é? Isso automaticamente que fazem…, eu estou a dizer isto na brincadeira, que fazem soar campainhas e a pessoa fica automaticamente pelo menos vigiada durante algum tempo." (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

A capacidade para identificar, com alguma precisão, o tipo de informação que possa interessar às entidades governamentais, poderá estar ligada a níveis elevados de conhecimento acerca da

vigilância eletrónica no geral. Uma vez que o conhecimento sobre este tipo de vigilância é mais difícil de obter quando comparado a outros.

Parte dos entrevistados (E8; E11; E14), referiu apenas informações recolhidas através dos serviços públicos que podem servir de suporte à governação, desconhecendo outros tipos de recolha que possam existir a nível governamental.

> "(…) quando o meu filho também foi para a faculdade (...) para metermos os papéis para ele ter direito a bolsa, eu não fazia ideia, (...) preenchermos a documentação toda, e eu cheguei a dizer ao ponto de dizer, que daqui a pouco só falta dizermos quantas vezes nós temos que utilizar o banheiro e ir à casa de banho, porque eles querem saber tudo da nossa vida e mais um pouco, para termos uma bolsa para o nosso filho, portanto, isto é, por isso é que eu digo, agora com essa pergunta que me está a fazer, eu acredito que eles vão vasculhar tudo bem "vasculhadinho" da nossa vida, eles devem saber mais da nossa vida do que a gente pensa, e hoje da forma como sabemos que está tudo ligado, em termos de banca, em termos de finanças, em termos de Segurança Social, pronto destes meios todos, portanto, há uma ligação entre todos eles (...)." (E11, feminino, 55 anos, 12º ano, assistente de contacto, Porto).

> "Eu essa questão tenho um bocadinho de dificuldade em responder, porque não sei exatamente que tipo de informação é que o Governo recolhe sobre as pessoas, eles têm toda a informação que querem sobre as pessoas, por exemplo, a parte da Segurança Social, das finanças, etc. Agora a partir da utilização da internet, não lhe sei responder a essa questão." (E14, feminino, 40 anos, doutoramento em informática, especialista em tecnologias de informação, Covilhã).

A recolha de informação através dos serviços públicos, no âmbito da vigilância governamental, aparenta ser a recolha mais facilmente identificada pelos entrevistados. O facto de os pedidos serem frequentemente diretos e obrigatórios, para que o cidadão aceda a algum serviço ou apoio social governamental, contribui para que assim o seja. Já as informações que são recolhidas em contexto online parecem ser mais difíceis de identificar, provavelmente devido às lógicas mais subtis aplicadas nesse tipo de recolha de informação.

Curiosamente, um dos entrevistados, quando questionado sobre a vigilância governamental em Portugal, deu a entender que, na sua opinião, esta não existe; uma vez que perceciona Portugal como sendo um país atrasado a nível tecnológico.

> "Não, eu até certa forma (suspiro profundo) a minha opinião é que Portugal é um país atrasado para caraças a nível de tecnologias, isso é a minha opinião pessoal. Não quer dizer que alguma instituição governamental não possa já ter tecnologias assim, mas parar ser sincero eu desconfio (risos) que não (risos)." (E3, masculino, 35 anos, 12º ano + curso técnico (IV) em informática, taxista, Açores).

A diversidade de respostas em relação à recolha de dados pessoais, por parte de entidades governamentais portuguesas, parece ser influenciada pela perceção de que Portugal não é um país que necessite de investir muito em processos de vigilância governamental, ou então, no caso do E3, que refere que Portugal simplesmente não dispõe das tecnologias necessárias para instituir uma vigilância governamental abrangente. O facto de não ter ocorrido, recentemente, nenhum caso grave e conhecido relacionado com a falta de proteção de dados pessoais por parte das entidades governamentais portuguesas, pode contribuir para que não exista uma reflexão aprofundada, por parte dos entrevistados, sobre os processos de vigilância governamental em prática no território português. Até no meio académico, como referiu Schneier (2015), analisar a profundidade e a capacidade da vigilância governamental é algo extremamente difícil, devido à possibilidade de determinados serviços secretos poderem quebrar as leis dos seus próprios Estados.

Propósitos e aceitação

Alguns respondentes (E1; E2; E7) aceitam e apreciam a existência da vigilância governamental, mencionando os seus contributos para a detenção de crimes e para o incremento da segurança.

> "Porque eu não tenho más intenções, mas isso é bom. Para quem tem más intenções isso é bom monitorizar porque com tanto terrorismo que anda por aí, se calhar até é uma boa hipótese de deter muitas coisas." (E2, feminino, 40 anos, 12º ano, escriturária, Açores).

> "Eu não me importo que vejam as minhas informações pessoais, desde que não tenha uma bomba à porta de casa se é que percebe o que estou a dizer, por causa dos extremistas islâmicos" (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

De entre os discursos de aceitação, foi também possível identificar um argumento frequentemente presente nas perceções dos cidadãos – o "não tenho nada a esconder" já mencionados por Solove (2011) e Augusto e Simões (2017). Aliado ao referido argumento, vem geralmente a perceção de uma troca de privacidade por segurança que, apesar de ser considerada por diversos autores como tendenciosa (Chandler, 2009) ou falaciosa (Pavone e Esposti, 2010), continua presente nas perceções de alguns cidadãos. Apesar desta troca ser mais frequente em contextos de insegurança pública, algo que nos últimos anos não decorreu em Portugal, alguns respondentes manifestaram claramente a disponibilidade para ceder e sacrificar direitos e liberdades em troca de incrementos de segurança. Nos imaginários da vigilância destes respondentes, talvez estejam presentes os mediáticos ataques terroristas que ocorreram na Europa nos últimos anos. As referidas tentativas para a criação do mito da vigilância (Marx, 2015), apesar da relação entre maiores níveis de segurança e um maior número de dispositivos de vigilância ainda não ter sido comprovada cientificamente (Marx, 2015; Hong, 2017), também parecem ter surtido efeito no caso de alguns respondentes.

De uma forma geral, a vigilância governamental, através dos serviços públicos, parece estar naturalizada e legitimada na perceção de alguns respondentes.

> "(…) Podem por exemplo, e isso também seria desejável era fazer um cruzamento, imagine, por exemplo relativamente à declaração de rendimentos que eu apresento, não é? Os meus vencimentos do meu trabalho, e de outras que pudesse ter. Face às despesas que eu tenho, pode haver ali um encontro que de facto eu estou a gastar mais do que aquilo que tenho é porque tenho uma fonte de rendimento que não está declarado." (E8, feminino, 50 anos, mestrado, técnica superior, Covilhã).

> "Os governos será mais a nível fiscal, a nível de números, quantias gastas por cada pessoa, talvez os locais onde essa pessoa esteve, é tudo um pouco suscetível que…lá está, mais uma vez como eu disse à bocado, o nosso NIF serve para tudo, e se nós estamos a dar o nosso NIF tanto à empresa como ao Governo, portanto o Governo sabe onde é que nós estivemos, sabe o que é que fizemos, agora se isso é bom ou mau? Será indiferente neste momento, já todo o ser humano tem uma pegada digital imensa, e já toda gente tem imensas informações sobre nós, não é por aí que vamos perder alguma coisa." (E12, masculino, 25 anos, licenciatura, mestrando e investigador em engenharia informática, Santarém).

O exemplo da aceitação, sem grandes questionamentos, à recente implementação do e-Fatura em Portugal, pode indicar, de certa forma, que não existe uma grande preocupação com novos mecanismos de recolha de dados no âmbito da vigilância governamental, mesmo quando a recolha é explícita e pode colocar em causa a privacidade dos cidadãos portugueses.

Porém, quando questionados sobre uma vigilância governamental na internet, semelhante à que Snowden expôs, a maioria dos respondentes manifestou uma aceitação relutante (E3; E4; E6; E7; E9; E10; E13; E15; E16). Dos seus discursos transpareceu a crença de que os processos de vigilância podem ajudar na deteção de diversas atividades ilícitas. No entanto, os respondentes sentem que os processos devem ser bem regulamentados e que se deve evitar uma invasão desnecessária da privacidade dos cidadãos.

> "(…) através dessa situação pode-se corrigir muitas fraudes fiscais por exemplo, que era o caso, e outros crimes até! Mas o problema está, até que ponto é que vai a invasão da vida pessoal para que isso aconteça?" (E14, feminino, 40 anos, doutoramento em informática, especialista em tecnologias de informação, Covilhã).

> "(…) mais uma vez eu acho que tudo bem temos aqui as questões do terrorismo, por exemplo, ou de grupos organizados em termos criminais, mas o que eu acho é que tem de haver limites, não pode ser a qualquer custo." (E16, feminino, 42 anos, doutoramento, docente universitária, Viseu).

As perceções sobre os propósitos e aceitação da vigilância governamental parecem ser significativamente influenciadas consoante o contexto específico em que os processos de

vigilância decorrem. A aceitação mais relutante da vigilância governamental na navegação *online*, parece estar relacionada com a perceção de que esta é mais invasiva e menos transparente do que a recolha mais direta de dados em serviços públicos. Enquanto na recolha de dados em serviços públicos o cidadão tem perfeita noção dos dados que está a ceder e as razões pelas quais lhes estão a ser requeridos esses dados, na internet a questão torna-se muito menos clara. Vários cidadãos não estão cientes que a sua atividade na internet pode colocá-los em listas de "pessoas de interesse" e, até mesmo os cidadãos que estão a par deste tipo de vigilância, não conhecem exatamente a forma esta ocorre nem que limites à invasão de privacidade existem. O desconhecimento, ou falta de transparência, da vigilância governamental na internet parece ser um dos fatores que mais dificulta a sua aceitação por parte de vários respondentes.

Perceção sobre a classificação e categorização dos cidadãos

Diversos respondentes consideraram que a utilização dos processos de *social sorting* na vigilância governamental é negativa (E1; E6; E7; E8; E11; E12; E13; E15; 16). Alguns respondentes basearam a sua opinião nas possíveis consequências que um processo de categorização poderá ter a nível de discriminação, manipulação da opinião pública, ou de invasão de privacidade.

> "Porque no fundo isso foi o que o Governo nazi fez, catalogou as pessoas, os homossexuais, os judeus, os de raça ariana, os indeterminados, catalogou as pessoas. É algo que sempre que se faz uma catalogação, pode ter problemas graves para o futuro" (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

> "Porque é assim, lá está, aí é o que eu digo, estão a mexer com a nossa vida privada, com a nossa vida particular, e de certa forma a rotular-nos daquilo que realmente nós somos, e eu acho que isso é, eu acho que não, acho que isso para mim…Não concordo, não concordo porque acho que até nós próprios é que temos de saber da nossa vida, e nós é que temos de a controlar e saber levar e saber geri-la, não precisamos que outros, seja neste caso, o Governo que nos venham eles a controlar e a rotular-nos a nossa, o estereótipo de vida (…). (E11, feminino, 55 anos, 12º ano, assistente de contacto, Porto).

A classificação de cidadãos parece evocar momentos na História com consequências aterrorizadoras, algo que pode explicar a perceção negativa sobre o *social sorting* governamental. Noutros casos, parece haver um certo incómodo baseado numa imposição de rótulos e desrespeito pela privacidade e liberdade dos respondentes.

Outros respondentes consideraram que existem aspetos positivos e negativos (E5; E6; E9; E10) no *social sorting*, reconhecendo que o tipo de informação que os processos de *social sorting* fornecem aos governos poderá auxiliar na melhoria da governação. No entanto, preocupam-se

com os impactos que essa informação poderá ter nas suas vidas, referindo que as categorias poderão ser manipuladas pelos governos em benefício próprio.

> "Se for com o objetivo de ajudar, de criar mecanismos de defesa, de segurança, de bem-estar para as pessoas acho que sim, que o devem fazer. Agora como tudo na vida (...), acho que nós não somos inocentes naquilo que fazemos, e o próprio Estado também (…) não o será (…)." (E9, masculino, 57 anos, 12º ano, assistente operacional, Covilhã).

> "(…) isso pode ser trabalhado desde que, claro, essas informações terão sempre de ser sigilosas, mas poderá ser trabalhado para melhorar a vida das pessoas. (...). Agora eu não tenho a certeza é se essas informações de facto, são utilizadas para isso." (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

A desconfiança sobre uma utilização correta destes processos e que beneficie os cidadãos pode ser explicada por níveis menos elevados de confiança social depositada nos governos (Jansson, 2012). Só um participante (E7) considerou que, em Portugal, os processos de *social sorting* teriam apenas aspetos positivos. Para o referido respondente, a confiança no Estado Português assim como a proteção que a União Europeia garante aos seus cidadãos, reduzem a sua preocupação.

> "Acho que Portugal não, Portugal sempre foi historicamente um país pacífico onde se defende a liberdade e é compreensivo. Acho que isso não se aplicaria a Portugal, mas podia-se aplicar a outras nações." (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

> "É algo que as pessoas se devem preocupar, mas felizmente temos uma União Europeia que nos protege, da, dessa parte da utilização dos dados. A única entidade mundial que está a fazer, está a fazer mais alguma coisa em relação a isso." (E7).

Como Jansson (2012) argumentou, os níveis de confiança social influenciam a perceção dos cidadãos sobre a vigilância governamental. Diversos respondentes mostraram-se algo desconfiados em relação aos governos portugueses, algo que poderá explicar a perceção, na generalidade, negativa por parte dos respondentes em relação ao *social sorting* governamental.

Desencadeamento ou aprofundamento das desigualdades sociais

Uma boa parte dos respondentes considerou que o *social sorting* poderia resultar num aprofundamento ou desencadeamento das desigualdades sociais (E1; E4; E5; E6; E7; E8: E9; E10; E11; E13; E15; E16). Os discursos variam entre os que denunciam lógicas de reprodução de desigualdades socioeconómicas, possíveis discriminações com base na etnia e religião e a possibilidade de uma categorização errónea de alguém.

> "(…) uma pessoa nova que está a tentar saber mais sobre a sua própria cultura, a sua religião e sem querer foi parar aos noticiários, aos sites até mesmo, ou vídeos ou pouco mais suspeitos. E possa ser identificado como um possível criminoso, por apenas curiosidade. Isso acho que é bastante possível e injusto." (E4, masculino, 25 anos, 10º ano, empregado de mesa\bar, Açores).

> (…) Claro que sim, claro que sim. Para já sabemos as pessoas de classes mais desfavorecidas estão mais expostas e têm um risco maior de estarem em contexto até de conflito, estão menos protegidas." (E8, feminino, 50 anos, mestrado, técnica superior, Covilhã).

A falta de precisão foi referida por alguns respondentes (E2; E4; E5; E7; E9) que transmitiram alguma preocupação com a possibilidade de os processos de *social sorting* catalogarem algum cidadão de forma errónea. Adicionalmente, consideraram que os dados desse modo obtidos não devem ser a única fonte de informação a ser utilizada pelos governos.

> "Pois, o problema é esse, é que às vezes podem não ser precisas, podem não ser reais e depois a pessoa pode-se sentir lesada nalgumas circunstâncias por causa dessa, lá está, de tirarem essa conclusão e de chegarem a criarem esse, essa categoria da pessoa e a dizer, esta pessoa está nesta categoria e enquadra mais neste quadro do que aquele, e pronto." (E11, feminino, 55 anos, 12º ano, assistente de contacto, Porto).

> "Sinceramente não, eles conseguem ter ideia do que é que aquela pessoa pode ser, mas para ter 100% de certeza disso, epá têm que falar das pessoas, têm de conhecer minimamente as pessoas, aí sim já vão conseguir, mas não vão fazer isso a toda a gente." (E13).

Os respondentes parecem reticentes à tendência para uma maior automação dos processos da vigilância referida por Lyon (2014). Essa hesitação deveu-se, em vários casos, principalmente, a questões relacionadas com a precisão e com a discriminação, uma vez que determinados dados podem ser erroneamente interpretados por dispositivos automatizados; especialmente face ao facto de essa mesma interpretação se tratar de um conjunto de processos que não são informados pelos contextos socioculturais.

4.6 – Vigilância Comercial

Tiveram-se em conta 3 indicadores. Em primeiro lugar, a noção sobre a recolha de dados, na qual se procurou captar a consciencialização dos processos de vigilância comercial. Em segundo lugar, o reconhecimento de vantagens e desvantagens da cedência de dados, neste indicador procurou-se explorar a forma como os cidadãos percecionam as vantagens e desvantagens que advém da cedência de dados pessoais. E por último, a opinião sobre o *social sorting* comercial, onde se explorou a opinião dos entrevistados em relação à categorização de consumidores.

Noção sobre recolha de dados

Nas questões relativas a este indicador foram apresentadas situações frequentes do quotidiano de qualquer utilizador de internet como, por exemplo, o *display advertising* ou a recolha de dados pessoais através de aplicações móveis.

Todos os entrevistados afirmaram que se apercebem da recolha de dados por motivos comerciais. Quando questionados sobre o *display advertising*, vários entrevistados (E1; E2; E5; E6; E8; E10; E13) referiram sentir-se incomodados pela sua existência. Nos seus discursos, o *display advertising* revelou-se ainda, no caso de alguns respondentes, como o momento em que se aperceberam ou refletiram sobre a monitorização da sua atividade *online*.

> "Fico muito assustada, porque isso de alguma forma… mostra que eu tenho um rasto online (…)." (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

> "Ah comecei logo a dizer, olha estes aqui já me estão aqui a tentar enfiar (risos)… claro que com uma visão crítica e aborrecida porque pensei logo que, então isto realmente é uma chatice porque qualquer coisa que a gente faça aqui, é monitorizada, é avaliada, não é? E isso é uma coisa que para mim é um bocado complicado sim". (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

Curiosamente nos discursos das entrevistadas E1, E2 e E8, o incómodo reportado parece ser motivado, não pela existência do *display advertising*, mas pela sugestão de produtos que não interessam, ou que já não interessam, às entrevistadas.

> "Por acaso não acho muita… não acho piada nenhuma porque isso, se tive a pesquisar e já não estou a pesquisar é porque não quero saber mais deles. Então estão ali só como a ali a fazer uma pequena publicidade para eu me relembrar do que é que eu vi para tentar comprar… Isso não acho… não gosto muito." (E2, feminino, 40 anos, 12º ano, escriturária, Açores).

> "Fico irritada (risos). Irritada porque, pois já comprei aquilo já não quero e eu só queria que aparecesse aquilo que eu preciso, ou queria ser eu a tomar a decisão daquilo que eu quero ver. E nós, é nesses momentos é que ficamos irritados porque percebemos que perdemos o controlo das nossas decisões, e que são os outros a decidirem." (E8, feminino, 50 anos, mestrado, técnica superior, Covilhã).

Outros entrevistados consideraram que o *display advertising* tem vantagens e desvantagens (E3; E11; E12; E15; E16), sendo que as vantagens identificadas com mais frequência foram, na sua maioria, a apresentação de preços mais competitivos dos produtos que os entrevistados desejavam comprar.

> "(…) às vezes é positivo porque às vezes até podemos estar a ver determinado produto num determinado site, e é um valor e é aquilo que a gente pretende". (E11, feminino, 55 anos, 12º ano, assistente de contacto, Porto).

> "Já é tão usual, hoje em dia, isso já acontece há bastante tempo (..), simplesmente se eu vir eu vou… Epá ok está mais barato aqui, deixa ver, se é um produto que eu realmente quero, é uma forma de eu poder procurar e procurar mais rápido aquilo que eu quero." (E12, masculino, 25 anos, licenciatura, mestrando e investigador em engenharia informática, Santarém).

Se atentarmos à diversidade de perceções em relação ao *display advertising*, especialmente ao nível dos seus aspetos positivos, pode-se sugerir que a monitorização exercida pelo comércio online pode ser benéfica para o cidadão. Porém, alguns entrevistados parecem estar melhor posicionados para reconhecer e aproveitar os benefícios provenientes desta nova economia, tal como argumenta Lyon (2006). Também a conveniência que advém deste tipo de processos de vigilância parece ser apreciada pelos entrevistados, na medida em que o *display advertising* pode poupar algum tempo e esforço aos cidadãos ao lhes serem apresentadas sugestões, em forma de *display advertising*, baseadas em algoritmos. Esta perceção parece estar presente nos respondentes com maior conhecimento sobre a vigilância comercial. Enquanto outros entrevistados, com menores níveis de conhecimento sobre esta questão, parecem refletir mais sobre a existência da vigilância comercial e o incómodo que a mesma lhes provoca.

Relativamente à recolha de dados pessoais na utilização de aplicações móveis, a grande maioria dos respondentes tem noção da sua existência (E3; E4; E5; E7; E9; E10; E12; E13; E14; E15), não se revelando surpresos quando confrontados com a notícia utilizada na questão 18 do guião (ver Anexo 3). Por outro lado, alguns entrevistados (E1; E13) mostraram-se surpreendidos pela possibilidade de as aplicações recolherem dados pessoais dos seus utilizadores, revelando alguma preocupação com a venda desses mesmos dados.

> "Sinceramente ficava preocupado, é uma notícia mesmo forte. Se isso acontece, lá está (…) epá, eu não sabia, não sabia que andam a vender dados das pessoas, mas se isso acontecer sinceramente é muito mau, é negativo." (E13, masculino, 24 anos, 12º ano, segurança, Covilhã).

A forma como os consentimentos são apresentados aos cidadãos dificulta a sua interpretação, resultando muitas vezes num desconhecimento completo sobre a venda de dados pessoais, por exemplo. As pessoas com menor conhecimento sobre a vigilância parecem ser mais vulneráveis às estratégias sofisticadas, e muitas vezes subtis, que determinadas entidades comerciais adotam com a intenção de obter consentimentos "informados". Alguns respondentes, como o E13, parecem preocupar-se com a venda de dados, podendo, caso soubessem da recolha e venda de dados recolhidos pelas aplicações móveis, adotar uma postura significativamente diferente sobre a utilização dessas aplicações.

Reconhecimento de vantagens e desvantagens da cedência de dados

Todos os respondentes referiram conhecer as vantagens oferecidas pela cedência de dados em algum momento, sendo que as vantagens referidas com mais frequência pelos respondentes prendem-se com promoções e ofertas especiais. Com a exceção da E11, todos os respondentes identificaram também desvantagens provenientes da cedência de dados, manifestando alguma preocupação com a sua privacidade, enquanto outros preocuparam-se com a possibilidade de serem manipulados a consumirem mais do que desejariam. No entanto, os respondentes, mesmo sentindo algum incómodo com os processos de vigilância, continuam a sujeitar-se à vigilância comercial devido às vantagens que lhes são oferecidas. Os respondentes pareceram avaliar a situação como uma troca de custo-benefício, onde a cedência de dados traz, na maior parte das vezes, mais benefícios do que custos. Os resultados parecem estar de acordo com o estudo de Zurawski (2011), onde se concluiu que, frequentemente, os indivíduos não são influenciados pela sua preocupação ou pela consciência de que os seus dados estão a ser recolhidos, tendendo a proceder a uma troca de dados pessoais por benefícios comerciais; mesmo quando revelam algumas preocupações com a cedência dos seus dados. Também o nível de confiança ou frequência de consumo de produtos/serviços de uma determinada entidade comercial, parece influenciar a decisão dos respondentes em proceder à referida troca. As preocupações com a privacidade e com a recolha de dados parecem ceder perante os possíveis benefícios oferecidos pelas entidades comerciais. Mesmo os entrevistados que se manifestaram preocupados com a recolha de dados relacionada com a vigilância comercial, afirmaram ser praticamente inevitável a cedência dos dados para a obtenção de benefícios comerciais.

> "(…) compras na internet como conheço muita gente que não o faz, não coloca os dados mesmo em sites de confiança, por exemplo fazer uma compra online no Continente, que há partida não tem nenhum problema, eu faria isso" (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

> "(…) não sou muito aquela pessoa de epá vou fazer este cartão que este cartão me poupa 1 euro… também não, a não ser que seja uma coisa que eu use muito… por exemplo o combustível como já referi aí sou atualmente taxista e atualmente todas as vezes que abasteço o meu táxi poupo 3 euros e 70 cêntimos num tanque. Isso no fim do verão dá-me muito dinheiro, aí vale a pena. (E3, masculino, 35 anos, 12º ano + curso técnico (IV) em informática, taxista, Açores).

> "Sim sim, tenho é inevitável quase (risos). (…) Oh por causa dos descontos e não sei quê, pronto (…) também é uma maneira de dar dados que não se deve dar. Embora aí só se dá… mas é suficiente, mas dá-se alguns dados é verdade, mas sim tenho alguns." (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

> "Pois, isso é outra questão. Inicialmente não, porque tinha de dar uma série de dados e achei melhor não, mas depois há aquelas coisas de termos uma série de pontos, bónus,

> descontos, e acabei por aderir ao cartão sim." (E14, feminino, 40 anos, doutoramento em informática, especialista em tecnologias de informação, Covilhã).

Como Acquisti, Taylor e Wagman (2016) sugerem, os dados pessoais parecem ter algum tipo de valor monetário para os cidadãos. Para o participante E3, por exemplo, o valor subjetivo dos dados pessoais é claramente superior a 1 euro, visto que o E3 não fornece os seus dados pessoais em troca de benefícios comerciais no valor de 1 euro. No entanto, quando o participante reflete sobre a obtenção de um desconto frequente no valor de 3,70 euros, já considera que vale a pena trocar os seus dados pessoas pelo desconto em questão.

Por outro lado, dois respondentes (E15; E16) referiram preferir, por vezes, não aceder a determinados serviços e promoções devido ao desconforto associado a questões de privacidade e provocado pela cedência dos seus dados.

Turow, Feldman e Meltzer (2005) salientam que as pessoas com maiores níveis de escolaridade aceitam mais facilmente os procedimentos relacionados com a vigilância comercial, porque acreditam saber tirar melhor proveito das suas vantagens, enquanto os utilizadores com menor escolaridade apresentam uma maior preocupação. No presente estudo, os resultados contrastam, de certa forma, com os resultados do estudo mencionado, na medida em que todos os respondentes conseguiram identificar vantagens, independentemente do grau de escolaridade. Verificou-se ainda que os respondentes com maiores níveis de escolaridade parecem estar conscientes das possíveis desvantagens que podem advir da cedência de dados, enquanto uma participante com menos escolaridade e maior dificuldade em identificá-las, como o caso da E11, uma participante que nunca frequentou o ensino superior e que não reconheceu qualquer tipo de desvantagem nos processos de vigilância comercial. Como referem Park, Shung e Shin (2018), a complexidade do processo cognitivo que possibilita a identificação das desvantagens que, geralmente, ocorrem de forma indireta e subtil da cedência de dados, poderá ser um fator que dificulta a compreensão das diferentes formas como os cidadãos podem ser prejudicados, enquanto as vantagens da cedência de dados são amplamente reforçadas por motivos comerciais. Os indivíduos tendem a centrar-se mais nos benefícios imediatos e na conveniência que lhes é oferecida pela vigilância comercial, algo que pode levantar questões que suscitam investigação em relação à possibilidade das pessoas com menos capital cultural, escolaridade e conhecimento informático estarem mais expostas às desvantagens.

Opinião sobre o *social sorting* comercial

Nas questões relacionadas com este indicador abordou-se os processos de *social sorting* que se traduzem, frequentemente, numa série de serviços e de promoções personalizadas para cada tipo de consumidor.

Um número bastante significativo de respondentes identificou as lógicas do *social sorting* como sendo globalmente positivas (E1; E4; E5; E6; E7; E8; E9; E10; E12; E14; E15; E16), apesar de revelarem um ligeiro incómodo com as referidas questões associadas à privacidade e à

manipulação. É possível notar alguma congruência com as perceções das vantagens\desvantagens que os processos de vigilância comercial podem implicar. Quando questionados sobre a possível discriminação de determinados consumidores, alguns entrevistados acreditam na existência de alguma discriminação (E8; E10; E14; E15; E16), referindo o facto de alguns consumidores terem acesso a serviços de maior qualidade devido a uma capacidade de consumo mais alargado, enquanto outros têm de se conformar com serviços de inferior qualidade. Autores, como Lyon (2005; 2014) e Pridmore (2012), já haviam alertado para esta possibilidade nas suas publicações, especialmente, no que toca ao atendimento desigual dos consumidores, algo que parece estar presente nas perceções dos entrevistados.

Outros entrevistados só identificaram uma possível discriminação no caso dos cidadãos que não sabem como usufruir das vantagens oferecidas pela cedência de dados.

> "Aaaa (hesitando) Eu (suspiro fundo) eu acho possível se as pessoas não tiverem conhecimento desses cartões, cupões. Só por aí, penso que só por aí, penso eu." (E1, feminino, 35 anos, 12º ano, assistente operacional, Açores).

Este desconhecimento das desvantagens, como foi referido anteriormente, poderá resultar em posições de maior vulnerabilidade, por parte dos cidadãos menos informados, no que respeita às formas como a vigilância atua, uma vez que desconhecem as formas como podem ser prejudicados.

4.7 – Ações de Negociação da Vigilância

A análise baseou-se em 4 indicadores. Em primeiro lugar, na valorização subjetiva da privacidade online, onde se procurou explorar até que ponto os entrevistados valorizam a sua privacidade em contexto online, tal como a sua capacidade para a manutenção dos graus que desejam. Em segundo lugar, no condicionamento da atividade devido à vigilância, sendo analisados os possíveis constrangimentos que a vigilância eletrónica pode causar no quotidiano dos entrevistados. Em terceiro lugar, no incómodo causado pela vigilância, onde se analisam as situações que incomodam os entrevistados e as perceções sobre a possibilidade de as evitar. E por último, nas estratégias de neutralização da vigilância, com o objetivo de identificar as estratégias de neutralização da vigilância que os entrevistados utilizam, bem como as respetivas motivações para o fazerem.

Valorização subjetiva da privacidade online

Os entrevistados afirmaram unanimemente que valorizam a sua privacidade online. Como se pode ver em alguns testemunhos abaixo, a maioria dos entrevistados (E3; E4; E5 E6; E8; E10; E11; E12; E13; E14; E15; E16) considerou, no entanto, que, apesar da sua vontade e esforço para preservar a sua privacidade online, não o conseguem fazer.

> "Privacidade na internet? O que é isso? Não tenho, nem ninguém tem, agora se eu gostava de ter? Gostava. Há formas de conseguirmos fazer algumas pesquisas, (…) para

> chegar ao ponto de o conseguir fazer e de ter já os conhecimentos para fazer isso, é porque já fizemos tudo isso sem estar protegido, sem salvaguardar a nossa privacidade." (E12, masculino, 25 anos, licenciatura, mestrando e investigador em engenharia informática, Santarém).

> "Ideologicamente sim, mas pragmaticamente nem tanto (risos) (…), tendo a ser favorável à manutenção da minha privacidade, não sou assim tanto, sou cada vez mais, mas não sou assim tanto como gostaria de ser. (…) Porque uma pessoa também depois não faz nada sinceramente (…)." (E15, masculino, 22, licenciatura, mestrando em relações internacionais, Guarda).

Este discurso, bastante frequente por parte de vários entrevistados, levanta questões sobre o já estudado paradoxo da privacidade em contexto de cedência de dados. O referido paradoxo refere-se a uma disparidade entre a intenção inicial para a não cedência de dados e o fornecimento, na prática, de dados pessoais. Os cidadãos afirmam, frequentemente, não ter intenção de fornecer dados pessoais, porém, quando são confrontados com situações práticas onde a cedência de dados é requerida, acabam por fornecê-los (Norgberg, Horne e Horne, 2007.) Vários estudos tentaram desenvolver uma explicação para o paradoxo da privacidade, para Baek (2014) o facto de os cidadãos raramente experienciarem diretamente as violações de privacidade, é uma das razões para a existência deste paradoxo no contexto *online*. Este argumento poderá estar relacionado com a perceção do E7, o entrevistado referiu valorizar a sua privacidade, porém, afirmou não se preocupar com a cedência dos seus dados, porque não se considera uma "pessoa de interesse".

> "(…) Porque, como já disse, acho que não tenho uma opinião de relevo na sociedade para me preocupar com a má utilização dos meus dados, eu sou simplesmente um habitante em dez milhões de portugueses. Não tenho nada que me destaque da população normal." (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

Por outro lado, contrariamente ao argumento de Baek (2014), as perceções de vários respondentes deste estudo, sugerem que as inconveniências, ou até mesmo a impossibilidade de livre acesso\navegação associadas aos comportamentos de proteção de privacidade, constrangem em demasia a sua atividade *online*. Sendo assim, o paradoxo da privacidade, neste contexto, pode ser motivado pela simples incapacidade de garantir os níveis desejados de privacidade online, sem que exista um constrangimento da atividade online para níveis que os entrevistados consideram indesejáveis.

Condicionamento da atividade devido à vigilância

Os resultados apresentados neste indicador foram informados através de questões, colocadas aos respondentes, que incidiam sobre potenciais condicionamentos na sua navegação online. A

análise focou-se nas pesquisas\navegação na web, e num evitamento da utilização de certas aplicações na tentativa de impedir a recolha de dados pessoais.

No que respeita ao condicionamento na navegação online, apenas dois entrevistados (E3; E5) referiram evitar pesquisar algo nos motores de busca que os pudesse ligar, de certa forma, a algum tipo de terrorismo. A grande maioria dos entrevistados (E6; E7; E9; E10; E12; E14; E15; E16) referiu que, quando desejam pesquisar ou entrar em determinado website, simplesmente o fazem sem grande preocupação com a possibilidade de estarem a ser monitorizados.

> "Oh, quer dizer eu sei quando estou a pesquisar estão a saber tudo o que estou a fazer, mas como maior parte das vezes são questões de trabalho, ou questões de resolução de problemas de dia-a-dia (…)." (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

> "Hmm não, quando eu tenho de pesquisar alguma coisa normalmente eu faço-o, eu faço a pesquisa. O que depois, depois de ter a minha primeira resposta, ou seja, quando visitamos a listagem dos resultados aí seleciono de certa forma onde vou fazer o clique. Mas a pesquisa normalmente faço-a naturalmente." (E6, masculino, 47 anos, 12º ano, empresário, Lisboa).

A noção que a atividade online dos entrevistados pode ser alvo de monitorização, não parece condicionar os seus comportamentos na internet. De acordo com alguns respondentes, a ausência de consequências provocadas pela monitorização da sua atividade *online,* como por exemplo, quando efetuam pesquisas nos motores de busca, bem como a impessoalidade dos temas que pesquisam, parecem justificar o seu não-condicionamento.

Por sua vez, ao interrogar-se os entrevistados sobre pesquisas em motores de busca, na resposta de uma participante (E5), poderá estabelecer-se ligações com a metáfora do panótico elaborada por Foucault (1995), nomeadamente, devido ao condicionamento da atividade da respondente. A atividade da respondente aparenta ser algo condicionada por um sentimento de incerteza semelhante ao que Foucault referiu, isto é, ao facto de não se saber exatamente se estamos ou não a ser alvo dos processos de vigilância. A incerteza sobre a sujeição, ou não, da participante aos processos de vigilância governamental parece condicionar a sua forma de agir na internet.

> "Não sei, mas sei lá as vezes penso em pesquisar alguma coisa em anónimo, alguma coisa pessoal por exemplo… Nem é pessoal, mas… se calhar penso duas vezes se eu pesquisar alguma coisa sobre terrorismo ou qualquer coisa assim. Penso sempre que de alguma forma isso está a ser, essas palavras estão a ser selecionadas para… Também por essas questões de segurança, se tivesse a frequentar páginas mais subversivas e cenas mais alternativas… penso que isso pode estar a ser controlado por entidades governamentais, não privadas. Mas não deixo de visitar." (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

Já os entrevistados que aparentam sentir-se mais condicionados pela vigilância, referiram preocupações que se prendem com questões relacionadas com o cibercrime, e que resultam numa maior ponderação na escolha dos websites que acedem.

> "Normalmente quando acho que o deva fazer, eu faço-o sempre. Ah! não entro em sites estranhos, esquisitos… não sou muito dado a esse tipo de situações, mas quando eu acho que há uma determinada informação que eu pretenda ter e está num determinado local eu entro sem problemas nenhuns." (E9, masculino, 57 anos, 12º ano, assistente operacional, Covilhã).

> "Sim, já cheguei a querer entrar um site… a pensar entrar, na altura estava com um amigo e ele disse para não entrar que aquilo criava vírus, uma vez entrou que aquilo depois o telemóvel nunca mais ficou em perfeitas condições, quando entrava na internet e assim. Ele disse que poderá, poderia ter sido o facto de ter entrado naquele link que criou, de alguma forma, problemas no telemóvel, agora se é verdade? Eu também não sei, mas ele disse que em princípio foi isso, então eu ia para entrar e pensei epá não, não vou arriscar por se calhar não compensa." (E13, masculino, 24 anos, 12º ano, segurança, Covilhã).

No que respeita ao condicionamento da atividade na internet, alguns entrevistados, que se manifestaram mais preocupados, refletiram imediatamente sobre a ligação entre vigilância e cibercrime, algo que poderá ser atribuído à noção das consequências diretas e graves que o cibercrime pode ter nas suas vidas. Enquanto outras consequências, com impactos mais indiretos, parecem ser colocadas em segundo plano.

Incómodo causado pela vigilância

Os resultados apontam para a existência de três tipos de perceções diferentes em relação ao incómodo causado pela vigilância. Alguns entrevistados referiram que se sentem incomodados com diversos aspetos da vigilância comercial (E1; E3; E4; E6; E8; E9; E16). Os aspetos mais invasivos provocaram um incómodo maior como, por exemplo, os diversos *pop-ups* com sugestões de produtos e até as notificações que pedem o consentimento informado para a recolha dos cookies.

Por outro lado, certos entrevistados consideraram não sentir um incómodo relevante (E2; E5; E7; E10; E13; E15), considerando que o desconforto causado pela vigilância não é suficientemente elevado para se sentirem incomodados, ou pelo simples facto de nunca terem sentido consequências diretas devido aos processos de vigilância de que são alvos.

> "(…) não é uma coisa assim muito grave. Pronto, não gostava, mas não era nada grave." (E2, feminino, 40 anos, 12º ano, escriturária, Açores).

> "Não, pessoalmente nunca me aconteceu nada de…não nunca me aconteceu nada, nunca tive problemas." (E13, masculino, 24 anos, 12º ano, segurança, Covilhã).

> "Não, porque não estou…nunca senti consequências disso." (E15, masculino, 22, licenciatura, mestrando em relações internacionais, Guarda).

Estes resultados parecem estar de acordo com o que Baek (2014) sugere afirmar que a ausência de consequências diretas contribui para uma postura menos preocupada em relação à vigilância.

Relativamente ao uso de extensões para reduzir o incómodo causado pela vigilância, vários entrevistados admitiram a utilização de *adblockers* (E3; E4; E6; E7; E9; E12; E14; E15), esta utilização parece estar relacionada com o nível de conhecimento informático dos utilizadores, sendo que se pode constatar que alguns entrevistados – que até nem referiram sentir um incómodo relevante com a vigilância, mas que têm um maior conhecimento informático – utilizam *adblockers*. Enquanto os entrevistados que disseram sentir-se incomodados e que, aparentemente, tinham um conhecimento informático menor, não os utilizavam frequentemente porque desconheciam este tipo de extensão.

Relativamente à possibilidade de resistência à vigilância, a grande maioria dos entrevistados considerou-a como quase impossível (E3; E4; E6; E7; E8; E9; E12; E14; E16). Essa impossibilidade mencionada pelos entrevistados deve-se aos constrangimentos que a resistência provocaria na navegação, já que ela seria necessariamente muito limitada. Outros entrevistados referiram ainda que a única forma de resistir à vigilância seria simplesmente a não utilização de dispositivos com acesso à internet.

> "Há, quando perdemos o acesso a quase toda a informação, aquilo que a internet nos propôs no início era que nós teríamos livre acesso a quase tudo. O que está a acontecer agora é que todo o acesso está a ser bloqueado, a internet descobriu que essa informação, que antes era útil e podia ser usada para produtos, começa hoje a ser cobrada. E nós só, eu acho importante porque também é preciso pagar o trabalho de algumas pessoas, mas também não vejo que pelo simples facto de fazermos uma pesquisa numa empresa que vende um determinado produto que depois haja outra empresa que possa assediar, ou que nos tente ou que nos importune por nós termos feito isso." (E6, masculino, 47 anos, 12º ano, empresário, Lisboa).

> "Não, não acho que seja correto. Até porque maior parte dos utilizadores nem sabe disso porque isso faz parte daquelas letrinhas pequeninas dos termos e condições, que raramente os utilizadores acabam por ler e acho que deveria ser algo mais explicito quando se está a descarregar uma aplicação ou qualquer outro tipo móvel, deviam dizer a sua informação vai ser vendida (gesticula demonstrando que deve ser uma informação bastante clara e direta), aceita? Em vez de colocarem as letras pequeninas nos termos e condições." (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

Parece haver uma aceitação forçada da vigilância por parte dos entrevistados. Muitos deles, ao refletir sobre o incómodo gerado pela vigilância comercial, parecem compreender a necessidade da existência de várias formas de rentabilizar os conteúdos disponibilizados de forma gratuita na internet. Porém, alguns entrevistados parecem discordar da forma como essa rentabilização é feita atualmente, mencionando um especial incomodo com as tentativas demasiado insistentes para uma obtenção de lucro através da vigilância comercial, considerada por alguns respondentes como uma forma de "assédio". Também o modo pouco claro como a troca de benefícios comerciais por dados pessoais se processa (Wottrich, Reijmersdal, e Smit, 2018), especialmente quando acompanhada de uma consciencialização elevada da vigilância comercial, incomoda significativamente os entrevistados.

De forma contrastante, dois entrevistados (E11; E13) afirmaram que era possível resistir à vigilância. A E11 acredita que o tem conseguido devido à sua navegação cuidada, enquanto o E13 acredita na existência de algum serviço pago que lhe possa permitir resistir à vigilância.

> "Não sei dizer, até à data tem sido (risos) Até à data não tenho…tenho evitado sempre, no futuro não sei, a gente costuma dizer, o amanhã a gente não sabe como vai ser, mas pronto. Presentemente mantenho a minha posição de partilhar os meus dados, mesmo só se eu achar que os posso partilhar, se achar que não devo partilhar, não partilho." (E11, feminino, 55 anos, 12º ano, assistente de contacto, Porto).

A capacidade de resistir à vigilância, muito provavelmente sobrestimada, pela E11, poderá ser motivada pela sua falta de conhecimento informático e acerca das lógicas da vigilância comercial. A tendência dos cidadãos para sobrestimar a sua capacidade para resistir à vigilância, já havia sido identificada por Turow, Feldman e Meltzer (2005), apesar de a premissa de que as pessoas com menos escolaridade se preocupam mais com os processos de vigilância, não constar nas perceções dos respondentes deste estudo. As duas outras entrevistadas (E1; E2) não emitiram qualquer opinião.

Estratégias de neutralização da vigilância

As estratégias de neutralização adotadas por respondente são apresentadas na Tabela 5.

Tabela 5 - Estratégias de neutralização da vigilância adotadas por participante

Entrevistados	Recusa	Evitamento	Distorção	Disfarce	Inviabilização
E1	X	X			NQ
E2					NQ
E3	X		X	X	
E4	X	X	X		NQ
E5		X	X		X
E6		X			X
E7	X		X		
E8		X			X
E9	X	X			X
E10	X		X		X
E11		X			
E12			X	X	
E13			X		X
E14	X	X			X
E15	X		X		X
E16	X		X		X

NQ – Não foi questionado.

Antes de proceder à interpretação e análise dos resultados presentes neste indicador, importa referir que o guião utilizado na realização das primeiras 4 entrevistas, não continha uma questão específica sobre a utilização desta estratégia. Durante a entrevista ao E3, surgiram algumas questões relativamente às pessoas taparem as suas *webcams* com autocolantes. Seguidamente, releu-se Marx (2016), o que permitiu encaixar esta ação nas estratégias de inviabilização definidas pelo autor, transpondo-se, posteriormente, uma questão sobre essa matéria para o guião utilizado nas restantes entrevistas.

Quanto às estratégias de neutralização utilizadas pelos entrevistados, as estratégias de recusa foram as mais frequentemente utilizadas pelos entrevistados (E1; E3; E4; E7; E9; E10; E14; E15; E16), tendo sido a recusa em fornecer um consentimento para a recolha de cookies a mais referida pelos entrevistados. De entre estes entrevistados, alguns optam por uma recusa mais intensa e procuram outras fontes para acederem ao conteúdo desejado (E3; E10). Enquanto outros entrevistados acabam por aceitar os cookies, embora relutantemente, de forma a aceder ao conteúdo que desejam (E7; E9; E15; E16), especialmente em casos de conteúdos interessantes a que estão a tentar aceder.

> "Se for uma coisa muito relevante, ou seja, se eu precisar mesmo se for de um site que eu estou, isto acontece às vezes, numa revista qualquer ou programa qualquer que eu quero…eu aceito às vezes, aceito sim. E penso lá está, é o que eu lhe dizia… não fico confortável." (E16, feminino, 42 anos, doutoramento, docente universitária, Viseu).

A decisão sobre a adoção de uma recusa mais direta ou de uma aceitação relutante, parece ser afetada principalmente pelo grau de interesse no conteúdo dos websites a que o participante

quer aceder. Outro fator que parece ser importante nesta tomada de decisão, prende-se com o incómodo e perda de tempo que a recusa dos cookies implica. Os diversos mecanismos desenvolvidos para persuadir à conformidade com a vigilância comercial, parecem surtir efeito em vários entrevistados, tal como Lyon (2006), Rogers (2008) e Marx (2015) haviam denunciado.

Importa salientar que foram poucos os entrevistados que leram os consentimentos para os cookies (E3; E6; E8; E14), tendo os restantes respondentes admitido, revelando-se um pouco embaraçados, que nunca os leram completamente. De forma coerente com as opiniões mencionadas na dimensão, e previamente apresentadas nos resultados sobre os consentimentos informados no geral, vários respondentes (E6; E8; E9; E12; E14; E15; E16) identificaram uma série de estratégias subtis que dificultam fortemente a leitura e a recusa dos consentimentos para a recolha de cookies.

> "Não (risos). Confesso que não, é que são letras tão pequenas e os contrastes também não ajuda, que eu não me dou a esse trabalho (risos)." (E9, masculino, 57 anos, 12º ano, assistente operacional, Covilhã).

> "Não, e acredito que as únicas pessoas que o tenham lido seja quem os escreveu. (…) Para já porque são muito extensos, por norma são muito extensos (…) é simplesmente um aviso, olhe estamos a recolher os seus dados, (…) está bem? Pronto. E é isto só que é escrito de uma forma muito extensa, muito complexa e para a qual as pessoas não têm tempo (…)." (E12, masculino, 25 anos, licenciatura, mestrando e investigador em engenharia informática, Santarém).

> "Comecei mas é aquilo que eu lhe dizia, aquilo é impossível uma pessoa começa…Eu acho que aquilo é intencional é feito de forma a que nos vençam por exaustão, e portanto e para além de que às vezes a própria termologia usada, a maneira como a informação é colocada mesmo em termos e frases, a terminologia não é… Sim mas já estive coisas em que me meti a ler e depois desisti." (E16, feminino, 42 anos, doutoramento, docente universitária, Viseu).

A decisão sobre a aceitação ou rejeição da cedência de cookies por parte dos respondentes, não parece ser influenciada pelo conteúdo dos consentimentos informados. Os respondentes parecem ter já a sua opinião formada sobre a cedência de cookies, sendo a recusa da cedência preferível na maioria dos casos. Por outro lado, a inconveniência e o incómodo, que a recusa da cedência cookies pode implicar, parecem ser os fatores mais importantes na tomada de decisão sobre a utilização desta estratégia de neutralização. Como Rogers (2008) referiu, o esforço para recusar cada cookie, leva a que mais tarde ou mais cedo os cidadãos acabem por seguir a opção por defeito – a aceitação.

Em linha com a tomada de decisão que gera menos esforço, parece estar a atitude de alguns dos respondentes menos informados sobre a vigilância e sobre as potenciais consequências da mesma. Estas respondentes, sem ler nem refletir sobre as informações que estão a fornecer,

simplesmente optam pela opção que requer menos esforço e que causa um incómodo menor, ou seja, a aceitação sem ler, questionar ou recusar.

> "Aceito (risos) Nem sequer leio (risos) (…), para que aquilo desaparecesse de lá (risos)". (E2, feminino, 40 anos, 12º ano, escriturária, Açores).

> "Isso clico para eles que aceito e deixo passar. Já tentei procurar e disseram-me que o melhor a fazer é clicares e deixa estar, e é o que eu faço clico e pronto." (E11, feminino, 55 anos, 12º ano, assistente de contacto, Porto).

Alem das implicações ao nível do esforço, a aceitação pouco informada, aliada à não reflexão sobre a cedência de cookies, poderá estar relacionada com níveis menos elevados de conhecimento e de preocupação com a vigilância eletrónica.

As estratégias de evitamento também foram frequentemente mencionadas pelos respondentes (E1; E4; E5; E6; E8; E9; E11; E14), sendo que, de entre as ações mais comuns, foram identificadas: a utilização cuidada e limitada do GPS e Wi-Fi nos seus dispositivos; uma navegação seletiva e, por último, um participante referiu preferir comunicar através do Serviço de Mensagens Curtas (SMS), visto que utiliza outro meio que não é o da internet.

Quanto às estratégias de disfarce, apenas dois respondentes referiram utilizá-las (E3; E12), sendo a utilização de Proxys e de redes privadas virtuais (VPN's) as ações mais referidas. Curiosamente, os únicos dois entrevistados que utilizaram este tipo de estratégia têm formação em informática, o que poderá ser explicado, por enquanto, pela reduzida disseminação dos Proxys e VPN's. Apesar destes resultados, de acordo com um website de revisão e avaliação de VPN's, o uso de VPN's em Portugal e no mundo é algo frequente, estimando-se, inclusivamente, que a sua utilização tenderá a ser cada vez mais frequente, sendo que os desejos de manter a anonimidade online, tal como contornar bloqueios antipirataria, são as principais motivações para a crescente utilização de VPN's (Mardisalu, 2019).

As estratégias de distorção foram mencionadas por vários respondentes (E1; E3; E4; E5; E7; E10; E12; E13; E15; E16), sendo o fornecimento de dados falsos a ação mais frequente. A decisão para o fornecimento de dados verdadeiros parece depender do contexto onde a cedência é requerida.

> "Por exemplo… quando peço, quando faço encomendas de um site, de uma loja, por exemplo, (…) foi só meter os dados, os meus dados, nada de especial, (…) pedia a morada para enviar a encomenda, mas isso é normal, isso hoje em dia é mesmo assim.(...) Agora, por exemplo, às vezes para entrar em certos jogos, de aplicação, para jogar já cheguei a meter dados tipo, (…) meto o email ou um nome qualquer (…)." (E13, masculino, 24 anos, 12º ano, segurança, Covilhã).

> "Pois, depende muito. Por exemplo se eu criasse uma conta no Continente para fazer contas online eu cedia. Porque, o facto de ser uma empresa portuguesa, (…) Porque sei

> que é algo real, não é? É um site que é real, que eu conheço pessoas que fazem compras através do site. Se for por exemplo um site de filmes ou assim, se for possível fugir à (entrega) informação verdadeira eu ponho um nome qualquer diferente." (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

Os respondentes, geralmente, dão dados verdadeiros nas situações onde a veracidade deles é requerida para que se concretize a sua vontade. Veja-se, por exemplo, o contexto de compras online, onde a morada é um requisito absoluto para que as compras cheguem aos respondentes, ou o caso do acesso online a determinados serviços públicos. Enquanto, noutros contextos, onde não são requeridos, necessariamente, dados verdadeiros para concretizar as intenções dos respondentes, são fornecidos dados falsos como, por exemplo, em *websites* de *streaming*, aplicações móveis, registos em *websites*, entre outros. O que vai de encontro ao que Marx (2016) refere: os contextos aliados à concretização dos objetivos dos respondentes, parecem ser decisivos na decisão para o fornecimento de dados falsos. Também os propósitos da recolha de dados, como referiram Kennedy, Elgesem e Miguel (2015), parecem ser importantes, dado que os respondentes compreendem e consideram natural a cedência de informações sobre a sua morada para que possam receber as suas encomendas.

Por último, as estratégias de inviabilização foram também frequentemente mencionadas (E5; E6; E8; E9; E10; E13; E14; E15; E16), sendo o cobrimento da webcam a ação mais referida. O facto de ser conhecido que Zuckerberg, um dos fundadores do Facebook, cobre a sua webcam, poderá ter influenciado os nossos respondentes.

Para além dessa estratégia, um participante mencionou ainda a desativação ou desinstalação do microfone do seu computador. A desativação ou desinstalação do microfone dos computadores pessoais pode-se associar facilmente a notícias sobre aplicações de assistência ao utilizador, como a Siri ou a Alexa, procederem à gravação dos utilizadores sem o consentimento dos mesmos.

É possível categorizar os respondentes deste estudo, consoante as categorias relativamente às atitudes e comportamentos perante a vigilância elaboradas por Marx (2016, pp.170). Seguindo as categorias do autor, como "verdadeiros conformistas" podem-se identificar os respondentes E2 e E7, uma vez têm uma atitude de aceitação da vigilância e um comportamento que não a tenta neutralizar. Na categoria de "conformistas intimidados" podem-se identificar um número significativo de respondentes (E1; E4; E5; E6; E8; E9; E10; E11; E13; E14; E15; E16), dado que têm uma atitude de rejeição perante a vigilância, mas que, nas suas ações - seja por não terem os recursos ou capacidades para a contrariar - acabam por a aceitar. E por último, na categoria de "rebeldes que se comportam de forma discreta", podemos identificar os respondentes E3, E10 e E12, uma vez que têm uma atitude de aversão em relação à vigilância massificada e tentam contrariá-la através da adoção de uma série de comportamentos efetuados de forma discreta.

4.8 - Perceção sobre as Consequências da Vigilância

Foram identificadas diversas consequências da vigilância, tanto de caráter mais geral como mais específico, como por exemplo: ao nível da privacidade; do condicionamento da vida pessoal; da manipulação de opiniões; de potenciar o cibercrime; das consequências no futuro profissional; e, por último, de ameaçar os direitos civis.

Quanto às consequências sobre a perda de privacidade, um número significativo de entrevistados (E1; E3; E6; E7; E8; E10; E11; E13; E14; E15; E16) considera que a principal consequência dos processos de vigilância é a própria perda de privacidade. Nos seus discursos, é possível verificar uma crença de que o direito à privacidade está a ser crescentemente ameaçado, algo que suscita algumas preocupações.

> "Pronto para mim, acho que isto…altera coisas importantíssimas que foram muito difíceis de conquistar como o direito à privacidade, o direito à liberdade, não é? Esse tipo de direitos que demoraram séculos a conquistar-se, não é?" (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

> "As pessoas sentem a sua vida privada invadida em todos os aspetos. (…) É o facto de alguém saber sempre onde é que uma pessoa está, o que é que está a fazer, o que vai comprar, e penso que isso deve ficar só no foro íntimo de cada um." (E14, feminino, 40 anos, doutoramento em informática, especialista em tecnologias de informação, Covilhã).

De entre os respondentes que referiram consequências relacionadas com a privacidade, dois participantes refletiram sobre a perda de privacidade pensando sobre o futuro adotando perspetivas distintas. O entrevistado E3 questiona se será positivo sacrificar a privacidade em troca de uma segurança garantida, o respondente mencionou o nível de segurança no filme "Minority Report" como exemplo, não emitindo diretamente qual seria a sua posição. Enquanto o E4 manifesta prontamente o seu desagrado com a crescente perda de privacidade que temos vindo a sofrer, demonstrando ainda uma preocupação com a evolução tecnológica, cada vez mais célere, da vigilância.

Alguns respondentes (E1; E2; E6; E7; E12; E16) emitiram opiniões sobre as consequências ao nível da privacidade refletindo sobre as consequências positivas e negativas que os processos de vigilância podem ter. Duas respondentes (E1; E2) refletiram imediatamente sobre uma troca de privacidade por segurança, a E1 afirmou sentir-se dividida, não conseguindo definir se aprova ou não a troca por ela percecionada. Enquanto a E2 referiu haver aspetos negativos e positivos, mencionando, no entanto, que havia mais aspetos positivos do que negativos visto que a vigilância lhe transmitia a ideia de que havia algum controlo sob as circunstâncias que pudessem pôr em causa a sua segurança. Por outro lado, a participante E16 considerou que há um lado

positivo, porém a entrevistada pensa que a forma como os processos de vigilância estão atualmente regulamentados não é suficiente para que o lado positivo seja mais saliente.

Por outro lado, dois respondentes, consideraram que as consequências podem ser de uma diversidade acentuada em termos de dimensão e natureza, podendo resultar, nas palavras do E7, tanto numa Terceira Guerra Mundial como num simples email com publicidade. O participante manifestou, também, alguma preocupação com uma certa discriminação proveniente dos processos de *social sorting*. Já o E6 limitou-se a especular sobre as consequências, veja-se o seguinte testemunho:

> "Eu posso especular, mas… Podem ser coisas muito graves, podem ser coisas muito boas, no fundo a sociedade, a sociedade é que irá valorizar ou desvalorizar esse tipo de coisas." (E6, masculino, 47 anos, 12º ano, empresário, Lisboa).

De forma similar o E12 não mencionou nenhuma consequência específica, o respondente limitou-se a considerar que existem consequências positivas e negativas.

> "Como já disse mais atrás, tem consequências boas e consequências más, cada pessoa vai interpretar como quer, cada qual vai puxar a brasa à sua sardinha e vai ser sempre assim, não há, a verdade é que…eles vão obter os nossos dados e vão, vai-nos caber a nós dizer se queremos que eles os recolham ou não, agora eu dizer ah eu não quero que recolham, eles vão recolher na mesma, não há grande hipótese aí." (E12, masculino, 25 anos, licenciatura, mestrando e investigador em engenharia informática, Santarém).

No discurso do E12 também é facilmente identificável um sentimento de resignação perante a vigilância. O que remete para o tipo de resignação enunciado por Hong (2017), segundo o qual muitos cidadãos não abdicam da sua privacidade voluntariamente, apenas a abdicam porque não têm outra opção, fazem-no manifestando sentimentos de resignação por não terem qualquer tipo de escolha.

Quanto às consequências ao nível da vida pessoal, uma participante (E10) referiu que atualmente apenas se sente condicionada, devido à vigilância, na sua navegação online uma vez que recusa dar dados e cookies frequentemente. Já sobre o condicionamento da sua vida pessoal fora da Web, a participante afirma não se sentir condicionada atualmente, mas teme que o venha a sentir no futuro. Por outro lado, dois entrevistados (E3 e E4) consideram que uma das consequências atuais da vigilância é um certo condicionamento comportamental que a vigilância provoca nos cidadãos. A natureza duradoura dos dados que são recolhidos, tal como incerteza relativamente à sua utilização, criam algumas preocupações que podem condicionar o comportamento.

> "As pessoas mais e mais ficam a pensar epá não vou fazer isto ou não vou fazer esta tolice porque se calhar tem câmaras a filmar não agem tão normal quando se calhar (…) é uma condicionante às pessoas, e as pessoas já devagarinho começam-se a perceber epá mas afinal se calhar enquanto estou a falar com a minha namorada e se

> calhar a fazer coisas impróprias eu vou tapar a minha webcam (…) e vejo que as pessoas cada vez mais já sentem um bocadinho condicionadas por isso." (E3, masculino, 35 anos, 12º ano + curso técnico (IV) em informática, taxista, Açores).

Em relação às consequências relacionadas com a manipulação de opiniões, algumas entrevistadas (E5; E8; E16) referiram aspetos que podem advir dos processos de vigilância. Estas entrevistadas manifestaram preocupações sobre as suas tomadas de decisão individuais poderem ser manipuladas.

> "(…) não sei é mais um mecanismo para te, para te manter dentro de um grupo que é aquele grupo que é "certo" para ti. É um grupo de poder de compra que é certo para ti, um grupo de pessoas que é certo para ti, um grupo de lazer, de ferramentas, (…) há uma espécie de rede que vai sendo criada e que mantém as coisas no seu lugar, não é?" (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

> "E além disso nós ficamos, muitas vezes, privados de pensar por nós mesmos porque somos influenciados mais facilmente pelos outros, e até de termos as nossas escolhas, (…) elas são cada vez mais influenciadas pela sociedade e por estas tecnologias. Porque isto é uma realidade que é construída em determinado momento, e para determinados objetivos." (E8, feminino, 50 anos, mestrado, técnica superior, Covilhã).

A ameaça que a vigilância pode representar para a autonomia dos cidadãos, sugerida por Simões e Jerónimo (2018), parece constar nos imaginários da vigilância destas respondentes.

Dois entrevistados manifestaram alguma preocupação quanto à vigilância poder potenciar o cibercrime. A existência de uma quantidade significativa de processos de recolha de dados que resultam em bases de dados de grande dimensão, fazem com que, na perspetiva de alguns entrevistados, o potencial acesso às mesmas por parte de hackers ou outras entidades com pretensões criminosas, seja preocupante.

Enquanto o E6 refletiu sobre a possibilidade de um ciberataque numa escala massiva, que pudesse utilizar informação sensível dos cidadãos para efetuar algum tipo de chantagem, o E13 apenas referiu a sua preocupação com a possibilidade de a venda de dados facilitar o cibercrime.

Em relação a consequências que podem afetar o futuro profissional, três entrevistados (E7; E12; E15), refletindo sobre consequências que os pudessem afetar pessoalmente, mencionaram a sua preocupação com estas. Estes entrevistados preocupam-se com a existência duradora de dados que forneceram quando eram mais jovens, e, também, com a possível perda de credibilidade que essas informações possam trazer e com as respetivas consequências para o futuro profissional.

> "Por exemplo, eu nem leio e concordo partilhar informação com um site, e passado muitos anos a informação vem ao de cima e poder ter consequências, consequências

> graves para o futuro profissional de uma pessoa por uma escolha que fez quando era mais nova." (E7, masculino, 20 anos, 12º ano, estudante universitário em medicina, Braga).

> "Pensei mais nisso, não nesse sentido de privacidade, mas no sentido para o futuro. Imaginemos vou para uma empresa, não quero ter as fotos de 2011 em que eu estava no 7º ano a fazer caretas e a pôr porcarias de descrições de rap e coisas assim, isso não quero ter." (E15, masculino, 22, licenciatura, mestrando em relações internacionais, Guarda).

Esta preocupação com o futuro profissional, poderá estar relacionada com a etapa estudantil em que se encontram, tal como a necessidade de manter uma imagem positiva que a futura ocupação profissional pode requerer. A reflexão sobre este tipo de consequências parece estar associada a uma preocupação com o que os seus "Data Doubles", conceito explorado por Haggerty (2006) e Galič, Timan e Koops, (2017), poderão transmitir acerca das suas vidas.

Por último, algumas entrevistadas parecem estar preocupadas com a ameaça que a vigilância pode constituir do ponto de vista de direitos civis, especialmente porque vêm alguns direitos a serem subtilmente retirados ou violados sem que os cidadãos se apercebam.

> "Pronto para mim, acho que isto…altera coisas importantíssimas que foram muito difíceis de conquistar como o direito à privacidade, o direito à liberdade, não é? Esse tipo de direitos que demoraram séculos a conquistar-se, não é? E que nós agora, por parvoíce, como eu agora por exemplo, porque eu ei de ter os dados ligados ou o Wi-Fi, não é? Por causa destas coisas estamos a perder sem nos darmos…sem termos uma consciência se calhar verdadeira disso, e para mim pronto…para mim o valor da liberdade e da privacidade e da democracia e essas coisas todas, são valores supremos, não é?" (E10, feminino, 52 anos, doutoramento, docente no Ensino Secundário, Braga).

> "E isso tem consequências, mas em parte a culpa é nossa, porque eu já posso ter consentido a venda dos meus dados e acho que, não sei se isso é legal, mas posso ter consentido e não faço ideia." (E5, feminino, 23 anos, licenciatura, mestranda em ciência política, Porto).

Apesar da diversidade de consequências identificadas pelos entrevistados, parece haver uma certa similaridade, nas suas perspetivas, relativamente a uma antevisão das consequências futuras serem predominantemente negativas. Algumas obras distópicas sobre a evolução das tecnologias de vigilância, parecem estar presentes nos imaginários da vigilância dos entrevistados, surgindo referências a obras literárias distópicas que abordam as potenciais consequências da vigilância, posteriormente adaptadas para o cinema, como o "Minority Report" e o "1984" de George Orwell. Os resultados desta dimensão parecem estar de acordo com o que Lyon (2018) havia sugerido em relação à importância das obras de entretenimento

na compreensão cultural comum de determinados fenómenos sociais como a vigilância, algo que parece influenciar significativamente os imaginários da vigilância.

Considerações Finais

A noção de vigilância como cultura preconizada por Lyon (2018) remete para a forma como esta se incorporou no nosso quotidiano. Aliada a esta teoria, surgem diversas questões relacionadas com o papel ativo dos cidadãos na vigilância eletrónica. Nesta investigação procurou-se explorar as perceções e práticas que os respondentes têm em relação à vigilância.

Enquanto o Capítulo 4 foi construído de forma a explicitar os principais resultados por cada dimensão de análise, nas considerações finais optou-se por salientar os aspetos mais relevantes em torno dos imaginários e das práticas em relação à vigilância.

Imaginários da Vigilância

Quase todos os respondentes têm consciência da vigilância eletrónica, embora o grau de conhecimento e consciencialização seja diversificado, tendo alguns, conhecimento dos mecanismos mais subtis da vigilância eletrónica. Alguns fatores como a leitura de notícias ou a reflexão sobre a sua navegação *online*, parecem contribuir para esse maior conhecimento. Alguns respondentes ainda estão alheios à sua existência ou confundem-na com o cibercrime. Estes têm algumas semelhanças ao nível sociodemográfico, nenhum frequentou o ensino superior e alguns declararam ter um baixo conhecimento informático.

A vigilância comercial foi o tipo de vigilância mais facilmente identificado por todos os respondentes. A experiência *online*, no caso de vários respondentes, parece ser responsável por esta perceção. Os entrevistados notaram que tanto o *display advertising* como as recomendações\sugestões oferecidas por diversos websites, eram claramente baseadas em dados que só poderiam ser obtidos através da monitorização da sua atividade *online*.

Os respondentes identificam aspetos positivos e negativos deste tipo de vigilância. Como aspetos positivos foram salientados por respondentes os seguintes: as recomendações personalizadas; os incrementos na conveniência da navegação *online* e, por último, as promoções e ofertas especiais que advém da monitorização comercial. Por outro lado, os aspetos negativos identificados foram: a perda de privacidade; o rasto digital da sua vida; a limitação das capacidades de escolha; a potencial manipulação para comprarem mais do que querem e, por último, a discriminação de alguns consumidores. Há respondentes que, apesar de identificarem diversos aspetos negativos, acabam por apreciar a vigilância comercial. Estes pareceram avaliar a situação como uma troca de custo-benefício, onde a cedência dos seus dados traz mais benefícios do que custos. Os respondentes menos informados sobre a vigilância comercial têm maior dificuldade em identificar os seus aspetos negativos.

A vigilância governamental foi menos referida pelos respondentes. Diversos entrevistados revelaram ter menos conhecimento sobre as formas como este tipo de vigilância funciona, nomeadamente sobre os tipos de dados e informações que são recolhidos. Em algumas

entrevistas foi, inclusive, necessário evocar o nome de Edward Snowden de forma a estimular a conversa e reflexão sobre a vigilância governamental. Tal desconhecimento ou desvalorização poderão estar relacionados, por um lado, com o contexto sociocultural português atual já muito distante do fascismo, além de que nenhum entrevistado experienciou, em idade adulta, incómodos relacionados com a vigilância governamental. Por outro lado, a existência de uma sociedade civil fraca e incapaz de alertar a população para a perda de direitos civis, pode levar a que não se consiga sensibilizar a população para assuntos relacionados com este tipo de vigilância. Ao refletir sobre as vantagens e desvantagens deste tipo de vigilância, uns respondentes mencionaram os incrementos na segurança, outros referiram-se ao auxílio para uma melhor governação. Como aspetos negativos alguns apontaram a possível discriminação baseada na etnicidade, outros a manipulação de dados recolhidos para beneficiar a imagem de governos, e quase todos mencionaram a perda de privacidade.

As reflexões em torno dos processos de *social sorting* surgem relacionadas com as perceções sobre a vigilância governamental e comercial. Apesar da diversidade de perceções sobre este tema, vários respondentes mostraram-se mais reticentes em relação à integração do *social sorting* na vigilância governamental quando comparada com a comercial. Estes mostraram-se especialmente preocupados com a imprecisão e a, possível, reprodução ou agravamento de desigualdades sociais provocado pela vigilância governamental.

Um número significativo de respondentes não pareceu associar a vigilância lateral diretamente à vigilância eletrónica. Porventura devido ao facto da hierarquia de poder, neste tipo de vigilância, ser menos acentuada. Porém, para alguns entrevistados, a vigilância tornou-se, de certa forma, numa forma de ver e de ser no mundo, à semelhança do que refere Lyon (2018), dado que vários entrevistados salientaram a importância que as redes sociais podem ter para se manterem em contacto ou informarem-se sobre outras pessoas; embora tenham também a noção de que a exposição voluntária e não cuidada nas redes sociais, os pode prejudicar. Em relação ao condicionamento da sua atividade nas redes sociais, os respondentes dividiram-se em dois grupos: os que não se sentem condicionados e os que se sentem condicionados.

Apesar da diversidade de perceções em relação às consequências da vigilância, houve dois aspetos comuns a quase todos os respondentes: as consequências tenderão a ser cada vez mais negativas e a reflexão sobre a perda de privacidade.

O direito à privacidade tem uma grande importância na formulação dos imaginários da vigilância dos respondentes. As reflexões sobre a privacidade foram notórias no discurso de uma boa parte dos entrevistados em diversas instâncias, nomeadamente quando refletiram sobre: (i) as preocupações com a vigilância; (ii) a valorização da privacidade online; (iii) as consequências da vigilância, e, por último, (iv) os aspetos negativos da vigilância.

Em relação às preocupações com a vigilância, a privacidade foi referida por quase todos os respondentes. Embora para dois, uma preocupação muito forte com a vigilância possa ser facilmente associada a algum tipo de paranoia injustificada.

Notou-se similaridades nas perceções em relação à valorização da privacidade na internet. No entanto, apesar desta perceção, alguns entrevistados referiram que não a conseguem proteger da forma como desejariam. O paradoxo da privacidade, neste contexto, pode ser explicado pela impossibilidade de salvaguardar a sua privacidade na navegação online.

A perda de privacidade, como foi referido anteriormente, surgiu nos imaginários dos respondentes como sendo um aspeto negativo, manifestando-se, nas suas perceções, em todos os tipos de vigilância.

Práticas em relação à vigilância

Quanto às práticas em relação à vigilância, a maioria dos respondentes considerou a cedência de dados pessoais como algo incómoda, evitando cedê-los em situações nas quais aquela não é obrigatória. Um respondente revelou uma perceção divergente das acima referidas, na qual se notou uma clara despreocupação com a cedência dos dados. No fundo notou-se, no discurso de um número significativo de entrevistados, que a cedência é quase sempre semiforçada; os entrevistados prefeririam não ceder os seus dados, porém, se não os fornecerem vêm o acesso barrado a determinados serviços e\ou conteúdos.

Diversos respondentes discordam da venda de dados pessoais, manifestando alguma desconfiança e desconhecimento sobre as formas como a recolha e venda de dados ocorre. Outros respondentes salientaram que não sabiam que os dados pessoais podiam ser vendidos.

A desconfiança aliada a posturas contra uma série de processos envolvidos na vigilância comercial, poderia fazer supor que os respondentes iriam valorizar mais a questão, lendo atentamente as notificações informativas sobre os processos de recolha e transmissão de dados pessoais, algo que não se notou nas suas falas. Apesar de os respondentes declararem, unanimemente, que o consentimento informado é fundamental em todos os processos de recolha de dados, vários confessaram que nunca os leram, o que revela alguma contradição entre os seus discursos e as suas práticas. Porventura dois fatores podem contribuir para a existência da contradição acima referida: a perceção de que os consentimentos são de difícil leitura e a existência de diversos mecanismos que persuadem à sua aceitação sem que o utilizador leia o consentimento na íntegra.

A forma como as notificações para os consentimentos informados são apresentadas aos utilizadores deveria ser alterada. Como foi explorado ao longo do Capítulo 2, as diversas estratégias sofisticadas e subtis que diversas entidades utilizam para persuadir no sentido da concessão dos dados, podem transformar a decisão de dar (ou não) um consentimento informado, num mero clique motivado por conveniência, algo que poderá resultar numa aceitação desinformada. Para que o utilizador não fique numa posição de grande vulnerabilidade perante as notificações de aceitação ou rejeição de cedência de dados, sugere-se que na formulação e apresentação destas, se tenha em conta pelo menos 5 aspetos: (i) a notificação não deve ser muito extensa e a linguagem utilizada deve ser o mais direta e

simplificada possível; (ii) o tipo e tamanho da letra utilizada nos consentimentos não deve dificultar a sua leitura; (iii) no caso de não consentimento, o intervalo de tempo para que a notificação de aceitação/rejeição de partilha de cookies reapareça deve ser maior do que é atualmente; (iv) a quantidade de cliques necessários para a recusa das notificações deve ser igual aos necessários para a sua aceitação, e por último, (v) barrar o acesso a quem não aceitar os *cookies* deve ser proibido ou pelo menos comunicado antes de o utilizador entrar no website.

Apesar da preocupação com a vigilância evidenciada por alguns respondentes, o "pouco" esforço que estes envolvem na leitura das notificações para o consentimento, tal como a aceitação pouco informada, merece uma investigação mais aprofundada.

Quanto à pactuação ou "negociação" da vigilância pode afirmar-se que os respondentes se dividiram fundamentalmente em duas posições: os que sentem um ligeiro incómodo, mas que não se sentem condicionados, e os que se sentem mais incomodados e condicionados. Enquanto o ligeiro incómodo referido por diversos respondentes pode ser, em grande parte, explicado pela ausência de consequências diretas provenientes da vigilância, as causas para o incómodo mais significativas prenderam-se, na perceção de vários entrevistados, com a forma demasiado insistente e intrusiva de recolha de dados para a obtenção de lucros no âmbito da vigilância comercial; outras causas enunciadas por alguns respondentes relacionam-se com o modo pouco claro como a troca de benefícios comerciais por dados pessoais acaba por ocorrer e, ainda, com a invasão da privacidade.

Os entrevistados revelaram utilizar diversas estratégias de neutralização da vigilância já apontadas em estudos realizados noutros países ocidentais, algo está de acordo com o Lyon (2018) afirmou. Os respondentes utilizam estratégias de neutralização, havendo apenas uma entrevistada que não o faz. Apesar da estratégia de recusa ser uma das mais utilizadas pelos respondentes, notou-se que a adoção desta estratégia é difícil de manter devido às consequências que ela tem na sua navegação *online*. Estes acabam por abandonar esta estratégia em consonância com a decisão do esforço menor - a cedência. Outra das estratégias mais comuns foi a que é designada por troca, praticada principalmente através do fornecimento de dados falsos em diversas situações. Importa também destacar que alguns respondentes referiram utilizar estratégias de disfarce, como por exemplo a utilização de VPN's e Proxys. Apesar de estas estratégias serem, porventura, das mais eficazes no combate à vigilância massificada, apenas os respondentes com níveis elevados de conhecimento informático mencionaram utilizá-las.

O contexto e os propósitos da vigilância são fundamentais na forma como os respondentes negoceiam a vigilância, algo que Marx (2015), Kennedy, Elgesem e Miguel (2015) já haviam referido. A sua influência notou-se principalmente nas perceções de diversos respondentes sobre a vigilância comercial e governamental. No âmbito da primeira, vários respondentes compreendem que é necessário recolher alguns dados pessoais para que se concretizem determinados serviços. Porém quando lhes são pedidos dados pessoais, que na sua perspetiva,

não são necessários para a prestação de determinado serviço, sentem-se mais incomodados. Em relação à vigilância governamental, a influência do contexto e dos propósitos observou-se nas respostas de vários respondentes sobre a aceitação e legitimação dos processos deste tipo de vigilância, sendo considerado, por vários, normal e aceitável que os governos recolham dados através dos serviços públicos e que tenham capacidades vigilantes na internet. No entanto, quando alguns respondentes foram confrontados com a existência de processos de vigilância massificados, adotaram perspetivas de uma aceitação mais relutante ou até de desaprovação.

As entrevistas parecem ter provocado uma certa reflexividade sobre as práticas em relação à vigilância. Alguns entrevistados refletiram, parecendo efetuar uma espécie de autoavaliação, sobre a possibilidade de negociarem a vigilância de uma forma mais adequada. Com o decorrer das entrevistas notou-se também que vários entrevistados, com baixos graus de consciencialização sobre a vigilância eletrónica, após refletirem sobre as questões que lhes foram sendo colocadas, manifestaram a sua intenção de adotar uma abordagem mais cuidada com a cedência de dados. Estes resultados salientam a importância de iniciativas levadas a cabo para uma maior consciencialização sobre vigilância eletrónica, para que se possibilite uma tomada de decisão mais informada por parte dos utilizadores.

Importa continuar a investigar as perceções e práticas dos cidadãos em relação à vigilância eletrónica, por várias razões. Em primeiro lugar, em relação ao caso específico desta dissertação, importava caminhar para um leque maior e mais diversificado de entrevistados, o que não foi possível devido a limitações temporais e financeiras. Em segundo lugar, quer as perceções quer as práticas em relação à vigilância estão sujeitas a alterações à medida que novas informações, contextos e/ou tecnologias vão surgindo. Em terceiro lugar, à medida que a atuação das entidades vigilantes se vai alterando no sentido de contornarem a resistência e luta de cidadãos pelo direito à proteção dos seus dados e à sua privacidade, estes por sua vez, vão também modificando as suas práticas no sentido de ultrapassarem a monitorização a que são sujeitos.

Bibliografia

Acquisti, Alessandro, Laura Brandimarte, e George Loewenstein (2015), "Privacy and Human Behavior in the Age of Information", *Science*, 347 (6221), pp. 509–514.

Acquisti, Alessandro, Taylor, Curtis, e Wagman Liad (2016), "The Economics of Privacy", *Journal of Economic Literature*, 54 (2), pp.442-492.

Andrejevic, Mark (2005) "The Work of Watching One Another: Lateral Surveillance, Risk, and Governance", *Surveillance & Society*, 2 (4), pp.479–497.

Andrejevic, Mark (2004), *Reality Tv: The Work of Being Watched,* Nova Iorque, Rowman & Littlefield Publishers.

Arksey, Hilary e Knight, Peter (1999), *Interviewing for Social Scientists*, Londres, SAGE Publications

Augusto, Fábio, and Simões, Maria João (2017), "To See and Be Seen, to Know and Be Known: Perceptions and Prevention Strategies on Facebook Surveillance." *Social Science Information*, 56(4), pp.596–618.

Baek, Young (2014), "Computers in Human Behavior Solving the Privacy Paradox: A Counter-Argument Experimental Approach", *The Journal of Consumer Affairs*, 41(1), pp. 33-42.

Ball, Kirstie, Haggerty, Kevin, e Lyon, David (2012), *Routledge Handbook of Surveillance Studies*, Nova Iorque, Routledge.

Baruh, Lemi (2010) "Mediated Voyeurism and the Guilty Pleasure of Consuming Reality Television", *Media Psychology*, 13(3), pp.201-221.

Bauman, Zygmunt e Lyon, David (2013), *Liquid Surveillance*, Cambridge, Polity Press.

Bloss, William (2007) "Escalating U.S. Police Surveillance after 9/11: An Examination of Causes and Effects.*", Surveillance and Society*, 4 (3), pp. 208–228.

Boyne, Roy (2000), "Post-Panopticism", *Economy and Society,* 29 (2), pp.285-307.

Calo, Ryan (2014), "Digital market manipulation." *Geo. Wash. L. Rev*, 82(4), pp. 996-1304.

Caluya, Gilbert (2010) "The Post-Panoptic Society? Reassessing Foucault in Surveillance Studies", *Social Identities,* 16(5), pp. 621–33.

Chandler, Jennifer (2009), "Privacy Versus National Security Clarifying the Trade-Off" em Ian Kerr, Valerie Steeves e Carole Lucock (orgs.), *Lessons From the Identity Trail: Anonymity, Privacy and Identity in a Networked Society*, Nova Iorque, Oxford University Press.

Crawford, Kate, Lingel, Jessa, Tero, Karppi (2015), "Our Metrics, Ourselves: A Hundred Years of Self- Tracking from the Weight Scale to the Wrist Wearable Device", *European Journal of Cultural Studies*, 18(4-5), pp.479-496.

Daphi, Priska, Lê Anja e Ullrich, Peter (2013), "Images of Surveillance: The Contested and Embedded Visual Language of Anti-Surveillance Protests", *Research in Social Movements, Conflicts and Change*, 35(1), pp.55-80.

Dijck, José V. (2014) "Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology", *Surveillance and Society*, 12(2), pp.197–208.

Elmer, Greg (2012), "Panopticon—discipline—control", em Kirstie Ball, Kevin Haggerty e David Lyon (orgs.), *Routledge Handbook of Surveillance Studies*, Nova Iorque, Routledge, pp.21-29.

Essén, Anna (2008), "The Two Facets of Electronic Care Surveillance: An Exploration of the Views of Older People Who Live with Monitoring Devices." *Social Science and Medicine*, 67 (1), pp.128–136.

Flick, Uwe (2009), *An Introduction to Qualitative Research*, Londres, Sage.

Foucault, Michel (1995), *Discipline and Punish: the birth of the prison,* Nova Iorque, Vintage Books.

Fuchs, Christian (2010), "StudiVZ: Social Networking in the Surveillance Society", *Ethics and Information Technology*, 12(2), pp. 171-185.

Fuchs, Christian (2011), "New Media, Web 2.0 and Surveillance." *Sociology Compass*, 5(2), pp.134–147.

Galič, Maša, Tjerk Timan, e Bert Jaap Koops (2017), "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation." *Philosophy and Technology*, 30(1), pp. 9–37.

Ganascia, Jean-gabriel (2010), "The Generalized Sousveillance Society", *Social Science Information,* 49(3), pp. 489–507.

Gandy, Oscar (1989), "The Surveillance Society: Information Technology and Bureaucratic Social Control.", Journal of Communication, 9(3), pp. 61–76.

Gandy, Oscar (2007), "Data mining and surveillance in the post 9/11 environment", em Sean Hier e Joshua Greenberg (orgs.), *The Surveillance Studies Reader*, Nova Iorque, Open University Press, pp. 147-157

Germain, Séverine (2013) "A Prosperous 'Business': The Success of CCTV through the Eyes of International Literature." *Surveillance and Society,* 11(1–2), pp.134–147.

Giddens, Anthony (1990), *The Consequences of Modernity,* Cambridge, Polity Press.

Giroux, Henry (2015), "Totalitarian Paranoia in the Post-Orwellian Surveillance State", *Cultural Studies*, 29(2), pp. 108-140.

Goffman, Erving (1956), *The Presentation of Self in Everyday Life*, Edimburgo, Universidade de Edimburgo

Gonzalez, Maria e Moraes, João (2014) "Complexidade e Privacidade Informacional: Um Estudo Na Perspectiva Sistêmica." *Coleção CLE*, 66(21), pp.161–180.

Gray, David (2004), *Doing Research in the Real World*, Londres, Sage.

Green, Nicola, e Nils Zurawski (2015), "Surveillance and Ethnography: Researching Surveillance as Everyday Life" *Surveillance and Society*, 13 (1), pp. 27–43.

Gu, Jie et al. (2017), "Privacy Concerns for Mobile App Download: An Elaboration Likelihood Model Perspective." *Decision Support Systems,* 94(1), pp.19–28.

Guerra, Isabel (2006), *Pesquisa Qualitativa e Análise de Conteúdo: Sentidos e Formas de uso*, Lisboa, Principia.

Guzik, Keith (2017), "Seeing a Bigger Picture", *Society*, 54 (4), pp.367–371.

Haggerty, Kevin e Ericson, Richard (2000) "The Surveillant Assemblage" *British Journal of Sociology*, 51(4), pp.605–622.

Haggerty, Kevin D. e Ericson, Richard (2006), "The New Politics of Surveillance and Visibility", em Keven Haggerty e Richard Ericson (eds) *The New Politics of Surveillance and Visibility,* Toronto, University of Toronto Press.

Haggerty, Kevin (2006), "Tear down the walls: on demolishing the panopticon", em David Lyon (org.), *Theorizing Surveillance: The panopticon and beyond,* Willan Publishing, pp.23-45.

Harding, Luke (2014), *The Snowden Files: The Inside Story of the Worlds Most Wanted Man*, Nova Iorque, Vintage Books.

Henderson, Angela C., Harmon, Sandra e Houser, Jeffrey (2010), "A new State of Surveillance? Application of Michel Foucault to Modern Motherhood" *Surveillance & Society*, 7(3-4), pp. 231-247.

Holm, Nicholas (2009), "Conspiracy Theorizing Surveillance: Considering Modalities of Paranoia and Conspiracy in Surveillance Studies", *Surveillance & Society*, 7(1), pp. 36-48.

Hong, Sun-ha, (2017) "Criticising Surveillance and Surveillance Critique: Why Privacy and Humanism Are Necessary but Insufficient", 15 (2), pp. 187-203.

Jansson, André (2012), "Perceptions of surveillance: Reflexivity and trust in a mediatized world (the case of Sweden)", *European Journal of Communication,* 27(4), pp. 410–427.

Jeness, Valerie *et al*. (2007), "Editors' Note: Taking a Look at Surveillance Studies" em Valerie Jeness, David Smith e Judith Stephan-Norris (eds.), *Contemporary Sociology*, 36 (2), pp.VII – VIII.

Kennedy, Elgesem e Miguel (2015), "On fairness: User perspectives on social media data mining", Convergence: The International Journal of Research into New Media Technologies, 23(3), pp. 270-288.

Lauer, Josh (2012) "Surveillance History and the History of New Media: An Evidential Paradigm." *New Media and Society,* 14(4), pp.566–582.

Los, Maria (2006), "Looking into the future: surveillance, globalization and the totalitarian potential", em David Lyon (org.), *Theorizing Surveillance: The panopticon and beyond,* Willan Publishing, pp.23-45.

Lyon, David (1994), *The Electronic Eye: the rise of surveillance society*, Minnesota, Polity Press.

Lyon, David (2003), *Surveillance After September 11*, Cambridge, Polity Press.

Lyon, David (2005), "Surveillance as social sorting: Computer codes and mobile bodies" em David Lyon (ed) *Surveillance as Social Sorting: Privacy, risk, and digital discrimination*, Londres, Taylor and Francis e-Library, pp. 13-30.

Lyon, David (2006), "The Search for Surveillance Studies" em David Lyon (ed), *Theorizing Surveillance: The panopticon and beyond*, Devon: Willan Publishing, pp.3-20.

Lyon, David (2007), " Sociological Perspectives and Surveillance Studies: "Slow Journalism" and the Critique of Social Sorting", *Contemporary Sociology,* 36(2), pp.107-111.

Lyon, David (2009), "Surveillance, power and everyday life" em Avgerou e outros (orgs.), *The Oxford Handbook of Information and Communication Technologies*, Oxford, Oxford University Press

Lyon, David (2014), "Surveillance, Snowden, and big data: Capacities, consequences, critique", *Big Data & Society,* pp.1-13.

Lyon, David (2015) "The Snowden Stakes : Challenges for Understanding" *Surveillance and Society*, 13(2), pp. 139–152.

Lyon, David (2018), *The Culture of Surveillance: Watching as a Way of Life*, Cambridge, Polity Press.

Lyon, David (2019), "Surveillance Capitalism, Surveillance Culture and Data Politics", em Didier Bigo, Engin Isin e Evelyn Ruppert (orgs.), *Data Politics: Worlds, Subjects, Rights*, Nova Iorque Routledge.

Mann, Steve (1998), ""Reflectionism" and "Diffusionism": New Tactics for Deconstructing the Video Surveillance Superhighway", *LEONARDO,* 31(2), pp.93-102.

Mann, Steve, and Joseph Ferenbok (2013), "New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World", *Surveillance & Society*, 11 (1-2), pp.18–34

Marx, Gary (2006), "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information – "Hey Buddy Can You Spare a DNA?"", em Monahan (org.) *Surveillance and Security: Technological Policies and Power in Everyday Life*, Nova Iorque, Routledge.

Marx, Gary (2012), "Your Papers please: personal and professional encounters with surveillance", em *Routledge Handbook of Surveillance Studies*, Nova Iorque, Routledge, pp. XX-XXXI.

Marx, Gary (2015), "Surveillance studies", em *International encyclopedia of the social & behavorial sciences*, 23(2), pp.733-741

Marx, Gary (2016), *Windows into the Soul: Surveillance and Society in an Age of High Technology*, Chicago University Press, Chicago.

McCahill, Michael e Finn, Rachel (2014), *Surveillance, Capital and Resistance,* Londres, Routledge.

Norberg, Patricia, Horne R, David e Horne A, David (2007), "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", *The Journal of Consumer Affairs,* 41(1), pp. 100–126.

Howe, Daniel (2015), "Surveillance countermeasures: Expressive privacy via obfuscation", *Datafied Research*, 4 (1), pp. 1-15.

Hull, Gordon (2015), "Successful Failure: What Foucault Can Teach Us about Privacy Self-Management in a World of Facebook and Big Data.*" Ethics and Information Technology*, 17(2), pp. 89–101.

Marwick, Alice (2010), "I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience", *New Media & Society,* 13 (1), pp. 114-133.

Marwick, Alice (2012), "The Public Domain: Social Surveillance in Everyday Life.", *Surveillance and Society,* 9 (4), pp.378–393.

Mertens, Donna (2018), "Ethics of Qualitative Data Collection", em Uwe Flick (ed), *Sage Handbook of Qualitative Research*, Londres, Sage.

Monahan, Torin (2011), "Surveillance as cultural practice", *Sociological Quarterly*, 52(1), pp. 495–508.

Park, Yong Jin, Jae Eun Chung, e Dong Hee Shin (2018), "The Structuration of Digital Ecosystem, Privacy, and Big Data Intelligence" *American Behavioral Scientist,* 62(10), pp.1319–1337.

Pavone, Vincenzo e Esposti, Sara (2010), "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security", *Public Understanding of Science,* 21(5), pp.556-572

Pridmore, Jason (2012), "Consumer surveillance: Context, perspectives and concerns in the personal information economy" em Kirstie Ball, Kevin Haggerty e David Lyon (orgs.), *Routledge Handbook of Surveillance Studies,* Nova Iorque, Polity

Quivy, Raymond e Campenhoudt, Van (2008), *Manual de Investigação em Ciências Sociais* (5ª ed), Lisboa, Gradiva.

Ragin, Charles (2011), *Constructing Social Research,* California, Sage Publications.

Rapley, Tim (2007), "Interviews", em Clive Seale *et al.*, *Qualitative Research Practice,* Londres, Sage, pp.15-33.

Ritchie, Jane (2003), "The Applications of Qualitative Methods to Social Research", em Jane Ritchie e Jane Lewis (orgs.), *Qualitative Research Pratice: A Guide for Social Science Students and Researchers*, Londres, Sage.

Ritchie, Jane, Lewis, Jane e Elam, Gillian (2003), "Designing and Selecting Samples", em Jane Ritchie e Jane Lewis (orgs.), *Qualitative Research Pratice: A Guide for Social Science Students and Researchers*, Londres, Sage.

Rogers, Richard (2008), "Consumer Technology after Surveillance Theory", em Jaap Koojiman, Patricia Pisters e Wanda Strauven (orgs.), *Mind the Screen,* Amesterdão, Amsterdam University Press.

Roulston, Kathryn (2018), "Qualitative Interviews", em Uwe Flick (ed), *Sage Handbook of Qualitative Research*, Londres, Sage, pp. 233-249.

Rule, James (2007), *Privacy in Peril*, Oxford, Oxford University Press.

Schneier, Bruce (2015), *Data and Goliath: The Hidden Battles to Colect Your Data and Control Your World*, Nova Iorque, W.W Norten & Company, Inc.

Schreier, Margrit (2018), "Sampling and Generalization", em Uwe Flick (ed), *Sage Handbook of Qualitative Research*, Londres, Sage, pp. 84-98.

Rainie, Lee e Madden, Mary (2015), *Americans' Privacy Strategies Post-Snowden*, Pew Research Center, disponível em <http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden>

Simões, Maria e Jerónimo, Nuno (2018), "Rear Window – transparent citizens versus political participation?", em Ann Saetnan, Ingrid Schneider e Nicola Green (eds.) *The Politics of Big Data: Big Data, Big Brother*, Oxford, Routledge

Solove, Daniel (2011), *Nothing to Hide: The False Tradeoff between Privacy and Security*, Londres, Yale University Press.

Stanton, Jeffrey e Weiss, Elizabeth (2000), "Electronic Monitoring in Their Own Words: An Exploratory Study of Employees' Experiences with New Types of Surveillance", *Computers in Human Behavior*,16(4), pp. 423-440.

Steeves, Valerie (2009), "Reclaiming the Social Value of Privacy", em Ian Kerr, Valerie M. Steeves e Carole Lucock (orgs.) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society,* Oxford, Oxford University Press.

Topak, Özgün (2017), "The Making of a Totalitarian Surveillance Machine: Surveillance in Turkey under AKP Rule", *Surveillance and Society,* 15 (3–4), pp. 535–442.

Turow, Joseph, Feldman, Lauren e Meltzer, Kimberly (2005), *Open to Exploitation: American Shoppers, Online and Offline*, Pensilvânia, Public Policy Center of the University of Pennsylvania.

Wood, David M. (2009) "The 'Surveillance Society': Questions of History, Place and Culture." *European Journal of Criminology*, 6 (2), pp. 179–194.

Weller, Toni (2012), "The Information State: An historical perspective on surveillance", em Kirstie Ball, Kevin Haggerty e David Lyon (orgs.), *Routledge Handbook of Surveillance Studies*, Nova Iorque, Routledge, pp. 57-63.

Wottrich, Verena, Reijmersdal, Eva e Smith, Edit (2018), "The Privacy Trade-off for Mobile App Downloads: The Roles of App Value, Intrusiveness, and Privacy Concerns." *Decision Support Systems*, 106(1), pp. 44–52.

Lee, Young-A (2014), "In Insight for Writing a Qualitative Research Paper", *Family and Consumer Sciences Research Journal*, 43 (1), pp.94–97.

Zurawski, Nils (2011), "Local Practice and Global Data: Loyalty Cards, Social Practices, and Consumer Surveillance", *The Sociological Quarterly*, 52 (4), pp.509-527.

Zureik, Elia (2007), " Surveillance Studies: From Metaphors to Regulation to Subjectivity", *Contemporary Sociology*, 36 (2), pp.112-115.

Outras fontes

Agência Lusa (2018), "Facebook multada em 565 milhares de euros pelo escândalo Cambridge Analytica", em *Observador* (25/10/2018), consultado a 22/06/2019, disponível em <https://observador.pt/2018/10/25/facebook-multada-em-560-milhoes-de-euros-pelo-escandalo-cambridge-analytica/>

Agência Lusa (2019), "MP abre inquérito aos incidentes no Bairro da Jamaica", em *Diário de Notícias* (22/01/19), consultado a 18/05/2019 disponível em <https://www.dn.pt/pais/interior/mp-abre-inquerito-aos-incidentes-entre-psp-e-populares-no-bairro-da-jamaica-10470829.html>

Brooker, Charlie (arg.), Foster, Jodie (dir.), (2017), "Arkangel", em Charlie Brooker (criadora), *Black Mirror,* Netflix, temp.4, ep. 02, emitido a 29/12/2017.

Cardoso, Margarida (2019), "PSP abre inquérito à denúncia de violência policial no Bairro da Jamaica", em *Público* (20/01/19), disponível em <https://www.publico.pt/2019/01/20/sociedade/noticia/familia-denuncia-violencia-policial-bairro-jamaica-1858659#gs.i4TeW6ob>

Comissão Europeia (2013), Responsible Research and Innovation (RRI), Science and Technology, Bruxelas, *Comissão Europeia.*

Comissão Europeia (2014), *Ciber Security*, Bruxelas, Comissão Europeia.

Gebel, Meira (2019), "After years of unrelenting privacy scandals, Facebook hires 3 of its fiercest critics", em *Business Insider* (30/01/2019), consultado a 23/06/2019, disponível em <https://www.businessinsider.com/facebook-hires-3-of-its-fiercest-critics-amid-growing-privacy-scandals-2019-1>

Mardisalu, Rob (2019), "VPN Statistics and Usage", em *The Best VPN* (21\03\2019), consultado a 15/09/2019, em <https://thebestvpn.com/vpn-usage-statistics>

Anexos

Anexo 1 - Consentimento Informado

Venho, por este meio, convidá-lo(a) a participar na investigação realizada para a minha dissertação. A minha dissertação, orientada pela Professora Doutora Maria João Simões, está a ser realizada no âmbito do mestrado, "Sociologia: Exclusões e Políticas Sociais" da Universidade da Beira Interior.

O objetivo principal desta dissertação é captar as perceções sobre as práticas em relação à vigilância eletrónica em Portugal. O nosso objetivo passa, fundamentalmente, por perceber o modo como os cidadãos portugueses percecionam e experienciam a vigilância em contexto eletrónico.

De forma a recolhermos os dados necessários para a nossa investigação, pedimos que preencha um pequeno formulário sociodemográfico, e também sua autorização para procedermos à gravação de uma entrevista científica.

Eu, Délcio Otávio Azevedo Faustino, serei responsável pela recolha e tratamento de dados. Importa realçar que a informação que recolhermos será apenas utilizada para efeitos de investigação científica, ser-lhe-á garantido o anonimato e a confidencialidade das suas respostas.

A sua participação tem um carácter voluntário. Por motivos éticos, tem a possibilidade de negar a participação ou de se retirar do estudo a qualquer momento. De acordo com as normas da Comissão Nacional de Proteção de Dados, os dados recolhidos são anónimos e a sua eventual publicação só poderá ter lugar em revistas da especialidade.

Obrigado pela atenção, se desejar participar deve assinar e datar este Consentimento Informado.

Ao assinar este documento confirmo o seguinte:

Compreendi a informação sobre o estudo acima referido, tendo-me sido disponibilizado tempo para refletir sobre a participação, assim como colocar todas as minhas dúvidas. Compreendo que a minha participação é voluntária, que posso desistir a qualquer momento sem dar qualquer justificação e que não irá existir qualquer tipo de remuneração ou custos pela minha participação neste estudo. É-me garantido que sempre que necessitar de algum esclarecimento o mesmo ser-me-á facultado.

Assinatura: _____

Data: _____

UNIVERSIDADE
BEIRA INTERIOR

Anexo 2 - Formulário Sociodemográfico

Número e Localização da Entrevista:

Número da entrevista:

Formulário Sociodemográfico

1. Sexo:

2. Idade:

3. Habilitações literárias:

4. Área profissional/Última profissão:

5. Situação profissional:

6. Local de residência:

Anexo 3 - Guião de Entrevista

Procedimento: Tendo sido explicados os objetivos da investigação e tendo-se obtido o consentimento informado do entrevistado(a), deu-se início à entrevista.

I - Consciencialização dos processos de vigilância

1 - Pensa que podem estar a ser recolhidas informações sobre as pessoas enquanto utilizam a internet? Consegue identificar algumas entidades que o fazem?

II – Cedência de dados pessoais

2- Quando lhe pedem os seus dados pessoais dá-os com facilidade? Porquê?

3 -Dá os seus dados pessoais mais facilmente a entidades públicas ou privadas? Porquê?

4 – Quando estão a ser recolhidas informações sobre si, considera importante que o informem sobre essa recolha? Porquê?

5 – Muita da informação que é recolhida sobre si é vendida, que opinião tem sobre isso?

III - Mecanismos de Recolha

6 - Através de que mecanismos acha possível recolherem dados sobre a sua atividade online? Se possível, enumere e comente alguns

7 - Para além da Internet, que outros modos conhece de recolher informações sobre as pessoas?

8 – Quando se visita por exemplo o Youtube, aparecem frequentemente sugestões de vídeos. Já lhe aconteceu? Porquê que isso acontece?

9 - Acha possível criar-se uma espécie de retrato online, com caraterísticas dos utilizadores, através da recolha de informação online? Porquê? Que consequências pode ter na seu dia-a-dia?

IV - Vigilância Lateral

10 - As redes sociais possibilitam expor muitos aspetos da nossa vida pessoal e pública, qual é a sua opinião sobre isso?

11- É importante, para si, poder ver o que os seus amigos publicam e/ou é publicado acerca deles? Porquê?

V – Vigilância Governamental

12 - Os Governos recolhem informações sobre a atividade online dos cidadãos, que tipo de informação acha que recolhem?

13 - Alguns governos também criam categorias e classificam os seus cidadãos com base na recolha de informação. Com que objetivos acha que o fazem? Deviam fazê-lo?

VI - Aspetos da Vigilância Comercial

14 - Costuma-se fidelizar nas lojas através de cartões, ou outro tipo de fidelização? Porquê?

15 - Já lhe aconteceu procurar um produto disponível para compra na internet, e passado uns dias aparecer-lhe vários anúncios desse mesmo produto durante a sua navegação? Como reagiu?

16 - Deparei-me recentemente com uma notícia no jornal digital denominado "Dinheiro Vivo" cujo título era "Desinstale estas aplicações. Estão a ganhar dinheiro com os seus dados", que opinião tem sobre esta notícia e como reagiria se a encontrasse?

17 - Através da recolha de informações online, algumas empresas conseguem categorizar e classificar os seus consumidores. Este processo tem consequências nas promoções, ofertas ou nos resultados das suas pesquisas. Qual é a sua opinião sobre isso?

VII – Ações de Negociação da Vigilância

18 - Considera ser uma pessoa que valoriza a sua privacidade na internet? Como e porquê?

19 - Alguma vez teve vontade de colocar um "like" ou partilhar alguma coisa nas redes sociais, mas acabou por não o fazer? Porquê?

20 – Alguma vez teve vontade de visitar determinado site ou pesquisar algum tema, mas acabou por não o fazer? Porquê?

21 – No dia-a-dia tem por hábito de usar dispositivos ou aplicações que, por exemplo, que registam informações para o(a) ajudarem a melhorar ou controlar a sua atividade?

22 - Desde que começou a usar a Internet até hoje os seus cuidados na internet alteraram-se? Porquê?

23 - Já alguma vez se sentiu incomodado em relação a algum tipo de recolha de informação a seu respeito? Porquê e em que contexto?

24 - Acha que é possível resistir à recolha de informação temos vindo a falar? Se sim, como?

25 – Quando acede a um *website*, e lhe aparece uma notificação a pedir o consentimento para a recolha dos seus cookies, como reage? Porquê?

26 - Quando decide pesquisar ou utilizar sites que não quer que se saiba que os visitou, que estratégias utiliza? Porquê?

27 - Quando tem de criar uma conta para aceder a conteúdo online, fornece os seus dados verdadeiros? Em que situações e porquê?

28 - Tem o WIFI e o GPS do seu computador portátil ou do telemóvel sempre ligado? Porquê?

29 – Costuma ter a *webcam* do seu portátil tapada? Porquê?

30 - Adota outros tipos de estratégias ou ações, em relação à vigilância, que não tenham sido mencionadas nesta entrevista?

VIII – Perceção sobre as consequências da vigilância

31 - Pergunta final: Se agora refletir um pouco sobre toda a recolha de informação que temos vindo a falar, que consequências acha que pode ter na vida das pessoas? E na sua especificamente? E se pensar no futuro?

Anexo 4 – Sinopses das entrevistas (em suporte digital)