Instituto Universitário de Lisboa

**Departamento de Sociologia**

# A Vigilância nas Sociedades Contemporâneas – O Estudo de Caso do INDECT

**Tiago Manuel Vaz Pinheiro Estêvão**

**Dissertação submetida como requisito parcial para obtenção do grau de Mestre em Comunicação, Cultura e Tecnologias de Informação**

**Orientadora**
**Doutora Rita Maria Espanha Pires Chaves Torrado da Silva**
**Professora Auxiliar – ISCTE - Instituto Universitário de Lisboa**

**Setembro de 2014**

## AGRADECIMENTOS

À minha orientadora de mestrado Doutora Rita Espanha, Professora Auxiliar do ISCTE-IUL, pela sua aplicada orientação, inesgotável paciência e empenhada motivação. Uma inspiração e uma referência pela sua dedicação enquanto docente de mestrado e orientadora de dissertação.

À Ni Cunha pelo inextinguível apoio e motivação. Pelas condições propiciadas em família, por suportar as ausências e os humores. Pelo amor e pela amizade.

À família, essencialmente tios e cunhados, pelo auxílio prestado na coordenação dos horários das aulas de mestrado com as recolhas da Alice no Jardim de Infância.

Por fim à minha filha Alice, pela inspiração, por me levar a perseguir e a concretizar sonhos.

## DEDICATÓRIA

Aos meus pais Alice e Ilídio, por toda a sabedoria e amor. Por todos os valores transmitidos e pela valorização da educação e do saber.

À Ni pelo amor, suporte e motivação nos momentos menos fáceis. Por possibilitar fazer “milagres” em família.

À minha filha Alice pela diária dosagem de inspiração, pelo barulho, pelo desassossego, pelas rotinas e alegrias diárias, pelos sorrisos e amor incondicional.

## RESUMO

Esta dissertação focaliza-se no tema da vigilância na sociedade contemporânea e encontra-se organizada em cinco capítulos principais. As temáticas em análise são essencialmente: a contextualização e a conceptualização da vigilância; a vigilância na sociedade contemporânea; o retrato da vigilância em Portugal; e o estudo de caso do projeto de investigação europeu - INDECT. O estudo do INDECT pressupõe a concreta identificação das opções metodológicas empregues em análise e a correspondente fundamentação teórica, realizada por uma pesquisa documental e por entrevistas suporte.
**Palavras-Chave:** Vigilância, Sociedade em Rede, Poder, Panótico, Privacidade.

## ABSTRACT

This dissertation focuses on the theme of surveillance in contemporary society is organized into five main chapters. The themes in question are essentially: the contextualization and conceptualization of surveillance; surveillance in contemporary society; portrait of surveillance in Portugal; and the case study of the European research project - INDECT. The study of INDECT presupposes the practical identification of methodological choices employed in analysis and the corresponding theoretical foundation, conducted by documentary research and support interviews.
**Keywords:** Surveillance, Network Society, Power, Panoptic, Privacy.

ÍNDICE


Agradecimentos ii

Dedicatória iii

Resumo iv

Abstract iv

1. Introdução 1

2. A Vigilância 4

2.1. Da Sociedade Disciplinar à Sociedade de Controlo: As Teorias Modernas e Pós Modernas da Vigilância 4

2.2. O Novo Panótico da Sociedade em Rede 6

2.3. A Sociedade de Risco e o Pânico Moral 7

2.4. A Privacidade e a Literacia 9

2.5. A Democratização da Vigilância 12

3. A Sociedade Vigilante 12

3.1. Os Panóticos da Sociedade Contemporânea 12

3.2. Retrato da Vigilância em Portugal 19

3.3. O Caso do INDECT 24

4. Opções Metodológicas 26

5. O Projeto INDECT e a sua Fundamentação Teórica 29

6. Conclusão 40

Bibliografia 46

Anexos I

# 1. INTRODUÇÃO

"BIG BROTHER IS WATCHING YOU" (Orwell, 1949: 7).

A citação anterior do romance ficcional *1984* de George Orwell, é o *slogan* do ditador Big Brother do império da Oceânia, e é representativo de uma sociedade onde um Estado totalitário assegura o seu poder através de uma constante vigilância por parte das autoridades.

A obra editada no período pós II Guerra Mundial, no ano de 1949, é inspirada na visão de Orwell dos Estados totalitários da época e é uma metáfora sobre o poder e as sociedades modernas. O *slogan* referido democratizou-se e é atualmente imagem e referência a Estados Governo controladores e invasivos dos direitos dos indivíduos.

A mesma referência ao imortal personagem Big Brother, de Orwell, é mediatizada através de um *reality show* televisivo com o mesmo nome, com projeção a nível internacional e onde os concorrentes estão isolados do mundo exterior e constantemente monitorizados através de um circuito fechado de televisão.

Nunca em tempo algum a vigilância foi alvo de tanta atenção, tão fomentada, tão discutida, analisada ou criticada. Enquanto prática, identificada por David Lyon (1994), a vigilância perpetrada por um Estado ao seu povo remonta ao antigo Egito, com o escrutínio das populações, através de censos, com finalidades de cobrança de impostos e de recrutamento de homens para exércitos. Atualmente a vigilância assume inúmeras e variadas facetas e disseminações, sendo realizada com a mesma finalidade de escrutínio de populações pelo Estado (agora com distintos intuitos e justificações dos apresentados anteriormente e que desenvolveremos mais à frente); para identificação de consumos por parte de entidades empresariais; ou ainda para averiguação de produtividade de empregados por empregadores (Lyon, 1998). O surgimento da Internet e posteriormente da Web 2.0 propiciou e estimulou a vigilância em todas as perspetivas identificadas anteriormente e concebeu outras, como a Vigilância Lateral (Andrejevic, 2007).

A par da evolução e propagação de métodos e sistemas de vigilância, surgem e multiplicam-se os estudos de vigilância que teorizam acerca das suas implicações e metodologias. Os estudos de vigilância encetados por autores como Michel Foucault

(1977), referenciando o Panótico[1], são ainda hoje uma referência incontornável para os estudiosos das ciências sociais.

A evidenciada disseminação da vigilância na sociedade contemporânea, nas suas mais diversas e distintas aplicabilidades em ambientes *online* e *offline*, acompanhada das céleres e constantes inovações tecnológicas, levam ao surgimento de novos paradigmas de vigilância. O Pânico Moral (conceito que desenvolveremos mais à frente) induzido por governantes e *media* numa Sociedade de Risco (conceito que desenvolveremos mais à frente), legitimam e incentivam a monitorização. Intrínseco ao fenómeno da vigilância, e resultante dele, propagam-se revelações de vigilância massificada, difundida e com implicações à escala mundial. Revelações como as realizadas por Edward Snowden, em junho de 2013, comprometendo Estados Governo e empresas multinacionais, são indiciadoras de um contexto de permeabilidade e ilícita convivência entre poder político e poder económico. Em suma, a atual conjuntura fomenta e viabiliza o surgimento de estudos de vigilância. A presente dissertação tem a seguinte estruturação:

Numa fase inicial da dissertação (Capitulo 2) efetuaremos uma revisão de literatura, tendo como base a correlação das seguintes áreas temáticas abordadas: as Teorias modernas e pós modernas da vigilância; o novo Panótico da Sociedade em Rede; a Sociedade de Risco e o Pânico Moral; a privacidade e a literacia. Por fim analisaremos a democratização da vigilância no contexto da sociedade contemporânea.

No capítulo seguinte (Capítulo 3), designado de - A Sociedade Vigilante, analisaremos os múltiplos e complexos panóticos existentes na sociedade contemporânea; realizaremos um retrato, de contextualização, da vigilância em Portugal; e por fim apresentaremos e decomporemos o projeto de investigação do INDECT (o estudo de caso considerado em dissertação).

Nos dois capítulos subsequentes (Capítulos 4 e 5), abordaremos as opções metodológicas consideradas no estudo do INDECT e a sua fundamentação teórica.

Por fim, no último capítulo (Capítulo 6), realizaremos um conjunto de notas conclusivas face ao novo paradigma da vigilância no panorama internacional,

[1] Termo utilizado para designar um estabelecimento prisional ideal, desenhado pelo filósofo Jeremy Bentham, em 1785. O conceito do desenho permite a um vigilante observar todos os prisioneiros sem que estes possam saber se estão ou não sendo observados. Michel Foucault, na sua obra *Vigiar e Punir: Nascimento da Prisão* (Foucault, 1977), viria a associar este termo a uma sociedade altamente disciplinar e vigiada.

evidenciando o contexto de programas e projetos europeus com finalidades de supervisão e monitorização dos cidadãos (como é exemplo o projeto INDECT).

O objetivo primordial do estudo em dissertação é o de produzir conhecimento, no que concerne ao entendimento, de qual o papel de projetos de investigação europeus (como o INDECT), vocacionados para a vigilância, no contexto atual português e europeu.

## 2. A VIGILÂNCIA

### 2.1. Da Sociedade Disciplinar à Sociedade de Controlo: As Teorias Modernas e Pós Modernas da Vigilância

Ao abordar o fenómeno complexo da vigilância na sociedade contemporânea, torna-se essencial logo de início tentar defini-la enquanto conceito, e contextualizá-la considerando as Teorias Modernas e Pós-Modernas.

São vários os autores que ao longo dos tempos teorizam acerca da vigilância, das suas condicionantes, evoluções e implicações (Foucault, 1977; Giddens, 1985; Deleuze, 1992; Lyon, 1998; Staples, 2000; Mann, 2003; Andrejevic, 2007; Albrechtslund, 2008; Fonio, 2008; Fuchs, 2011; Trottier, 2012).

> "Nos tempos modernos, a vigilância apareceu como parte da economia política do capitalismo (Marx), como um produto da organização burocrática (Weber) e como uma mudança de punição e espetáculo para a autodisciplina (Foucault)" (Lyon, 2007: 4)[2].

Anthony Giddens compreende a vigilância como uma atenção rotineira, focada e sistemática, com vista à recolha de dados, com o fim último de influenciar, gerir, proteger ou dirigir indivíduos. Esta monitorização não é aleatória, nem ocasional, nem espontânea. É deliberada e depende de protocolos e técnicas (Giddens, 1985).

Por sua vez David Lyon entende a vigilância como:

> "Qualquer recolha e tratamento de dados pessoais, seja identificável ou não, para fins de influenciar ou gerir aqueles cujos dados foram acumulados" (Lyon, 2001: 2).

O mesmo autor, David Lyon, identifica dois tipos de Teorias da Vigilância, as Modernas (de uma Sociedade Disciplinadora) e as Pós-Modernas (de uma Sociedade de Controlo) (Lyon, 2001). Desta forma:

> "A teoria de vigilância moderna relaciona-se com os tratamentos clássicos que entendem a vigilância como uma consequência de empresas capitalistas, a organização burocrática, o Estado-nação, a tecnologia maquinal e o desenvolvimento de novos tipos de solidariedade, envolvendo menos confiança ou pelo menos diferentes tipos de confiança" (Lyon, 2001: 109)[3].

[2] Tradução livre.
[3] Tradução livre.

Michel Foucault, na sua conceção de Panótico, associa a vigilância a locais fechados, onde o indivíduo está confinado, como por exemplo as prisões, os asilos, os hospitais, as escolas ou os locais de trabalho (Foucault, 1977).

> "O panotismo é o princípio geral de uma nova "anatomia política" cujo objeto e fim não é a relação de soberania mas a relação de disciplina" (Foucault, 1977: 197).

Com esta afirmação, identificada na obra *Vigiar e Punir: Nascimento da Prisão* (Foucault, 1977), o autor defende que os métodos tradicionais de soberania mudaram, reformulando a anatomia política e baseando-se essencialmente em mecanismos disciplinadores. Foucault distingue esta nova forma de soberania dominante como não fazendo uso da força física, mas da vigilância.

Foucault, na sua análise de poder (Foucault, 1977), considera três mecanismos: os Suplícios, as Disciplinas e a Biopolítica. Segundo o autor, o primeiro mecanismo de poder - os Suplícios - decorreu até ao final do século XVIII e refere-se a punições físicas contra o indivíduo (torturas, humilhações, entre outras). Os outros mecanismos de poder – as Disciplinas e a Biopolítica – surgem no início do século XIX e vão até à contemporaneidade. As Disciplinas aplicam-se aos indivíduos, definindo modelos de comportamento padronizados. As Disciplinas são efetivadas a partir de uma vigilância ilimitada, permanente, exaustiva e indiscreta – o Panótico (Motta, Alcadipani, 2004); por sua vez o mecanismo da Biopolítica aplica-se não a um indivíduo particular, mas a um grupo de indivíduos (comunidade, população), não tem um fundamento disciplinador mas sim de formação de conduta, definindo instrumentos de regulamentação e de segurança. Este mecanismo é característico dos Estados Governo (Motta, Alcadipani, 2004). É possível afirmar que ambos os mecanismos de poder são verificáveis na sociedade contemporânea (Estêvão, 2014). As Disciplinas e o Novo-Panótico, como sustentado nas Teorias Pós-Modernas da Vigilância (vigilância disseminada e sem estar confinada a espaços fechados). A Biopolítica, por sua vez, é verificável através da definição do que é aceitável e "normal"; imposto por quem governa à sua comunidade, robustecendo o poder, por exemplo através de regulamentação.

Assim:

> "A teoria de vigilância pós-moderna lida com novas formas de vigilância e visibilidade, é caracterizada por ter um elevado componente de base

tecnológica, por ser realizada diariamente e disseminada espacialmente" (Staples, 2000: 11)[4].

Autores como Gilles Deleuze (1988, 1992) inicialmente, e mais tarde como Mark Andrejevic (2007) e Anders Albrechtslund (2008), teorizam e defendem o oposto às referidas Teorias Modernas das Sociedades Disciplinadoras, expressando que esses espaços fechados de confinamento já não são os únicos ou os principais locais de vigilância, existindo inúmeros instrumentos e modelos de vigilância agora em prática (videovigilância, sistemas biométricos, monitorização por hábitos de "consumos" *online*, entre outros) (Estêvão, 2014). Estas Teorias Pós Modernas da Vigilância são pois caracterizadoras das Sociedades de Controlo.

Gilles Deleuze, na sua definição de Sociedade de Controlo (Deleuze, 1992), identifica o desenvolvimento das tecnologias de informação como as responsáveis da passagem de uma Sociedade Disciplinadora para uma Sociedade de Controlo. A recolha e o registo de informações pessoais passa a ser um instrumento de controlo privilegiado para entidades governamentais e empresariais, com fins de controlo de segurança e policiamento e de *marketing*.

A Sociedade de Controlo, com as suas Teorias Pós Modernas da Vigilância, está intrinsecamente ligada à Sociedade em Rede, como veremos de seguida.

## 2.2. O Novo Panótico da Sociedade em Rede

O surgimento da Sociedade em Rede robusteceu a multiplicidade de interpretações divergentes na teorização de vigilância. Definindo primeiramente Sociedade em Rede:

> "…em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentadas na microeletrónica e em redes digitais de computadores que geram, processam e distribuem informação a partir de conhecimento acumulado nos nós dessas redes. […] É um sistema de nós interligados" (Castells, Cardoso, 2005: 20).

Interpretações antagónicas surgem igualmente referentes à vigilância na Sociedade em Rede. Assim, autores como Manuel Castells (2001), Joseph Turow (2005; 2006) ou Mark Andrejevic (2002) defendem nas suas premissas a ideia de vigilância na Internet com base no Panótico. Ou seja, consideram a vigilância *online*

[4] Tradução livre.

negativa, evidenciando, como aspetos inerentes o seu poder de dominação, controlo e disciplina.

Pelo contrário, autores como David Lyon (1998; 2003), Hille Koskela (2004), Anders Albrechtslund (2008), defendem a vigilância na Internet como distante das noções do Panótico. Ou seja, a vigilância *online* não possuí um papel coercivo, identificando-se-lhe características positivas (ou neutras), evidenciando-se o seu papel funcional e lúdico.

David Lyon, na sua obra *The World Wide Web of Surveillance* (Lyon, 1998), distingue três formas principais de vigilância na Internet: A (1) Vigilância pela Entidade Patronal – que se distingue pela monitorização, por parte das entidades empregadoras, dos hábitos e rotinas *online* dos empregados, com o fim último do aumento da produtividade de tipo Taylorista (Fuchs, Boersma, Albrechtslund and Sandoval, 2011); A (2) Vigilância de Segurança e Policiamento – perpetrada pelos Estados Governo, que proliferou após os ataques terroristas de 11 de setembro de 2001, que privilegia políticas de controlo e supervisão, com vista a reinstalar um sentimento de segurança (Lyon, 2007; Frois, 2011); Por fim, o autor apresenta a (3) Vigilância com Fins Comerciais e *Marketing* – onde surgem as redes sociais *online* (Web 2.0), recolhendo de forma massiva dados de utilizadores, analisando, classificando e definindo tipologias de consumidor, avaliando os seus interesses e associando-os a determinados consumos e a campanhas de *marketing* pré-definidas (Fuchs, 2008, 2011).

Mark Andrejevic acrescentou às três formas principais de vigilância na Internet, avançadas por David Lyon, uma nova forma de designar vigilância que nomeou como - (4) Vigilância Lateral - que se desenvolve essencialmente na Web 2.0 (Andrejevic, 2007) e onde todos somos controladores e assumimos o papel de *Little Brothers*[5] (Estêvão, 2014). Desta forma consensual, modelo a que o autor Reginald Whitaker designa de “Panótico Participativo” (Whitaker, 1999), todos vigiam e todos são alvo de vigilância.

## 2.3. A Sociedade de Risco e o Pânico Moral

"O conceito de Sociedade de Risco é relevante para o desenvolvimento de

[5] Expressão resultante de uma outra, Big Brother, referente à obra *1984* de George Orwell e que pretende definir uma vigilância entre pares (*peer-to-peer*).

explicações resultantes da ansiedade dos Pânicos Morais" (Thompon, 1998: 21-22)[6].

As sociedades ocidentais contemporâneas vivem, após os atentados de 11 de setembro de 2001 nos EUA, num contexto regido pelo medo e pela insegurança (Beck, 2002)**.** Ulrich Beck, em *The Terrorist Threat – World Risk Society Revisited* (Beck, 2002), defende que os atentados levaram a um completo colapso na linguagem, como a conhecíamos até então. O autor sustenta que desde aquele momento, desde a implosão das torres gémeas que o entendimento de conceitos como - segurança, terrorismo ou guerra - mudaram radicalmente. Os atentados de 11 de setembro de 2001 expressam, também de forma simbólica, e são ponto fundamental no século XXI, na definição da nossa sociedade como uma Sociedade de Risco (Beck, 2002)**.**

> "Há uma perspetiva sinistra para o mundo após o 11 de setembro. É que o risco incontrolável é agora irremediável e profundamente estruturante de todos os processos que sustentam a vida em sociedades avançadas. O pessimismo parece ser a única atitude racional " (Beck, 2002: 46)[7].

Neste contexto, o autor faz ainda referência a um conjunto de seis lições que se podem retirar dos acontecimentos de 11 de setembro de 2001. Destacamos assim, duas das seis lições evidenciadas por Ulrich Beck (2002). A primeira lição é que, segurança nacional já não é segurança nacional. As novas alianças globais dos Estados-nação modernos têm como finalidade a preservação da segurança interna e não da externa. Existe atualmente uma política de cooperação transnacional relativamente à segurança interna e externa. A segunda lição é que acontecimentos como os atentados de 11 de setembro de 2001, alimentados e fundamentados pelo Pânico Moral (conceito que analisaremos de seguida), levam ao desenvolvimento de "Estados Nação Fortaleza" onde a anteriormente referida cooperação transnacional de segurança leva a construir "Estados Nação de Vigilância", a dinamizar políticas de supervisão e controlo e a pôr em causa liberdades democráticas" (Beck, 2002 citado por Estêvão, 2014: 163-164).

O conceito de Pânico Moral é sustentado por Stanley Cohen, na sua obra *Folk Devils and Moral Panics* (Cohen, 1972). O Pânico Moral é definido pelo autor como um sentimento intenso, expresso numa população sobre um qualquer tema que pareça ameaçar a ordem social (Estêvão, 2014).

[6] Tradução livre.
[7] Tradução livre.

Outros autores, como Dawn Rothe e Stephen Muzzatti, tecem considerações específicas acerca do conceito de Pânico Moral, resultante do terrorismo, na sociedade norte americana (Rothe, Muzzatti, 2004). Os dois autores sustentam que a sociedade atual tem sido inundada de informações, imagens e depoimentos distorcidos e exagerados, difundidos pelos *media* e pela classe política, capazes de fomentar o Pânico Moral e um sentimento de insegurança e medo generalizado, a um nível planetário (Estêvão, 2014). No seu estudo acerca das implicações do Pânico Moral nos EUA, após os atentados terroristas de 2001, consideram que surgiram informações inexatas e distorcidas referentes à gravidade da situação (número de pessoas que participaram, número de vítimas, danos e efeitos dos atentados) (Rothe, Muzzatti, 2004). Um outro autor, Kenneth Thompson, na sua obra *Moral Panics* (1998), implica da seguinte forma os *media* na disseminação do Pânico Moral:

> "Os *media*, especialmente, não necessariamente conscientes geram um Pânico Moral com a intenção de desviar a atenção de problemas económicos. Estes problemas criam tensões e os *media* respondem ampliando os sintomas das mesmas tensões, como os receios a uma quebra na lei e na ordem" (Thompson, 1998: 19)[8].

Desta forma, associando os dois conceitos desenvolvidos:

> "A Sociedade de Risco em que vivemos atualmente, alimentada por um Pânico Moral dirigido à população pela classe política e pelos *media*, leva à proliferação e legitima a supervisão e o controlo, por parte do Estado" (Estêvão, 2014: 164).

## 2.4. A Privacidade e a Literacia

> "Exigimos o reconhecimento do nosso direito à privacidade, queixamo-nos quando a privacidade é invadida, encontramos dificuldades quando tentamos explicar o que se entende por privacidade, em que áreas, qual o seu conteúdo, o que constitui uma perda de privacidade, uma perda para o que temos consentido, uma perda justificada, uma perda injustificada" (McCloskey, 1985 citado por Tavani, 2008: 131)[9].

É difícil, como se verifica pela explicação de H.J. McCloskey, definir claramente privacidade enquanto conceito, pelos distintos significados e sentidos que pode possuir perante distintos sujeitos.

[8] Tradução livre.
[9] Tradução livre.

Em 1890, nos EUA, Samuel Warren e Louis Brandeis definiam privacidade no texto *"The Right to Privacy"* como "*the right to be let alone*" (Warren, Brandeis, 1890: 193).

Anos mais tarde, Alan Westin define-a do seguinte modo:

> "Privacidade é a alegação de indivíduos, grupos ou instituições de determinar por si mesmos quando, como e em que medida a informação sobre eles é comunicada aos outros" (Westin, 1967: 7).

A vigilância e o constrangimento que provoca no sentimento de privacidade dos cidadãos é hoje um tema em discussão, muito mediatizado pelos meios de comunicação social. São exemplo, as inúmeras e sempre presentes ferramentas ao serviço da vigilância, em ambiente físico e digital, que compõem a sociedade atual. Mais à frente realizaremos um retrato do complexo fenómeno da vigilância na sociedade contemporânea (3.1. Os Panóticos da Sociedade Contemporânea).

Com o surgimento da Sociedade em Rede prospera a partilha de informação *online* por parte dos utilizadores das redes sociais. A vigilância deixa de ser um benefício exclusivo de quem detém poder - de poucos a vigiar muitos, e passa cada vez mais a ser um fenómeno descentralizado - de muitos a vigiar muitos.

Steve Mann introduz o conceito de - *Sousveillance* (Mann, 2003), que identifica um fenómeno novo em que aqueles que geralmente são alvo de vigilância, passam a vigiar.

> "A maioria das pessoas não tem consciência de como os dispositivos e aplicações mais familiares que usa comprometem a sua privacidade" (O'Hara, Shadbolt, 2009: 206).

Caso paradigmático, exemplificativo da escassa consciencialização dos cidadãos relativamente à definição de políticas de privacidade, é o referente ao uso de redes sociais digitais (Web 2.0), de onde evidenciamos o Facebook. Um relatório disponibilizado pelo próprio Facebook e difundido pelos *media* divulgava que só nos EUA, em 2012, 13 milhões de utilizadores nunca tinham feito qualquer tipo de configuração de privacidade.

É neste contexto que se evidencia a literacia digital, que capacita os indivíduos de registarem *online* os seus desempenhos, assegurando o pleno conhecimento da informação que pertence à esfera pública e à esfera privada. A literacia digital torna-se hoje essencial para quem se move na Sociedade em Rede, nomeadamente no entendimento dos vários ambientes *online*, na gestão de definições de utilizador, e na proteção de dados pessoais (Buck, 2012).

Thomas Levin, que desenvolveu uma definição correlacionando diretamente literacia e vigilância, explica:

> "Central à alfabetização da vigilância é o desenvolvimento de uma sensibilidade pedagógica face à mesma, onde se desenvolvem literacia e aptidões para percecionar a vigilância nas suas inúmeras manifestações" (Levin, 2010: 191)[10].

Cada vez mais, na sociedade contemporânea, as redes sociais se assumem como práticas quotidianas de alfabetização, no sentido que desempenham um cada vez mais importante papel na forma como se interage com outras pessoas. As referidas práticas de alfabetização, que decorrem na Web 2.0, têm implicações tanto na vida *online* como *offline* dos utilizadores (Buck, 2012).

As vantagens são evidentes para aqueles que digitalmente literatos usufruem de tecnologia e a utilizam confortavelmente nas mais variadas dimensões, seja no campo da vida social ou no campo da vida profissional (Borges, Oliveira, 2011).
Segundo as mesmas autoras:

> "No âmbito do desenvolvimento democrático, a Unesco vem defendendo a educação digital como parte da formação de qualquer cidadão, em qualquer nação, no sentido de fomentar o direito à informação e a liberdade de expressão como instrumentos de construção e sustentação democrática" (Borges, Oliveira, 2011: 292).

A correlação entre privacidade e literacia torna-se incontornável na Sociedade em Rede. A info-exclusão (*digital divide*), seja pelo desigual acesso às tecnologias de informação, seja pela desigual literacia na utilização das mesmas tecnologias, tem repercussões evidentes ao nível da transmissão da informação e na comunicação, originando uma maior propensão ao controlo e monitorização. No ecossistema da Web 2.0 torna-se indispensável um lúcido entendimento dos vários ambientes *online*, nomeadamente na gestão de acordos de utilizador e de dados pessoais (Buck, 2012). Simplista, redutor e até ingénuo seria adiantar a literacia como base exclusiva e conclusiva na proteção da privacidade. O autor James Rule adianta:

> "Se não há de facto limites naturais para o crescimento da vigilância, sérios esforços para proteger a privacidade só podem surgir através de limites auto conscientemente criados pela invenção humana. Mas os princípios que podem servir para orientar tais limites, provaram ser difíceis de definir" (Rule, 2007: 22)[11].

[10] Tradução livre.
[11] Tradução livre.

Aquando dos argumentos conclusivos, retomaremos este tema.

## 2.5. A Democratização da Vigilância

A sociedade atual atravessa momentos de transformação significativa (Castells, Cardoso, 2005). Teorias surgem, sustentadas por diversos autores, de eventuais sinais de desagregação dos modelos sociais vigentes ao longo do século XX e que levam ao colapso dos pilares tradicionais da sociedade, como a família ou os modelos da democracia representativa (Castells, Cardoso, 2005).

Os modelos de democracia representativa são pouco adaptados à Sociedade em Rede, tornando-se premente por parte dos governantes responsáveis a apropriação de eficazes canais de comunicação. Parece pois urgente, por parte das entidades governativas, a utilização (domesticação) de ferramentas digitais com a finalidade de melhorar a comunicação entre a classe política e o cidadão (Cardoso, Nascimento, Morgado, Espanha, 2005).

Ainda segundo os autores inicialmente referenciados, talvez não esteja esta sociedade condenada à desintegração, mas sim se esteja perante um processo de rutura com um anterior paradigma de sociedade, levando ao surgimento de outro modelo, baseado numa estrutura social redefinida (Castells, Cardoso, 2005).

Enquanto modelo de sociedade em transformação tem na Internet e nos *mass media* as suas ferramentas de socialização. Este novo paradigma de reconstrução social pressupõe um cada vez maior número de indivíduos, unidos em rede.

A sociedade unida em rede é cada vez mais uma constatação na sociedade atual. Indissociável ao fenómeno da Sociedade em Rede surge a monitorização e a vigilância. A Internet é hoje alvo de profunda vigilância, despoletada por inúmeros interesses e efetivada por inúmeros intervenientes. O novo paradigma da vigilância, como veremos no capítulo seguinte, está cada vez mais omnipresente na sociedade contemporânea.

# 3. A SOCIEDADE VIGILANTE

## 3.1. Os Panóticos da Sociedade Contemporânea

Nunca, desde o período da Guerra Fria[12], a vigilância foi tão disseminada e global como é atualmente. Mark Andrejevic (2007) evidencia, como ponto de distinção

[12] Período histórico de disputas estratégicas entre os EUA e a União Soviética, compreendendo o período entre o final da Segunda Guerra Mundial (1945) e a extinção da União Soviética (1991).

entre o período da Guerra Fria e o posterior período apelidado de Guerra ao Terror[13], como o surgimento da envolvente digital e do consequente monitoramento disseminado. Segundo o autor existe, na atual sociedade, um generalizado consentimento à presença de práticas de vigilância, nas suas mais distintas facetas. Resultantes dos dois períodos distinguidos surgem projetos e programas de vigilância (e espionagem) como o Echelon[14] e o Prism. O último referenciado desenvolveremos mais à frente.

David Lyon, elaborando um retrato do fenómeno da vigilância, refere que falar de uma vigilância a nível global, embora possa parecer um ato manifestamente conspirativo, é resultado sobretudo de uma sociedade contemporânea com processos económicos e políticos globalizados (Lyon, 2007). Segundo o mesmo autor, o fenómeno da vigilância na sociedade contemporânea e dos seus multifacetados panóticos é hoje envolto em complexos e intricados enredos (Lyon, 2007).

A denominada, por Catarina Frois, de sociedade vigilante (Frois, 2008), proliferou após os ataques terroristas de 11 de setembro de 2001. Com estes ataques desenvolveu-se uma crescente cultura de medo, que se instalou após o sucedido, suscitando uma consequente reação por parte dos Estados Governo, com vista a reinstalar um sentimento de segurança (Frois, 2011; Lyon, 2007).

Os atentados perpetrados pela Al-Qaeda, organização terrorista fundamentalista islâmica, introduziram um sentimento generalizado de insegurança mundial e levaram à reformulação, em alguns países por completo, dos sistemas de segurança e defesa nacional.

A segurança é hoje tida como uma prioridade em países como os Estados Unidos da América, Reino Unido ou Espanha que tendo sido alvo da "Jihad"[15], através de atentados terroristas, elaboraram sofisticados sistemas de vigilância. Após os atentados legitimaram-se por parte de muitos governos, e sem grande oposição, medidas e procedimentos de vigilância e controlo à escala mundial (Beck, 2002; Andrejevic, 2007; Rule, 2007; Salter, 2008).

No decorrer das ações terroristas ocorridas, por exemplo, em Nova Iorque (2001), Madrid (2004), Londres (2005), Boston (2013) e Volgograd (2013) e outros acontecimentos de foro criminal como os crimes contra pessoas (nomeadamente massacres) que se verificaram em Columbine (EUA, 1999), na Ilha de Utoya (Noruega, 2011) e em Newtown (EUA, 2012), ou ainda crimes contra o património

[13] Iniciativa militar despoletada pelos EUA, a partir dos ataques de 11 de setembro de 2001.

[14] Projeto secreto de espionagem dos anos 80, que fazia a interceção mundial de comunicações através de palavras-chave. Era encabeçado pelos EUA (NSA) e tinha a participação do Reino Unido, Canadá, Austrália e Nova Zelândia.

[15] Significa "esforço" em árabe. No Ocidente é muitas vezes sinónimo de Guerra Santa.

(nomeadamente tumultos) que se verificaram em Paris (França, 2005, 2009), em Londres (Reino Unido, 2011), e em Estocolmo (Suécia, 2013) e sob o pretexto de proteger os cidadãos de ameaças de criminalidade e terrorismo, surgem incentivos fortes à criação de legislação governamental favorável ao controlo e monitorização de populações (Estêvão, 2014).

Nos EUA, o *"USA Patriot Act: Lei de 2001 para unir e fortalecer a América, fornecendo instrumentos apropriados requeridos para intercetar e obstruir o terrorismo"*[16] torna-se decreto pela mão do presidente George W. Bush em 26 de outubro de 2001. Assim, "apenas quarenta e seis dias foram suficientes para validar pelo congresso norte-americano uma lei considerada por muitos controversa, entre outros fatores pela viabilização e incentivo da vigilância, sob várias formas, de indivíduos suspeitos de conspiração terrorista" (Estêvão, 2014: 158). A referida lei promulgada adota um conjunto de medidas, assentes na vigilância e monitorização, com a finalidade de manterem a segurança nacional (Andrejevic, 2007; Rule, 2007; Fuchs, Boersma, Albrechtslund and Sandoval, 2011). Neste contexto, é possível afirmar que "a segurança está a ser implementada de duas formas: numa, a tecnologia é um instrumento colocado ao dispor de uma maior visibilidade do que se faz e quem faz; noutra são abolidos os direitos individuais em prol de um bem comum" (Frois, 2008: 130).

Vulgarizam-se, por ação dos *media*, expressões como *Drones*, *Stingray, Passenger Name Record* (PNR) ou *Terrorist Finance Tracking Programme* (TFTP). Em discussão na opinião pública estão os limites da privacidade e a utilização dos já referidos e polémicos sistemas de vigilância como os *Drones* para fins civis (aparelhos voadores não tripulados com câmaras de vigilância), ou os dispositivos *Stingray* (simuladores de antenas de receção móvel, alegadamente usados pelo governo dos EUA, para monitorizar conversações em telefones móveis de suspeitos de crimes. A polémica surge quando no decorrer do processo de monitorização são extraídos dados de telemóveis, mesmo não estando em uso, de cidadãos que não estão sob investigação) (Qiu, 2007; Trottier, 2013; Harding, 2014).

Igualmente polémica é a aplicabilidade de Acordos como o *Passenger Name Record* (PNR), em vigor nos EUA após o 11 de setembro de 2001 e proposto no Tratado de Lisboa em 2007 para o espaço europeu. O procedimento para fins comerciais já era efetivado pelas companhias aéreas antes do ano de 2001, onde eram recolhidos, guardados e analisados os dados dos passageiros (Salter, 2008; Estêvão, 2014). Após os atentados de 2001 os dados PNR, no contexto norte-

[16] Tradução livre.

americano, passaram a ser fonte fundamental para reconhecer e elaborar perfis de eventuais terroristas (Lyon, 2007; Salter, 2008).

Identicamente, com a propósito da luta contra o terrorismo, surgem outros Acordos, com origem nos EUA, como o *Terrorist Finance Tracking Programme* (TFTP), elaborado com a finalidade primária de monitorizar os fluxos monetários interbancários de origem terrorista, fazendo uso de informações disponibilizadas pela Society for Worldwide Interbank Financial Telecommunication (SWIFT)[17], com sede em Bruxelas. A controvérsia com o Acordo TFTP remonta a 2006, com acusações de violação da lei da privacidade da UE (Gates, 2012). Porém, a partir de 1 de agosto de 2010, o Acordo TFTP (USA-UE) é extensível à União Europeia, viabilizando a partilha de informações interbancárias intercontinentais. A relação EUA-UE, face ao TFTP, volta a estar comprometida e envolta em polémica a partir do segundo semestre do ano de 2013 (como evidenciado de seguida), aquando da divulgação de alegados casos de vigilância massificada perpetrada pelos EUA a países da UE (Traynor, 2013).

No decorrer dos primeiros dias do mês de junho de 2013 surgiu, difundida pelo jornal britânico The Guardian e pelo norte-americano The Washington Post, uma controversa revelação envolvendo alegadamente um programa de vigilância intitulado - Prism. O referido programa governamental, desenvolvido nos EUA, envolve a troca de informações entre entidades como a National Security Agency (NSA) e empresas como a Google, a Microsoft, o Facebook, o Yahoo!, o Youtube, o Skipe ou a Apple. As informações partilhadas entre as empresas multinacionais referidas e a agência de segurança nacional norte americana (NSA) envolvem dados de milhões de utilizadores, nomeadamente correio eletrónico, fotos e vídeos. Também referenciado pelos mesmos jornais e referente à mesma agência, a National Security Agency (NSA), está a acusação de alegado envolvimento com a empresa de telecomunicações norte-americana Verizon, na gravação de milhões de conversas em chamadas telefónicas (Harding, 2014).

A metodologia de recolha massificada de dados é segundo Edward Snowden, (antigo assistente técnico da NSA e a principal face no processo de acusações) realizada de forma sistemática, massiva e indiscriminada. O motivo apontado para o procedimento é a maior eficácia de escrutínio que a recolha massiva representa, face à recolha seletiva, fazendo uso de algoritmos avançados que identificam perfis de risco (Harding, 2014).

Os desenvolvimentos ao momento, referentes às declarações de Edward Snowden, apontam para uma crescente instabilidade na política internacional,

[17] Sociedade cooperativa internacional que tem como objetivo criar um canal de comunicação global entre entidades bancárias internacionais, bem como padronizar transações financeiras.

resultante das periódicas revelações (última aparição em entrevista televisiva realizada pelo canal norte-americano NBC, a 28 de maio de 2014) de vigilância em massa perpetrada pela agência de segurança norte-americana NSA e pela sua congénere britânica Government Communications Headquarters (GCHQ) a milhões de cidadãos de todo o mundo e a Estados Governo como a Alemanha, o Reino Unido e o Brasil (Estêvão, 2014). A meados do mês de maio de 2014, Edward Snowden, pela mão do autor Glenn Greenwald expõe, na obra não ficcional *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Greenwald, 2014), os meandros do já referenciado programa Prism. Edward Snowden, que completou um ano de asilo político na Rússia (a 1 de agosto de 2014), vê prolongada, pela mão do presidente russo Vladimir Putin, a autorização de residência na Rússia por mais três anos.

Do atual panorama da Sociedade em Rede, evidenciamos a proliferação de uma vigilância com fins comerciais e de *marketing* desenvolvida na Internet (Lyon, 2003).

> "A Internet tornou-se uma indústria multibilionária, onde um conjunto de empresas recolhem e analisam uma grande quantidade de dados de consumo pessoais, a fim de direcionar uma publicidade personalizada" (Lyon, 2003: 162).

As características apontadas pelo autor à Internet são extensivas à Web 2.0, onde atualmente aplicações como o Facebook ou o Foursquare utilizam a vigilância de forma massificada junto aos seus utilizadores. A vigilância é, no entanto, personalizada e individual, na medida em que compara interesses e comportamentos com outros utilizadores, definindo e classificando tipologias de potenciais consumidores. Esta classificação é realizada com base em mecanismos de comparação e algoritmos de seleção que estipulam perfis e direcionam consumos (Fuchs, Boersma, Albrechtslund e Sandoval, 2011).

Neste contexto, "ferramentas de Web 2.0 como o Facebook, fazem uso de configurações de privacidade, onde o fornecimento de dados é exigido ao utilizador a fim de ser capaz de usufruir da aplicação. Aplicações digitais em plataformas móveis (como por exemplo *smartphones*) estão hoje capacitadas de identificar e recolher hábitos *online* dos utilizadores, nomeadamente contatos, ficheiros, localização, e muito mais" (Estêvão, 2014: 161). Perfis elaborados de utilizadores estão pois a ser coletados, por empresas multinacionais, com base na recolha de dados de plataformas móveis (Marx, 2002; Cottrill, 2011).

Igualmente as tecnologias de reconhecimento facial, ficcionadas em filmes como *Minority Report*[18], estão atualmente em pleno desenvolvimento. Empresas

[18] Baseado no conto de ficção científica, escrito por Philip K. Dick, publicado em 1956 - http://www.imdb.com/title/tt0181689/?ref_=nv_sr_1

multinacionais como a Google e a Apple estão no atual momento a desenvolver bases de dados com impressões faciais, fazendo uso de fotografias e perfis de utilizadores de redes sociais como o Facebook (Andrejevic, 2007; Estêvão, 2014).

Nos EUA, a legislação em vigor apresenta limitações rigorosas que restringem a utilização de impressões faciais, para usos de controlo laboral e de segurança nacional. Contudo estas limitações legislativas, referentes à utilização das impressões faciais, não contemplam a aplicação para fins comerciais e de *marketing* realizadas por empresas multinacionais. O controlo e a supervisão empresarial, por parte das empresas multinacionais, estão pois salvaguardados pela constituição norte-americana (Papacharissi, Gibson, 2011). Na Europa, nomeadamente na União Europeia, a legislação em vigor é mais rigorosa e penalizadora dos usos das impressões faciais para fins comerciais (Pidd, 2011; Welinder, 2012; Anjos, 2013; Estêvão, 2014).

Segundo dados recentemente revelados pelo Facebook e divulgados pela imprensa mundial esta empresa multinacional, líder de mercado no sector das ferramentas digitais detinha, a junho de 2014, cerca de 1.32 bilião de utilizadores ativos mensalmente (1/7 da população mundial).

Ainda que não recentemente, Lyon identifica um conjunto de tecnologias emergentes no âmbito da vigilância (Lyon, 2007), que passam pelas Tecnologias Biométricas – comuns na monitorização laboral através da leitura por dedo, íris, mão, face e voz; as Tecnologias Genéticas – relacionadas com o genoma humano e com principais aplicabilidades, para já, na utilização forense e controlo criminal; as Tecnologias de Localização – referentes à georreferenciação GPS (*Global Positioning System*), evidenciada nas suas distintas aplicabilidades, como na monitorização de viaturas por entidades patronais, na deteção de suspeitos por parte de forças policiais ou ainda para fins de *marketing*, localizando espacialmente um potencial consumidor e disponibilizando-lhe informações de consumos; por fim as Tecnologias de Rastreio – referentes à identificação RFID (*Radio-Frequency IDentification*), caracterizada pela identificação automática através de sinais de rádio. As suas aplicabilidades vão desde utilizações em aeroportos, em supermercados e em autoestradas (tecnologia usada no sistema de portagem eletrónica - Via Verde).

A teorização e conceptualização de vigilância está longe de ser consensual existindo, ao longo dos tempos, distintas interpretações das suas aplicabilidades na sociedade moderna.

Catarina Frois, na sua obra *Vigilância e Poder* (Frois, 2011), realiza um retrato da política de segurança e da implementação da videovigilância em Portugal. Neste estudo académico, a autora efetua uma reflexão crítica à interpretação e associação

de vigilância como um fator exclusivamente negativo de poder, instigando o controlo e a disciplina. Na obra referenciada é colocada a seguinte questão a discussão:
"Falamos de vigilância no sentido de controlar com o intuito de penalizar ou falamos de proteger?" (Frois, 2011: 122).
Em resposta a esta questão, a autora evidencia o seguinte exemplo:

> " …se pensarmos por exemplo em "vigilância médica", seja na interação médico-paciente, seja na deteção e monitorização de doenças infeciosas. Controla-se para identificar determinada epidemiologia, ao mesmo tempo que se protege o portador e quem o rodeia. Esta ambivalência pode derivar negativamente, em que este controlo sobre uma determinada pessoa é usado para a discriminar pela sua condição em prol da proteção não do sujeito mas sim de um coletivo" (Frois, 2011: 122).

A complexa interpretação de vigilância depende, em larga escala, dos limites do aproveitamento ou aplicação que se dá à informação recolhida. O surgimento da Sociedade em Rede robusteceu a multiplicidade de interpretações divergentes na teorização de vigilância.

Surgem desta forma, na sociedade contemporânea, novos paradigmas de vigilância, como a já identificada anteriormente - Vigilância Lateral (*peer-to-peer*).

Este tipo de vigilância, também designada por Interpessoal (Trottier, 2012), que decorre nas redes sociais, pode ter distintos fins e aplicabilidades, das mais elaboradas prospeções de *marketing* digital, realizadas por entidades empresariais, às mais inofensivas prospeções de cariz sexual, a que Andrejevic designa de - *Online Dating* (Andrejevic, 2005). Uma relevante aplicabilidade da Vigilância Lateral na Web 2.0 é a sua vertente participativa, específica em funções de segurança e policiamento. Esta carateriza-se pela partilha de informação verídica e pela investigação, condenação e divulgação de ações impróprias, através de ferramentas de Web 2.0 (Andrejevic, 2005). Segundo Daniel Trottier, a principal razão para a disseminação deste tipo de vigilância na Web 2.0, prende-se essencialmente pela extensão social crescente na Sociedade em Rede e não pelos constantes desenvolvimentos tecnológicos (Trottier, 2012).

Tomando como estudo de caso os tumultos de Vancouver de 2011[19], Christopher Schneider e Daniel Trottier vieram demonstrar que a Vigilância Lateral nas redes sociais é uma ferramenta de valor acrescido para as forças policiais e de segurança. Segundo os autores, no caso referenciado, o *crowdsourcing* de

[19] Perturbação da ordem pública na baixa da cidade de Vancouver, a 15 de junho de 2011, após um jogo da final da Liga profissional de hóquei em gelo.

policiamento efetuado na rede social Facebook, foi um exemplo bem-sucedido de cooperação entre uma sociedade civil mobilizada e digitalmente literata e as forças policiais (Schneider, Trottier, 2012).

## 3.2. Retrato da Vigilância em Portugal

Perante o verificado panorama de disseminação de políticas, métodos e instrumentos de supervisão e controlo na sociedade contemporânea, torna-se pertinente ao estudo analisar e enquadrar a vigilância, no contexto particular português.

Iniciamos com um dado facultado pela presidente da Comissão Nacional de Proteção de Dados (CNPD), não representativo da atual conjuntura portuguesa, mas contudo digno de referência: "Portugal foi, em 1976, o primeiro país do mundo a considerar em Constituição (artigo 35º), o direito à proteção de dados pessoais" (Anjos, 2013: 37).

Em Portugal a vigilância, nomeadamente a videovigilância no espaço público, tem vindo a tomar lugar em alguns locais específicos, de algumas cidades. A implementação de sistemas de videovigilância, no espaço público, surge em Portugal no decorrer do Campeonato Europeu de Futebol de 2004 (Frois, 2011).

Os eventos desportivos de grande projeção internacional têm sido, nos últimos anos, um dos grandes disseminadores de sistemas de videovigilância em vários países. É exemplo disso, o caso da Grécia e os Jogos Olímpicos de Atenas que decorreram também eles no ano de 2004 (Frois, 2011, 2013).

Em Portugal a adoção de sistemas de videovigilância é uma prática muito recente, tendo sido só a partir de 2005 com a Lei nº 1/2005, que regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum, que se começou a utilizar no espaço público esta ferramenta de vigilância (Frois, 2011).

A Comissão Nacional de Proteção de Dados (CNPD) era até ao surgimento da Lei nº 9/2012 de 23 de fevereiro (que procede à terceira alteração à Lei n.º 1/2005), a entidade com poder vinculativo com os seus pareceres, no que respeitava à instalação de câmaras de vigilância no espaço público.

Até ao surgimento da alteração à lei eram valorizados, na atribuição de autorizações de instalação de videovigilância, locais ou zonas específicas, delimitadas espacialmente, onde se aglomerassem durante determinado período de tempo um elevado número de pessoas (Frois, 2011). São os casos dos projetos de videovigilância requeridos e aprovados pela CNPD na Zona da Ribeira no Porto, na

Zona Histórica de Coimbra, no Santuário de Fátima e na Zona do Bairro Alto em Lisboa. Ao momento unicamente estão em pleno funcionamento, captando e gravando imagens, as câmaras de videovigilância em Coimbra e no Santuário de Fátima. Na Zona da Ribeira do Porto as câmaras de videovigilância, já tendo estado em pleno funcionamento, encontram-se somente a captar imagens sem proceder à sua gravação. Em Lisboa, na Zona do Bairro Alto, as câmaras de videovigilância, instaladas desde janeiro de 2013, encontram-se igualmente somente a captar imagens sem proceder à sua gravação.

Sendo o estudo de caso do INDECT central à dissertação em causa, e tendo o mencionado projeto de investigação da União Europeia a videovigilância como uma das suas primordiais áreas de atuação (investigação), torna-se importante a contextualização da regulamentação atual da videovigilância no contexto português.

A Lei nº 9/2012, de 23 de fevereiro[20] "procede à terceira alteração à Lei n.º 1/2005, de 10 de janeiro, que regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum".

A referida lei, logo no artigo 2º, evidencia duas novas finalidades da videovigilância:

"1 — e) Prevenção de atos terroristas;

f) Proteção florestal e deteção de incêndios florestais".

As novas finalidades que surgem na alteração à lei são resultado de políticas governamentais, altamente mediáticas. Iremos abordar unicamente as políticas de disseminação da videovigilância com o intuito de prevenção de atos terroristas.

O artigo 3º, da mesma lei, referencia que:

"1 — A instalação de câmaras fixas, nos termos da presente lei, está sujeita a autorização do membro do Governo que tutela a força ou serviço de segurança requerente";

"2 — A decisão de autorização é precedida de parecer da Comissão Nacional de Proteção de Dados (CNPD), que se pronuncia sobre a conformidade do pedido face às necessidades de cumprimento das regras referentes à segurança do tratamento dos dados recolhidos, bem como acerca das medidas especiais de segurança a implementar adequadas a garantir os controlos de entrada nas instalações, dos suportes de dados, da inserção, da utilização, de acesso, da transmissão, da introdução e do transporte…".

As alterações aos números 1, 2 do artigo 3º são demonstrativas da passagem de poder vinculativo da Comissão Nacional de Proteção de Dados para o Ministério da Administração Interna (MAI). Anteriormente a esta última alteração à lei, a CNPD era a

[20] http://www.cnpd.pt/bin/legis/nacional/LEI_9_2012.pdf

entidade que efetuava os estudo, analisando em conformidade as reais necessidades e justificações para a implementação de sistemas de videovigilância.

Como já referenciado, a atual implementação de sistemas de videovigilância na via pública está dependente unicamente da deliberação do Ministério da Administração Interna (MAI). Por outro lado a CNPD pode-se pronunciar e emitir um parecer, não vinculativo, formulando recomendações e dispensando a adoção de algumas medidas de segurança. No mesmo artigo 3º, no nº 7, da mesma alteração à referida lei:

> "7 — A CNPD pode, fundamentadamente, no quadro da emissão do parecer a que se refere o n.º 2:
>
> a) Formular recomendações tendo em vista assegurar as finalidades a que se refere o n.º 2, sujeitando a emissão de parecer totalmente positivo à verificação da completude do cumprimento das suas recomendações;
>
> b) Dispensar expressamente a existência de certas medidas de segurança, garantido que se mostre o respeito pelos direitos, liberdades e garantias dos titulares dos dados".

Igualmente com esta alteração à lei, o prazo máximo de emissão de parecer passa a 60 dias, sendo considerado automaticamente positivo na ausência de parecer até esta data. No mesmo artigo 3º, no nº 3, da mesma alteração à referida lei:

> "3 — O parecer referido no número anterior é emitido no prazo de 60 dias a contar da data de receção do pedido de autorização, prazo após o qual o parecer é considerado positivo".

Face a estas alterações, na lei da videovigilância, é percetível uma clara intenção na minimização de poderes da CNPD face à implementação de sistemas de videovigilância.

Ao contrário do que sucede com outros países, e segundo Catarina Frois, onde a implementação da videovigilância é ocasionada por atos de violência, terrorismo ou guerra, em Portugal a motivação prende-se por estar essencialmente na "linha da frente" no que se refere às novas tecnologias de ponta (Frois, 2008).

> "…no contexto português, como ficará claro, o grande *slogan* não se prende com guerra e terrorismo, mas sim com modernização" (Frois, 2008: 113).

Ainda em contexto nacional, no decorrer do ano de 2005, e aproveitando uma política de incremento de sistemas de monitorização e supervisão (que levou à criação da já referida Lei nº 1/2005), é comunicado pelo governo socialista em funções, a intenção da criação de uma base de dados genética (Frois, 2008; Machado, Frois, 2014). Em fevereiro de 2008 é pois aprovada em Assembleia da República a Lei nº

5/2008, que sustenta a criação de uma base de dados de perfis de ADN para fins de identificação civil e criminal (forense). As críticas associadas à biovigilância, nomeadamente à utilização de perfis de ADN, são fundamentadas em pressupostos de Estados Governo mais controladores, com estratégias governamentais menos tolerantes, assentes na intensa regulação, inspeção e controlo (Machado, Silva, 2008; Machado, Frois, 2014).

> "As bases de dados genéticas por perfis de ADN representam o reforço dos poderes do Estado, em nome do bem coletivo – a segurança e a tranquilidade -, mas essa necessidade pode significar a compressão ou limitação dos direitos, liberdades e garantias dos cidadãos" (Machado, Silva, 2008: 157-158).

Em Portugal, a par do que acontece em outros países europeus, a motivação estratégica para a fundação de uma base de dados de perfis ADN, com fins forenses, é essencialmente de caráter político e governativo, comunicado e valorizado como um fiável instrumento de combate à criminalidade (Machado, Silva, 2008). Os argumentos da fiabilidade e da eficácia, associados à investigação forense, viabilizaram a criação de legislação própria, com o fim específico da criação de bases de informação genética (Machado, Silva, 2008).

Um outro caso que tem sido apontado por alguns autores, como Catarina Frois, como um exemplo de monitorização da comunidade civil em Portugal, é o Cartão do Cidadão (Frois, 2008). A par do que acontece em outros países da Europa, no Cartão do Cidadão estão dispostos elementos de identificação e dados biométricos que integram uma base de dados capaz de traçar perfiz elaborados de cidadãos (Lyon, 2007; Rule, 2007).

Ainda segundo David Lyon:

> "É de certa forma enganador falar apenas de cartões, já que de facto são sistemas de identificação em que o cartão é o elemento portátil que atesta a elegibilidade ou pertença e, por outro lado, a base de dados a que este se refere permite a classificação e categorização" (Lyon, 2004: 2)[21].

Igualmente o Recenseamento Geral da População (Censos) é identificado pelo mesmo autor (Lyon, 2007) como um evidente instrumento de vigilância e controlo da população. No ano de 1864 realizou-se em Portugal o 1º Recenseamento Geral da População, tendo por base as orientações do Congresso Internacional de Estatística, que teve lugar em Bruxelas, em 1853. O último censo nacional foi efetuado no ano de 2011.

[21] Tradução livre.

Relativamente ao tema da literacia digital, enquanto garante de uma maior alfabetização na atual Sociedade em Rede, é relevante identificar iniciativas como o Projeto Dadus, criado em 2008 e pioneiro a nível europeu, que resulta de um protocolo assinado entre o Ministério da Educação e a Comissão Nacional de Proteção de Dados. Este projeto tem como fundamento a sensibilização da comunidade escolar (2º e 3º ciclos do ensino básico) para as questões da proteção de dados pessoais e da privacidade.

No contexto europeu e como mote para o estudo de caso do projeto de investigação INDECT, é pertinente caracterizar o caso do Reino Unido enquanto um dos membros integrantes do referido projeto e um exemplo paradigmático a nível mundial de videovigilância massificada.

A cidade de Londres é hoje a cidade do mundo com mais câmaras de videovigilância (Frois, 2008). Dados com 10 anos já surpreendiam pela soma:

> "Estima-se que existam 4,2 milhões de câmaras no Reino Unido, ou uma por cada 14 pessoas" (Norris, MacCahill, Wood, 2004:110)[22].

A proliferação de sistemas videovigilância no Reino Unido surgiu após 1993, com o assassinato de uma criança de dois anos (James Bulger), por duas crianças de 10 anos. No caso documentado, o sistema de *CCTV*[23] do centro comercial desempenhou um papel decisivo no desvendar do *modus operandi* dos dois assassinos (Frois, 2011). Estava assim justificada a implementação de sistemas de videovigilância e foi este o fundamento para a sua implementação e massificação no território do Reino Unido. A aliar a este incidente, na justificação para um aumento da videovigilância, junta-se o atentado terrorista ao metropolitano de Londres a 7 de julho de 2005.

Seguindo as preocupações da agenda internacional, face a ameaças de violência, de terrorismo ou de guerra, a União Europeia tem vindo a fomentar o desenvolvimento de políticas e regulamentações específicas, relativas à vigilância a uma escala comunitária. É neste contexto que surgem projetos de investigação como o INDECT (*Intelligent information system supporting observation, searching and detection for security of citizens in urban environment*), o qual apresentaremos de seguida.

[22] Tradução livre.
[23] *Closed-Circuit Television.*

## 3.3. O Caso do INDECT

O INDECT é um projeto de investigação da União Europeia, criado a 1 de janeiro de 2009 e com finalização a 30 de junho de 2014. Segundo dados obtidos junto ao portal da CORDIS[24] (Community Research and Development Information Service) tem um custo total associado de investigação de 14.828.107 euros. Deste total, 10.906.984 euros são financiados pela União Europeia.

O INDECT tem como objetivo final o desenvolvimento de ferramentas com vista a melhorar a segurança dos cidadãos e proteger a confidencialidade das informações gravadas e armazenadas.

No INDECT as ameaças são consideradas tanto em ambiente físico como digital.

O desenvolvimento deste projeto de investigação envolve a participação de cientistas e investigadores europeus de nove países: Polónia (coordenador do projeto), Alemanha, França, Espanha, Reino Unido, Bulgária, República Checa, Eslováquia e Áustria.

O projeto define-se como: "*Intelligent information system supporting observation, searching and detection for security of citizens in urban environment".* A sua missão, segundo o que está descrito no *website* institucional[25], é a de:

> *"Desenvolver um conjunto de soluções de apoio à decisão humana, com base no desenvolvimento de algoritmos avançados, com vista a proteger o cidadão em ambiente urbano. A finalidade última é detetar ameaças terroristas e atividades criminosas como conflitos urbanos, roubos, vandalismo, pornografia infantil e tráfico humano, entre outros".*

Segundo a informação presente no portal da CORDIS, os principais objetivos do projeto INDECT são: *"desenvolver uma plataforma para registo e intercâmbio de dados operacionais; aquisição de conteúdos multimédia; processamento inteligente de informações; deteção automática de ameaças e reconhecimento de comportamentos anormais ou violentos, com vista a desenvolver o protótipo de um sistema integrado, centrado em rede de apoio a atividades operacionais de forças policiais".*

Segundo o mesmo portal da UE, este projeto visa reforçar a segurança dos europeus protegendo e salvaguardando a sua privacidade.

[24] Portal repositório público da Comissão Europeia para a divulgação de informações sobre projetos de investigação, financiados pela UE.
[25] http://www.indect-project.eu/

Segundo o descrito no *website* institucional do INDECT, as aplicabilidades deste projeto colaborativo europeu assentam em três categorias: (1) *Monitorização inteligente para deteção automática de ameaças em ambiente urbano*, tendo como recurso imagens provenientes de câmaras de videovigilância (*CCTV*). Ao contrário do verificado até à data com a abordagem tradicional, o inovador sistema de monitorização efetuado por *CCTV*'s provenientes do INDECT (aplicando algoritmos avançados), não realiza uma monitorização contínua de uma área intervencionada, onde o operador tem acesso indiscriminado a imagens obtidas, mas sim deteta situações potencialmente ameaçadoras, alertando o operador. Segundo o que está descrito no *website* institucional, a nova abordagem está de acordo com todas as normas existentes e visa melhorar a eficácia da monitorização dos vídeos existentes, tendo em conta a privacidade dos intervenientes; (2) *Deteção de ameaças disponibilizadas a nível informático*, com a identificação de fontes de distribuição de pornografia infantil, ou de comércio ilegal de órgãos humanos, entre outros. Desenvolvimento de ferramentas de deteção rápida de conteúdos ilegais, como a pornografia infantil, armazenados em dispositivos de armazenamento (discos rígidos); (3) *Proteção da privacidade e dos dados dos intervenientes*, com o desenvolvimento de duas ferramentas: Marca d'água Digital e Algoritmos Criptográficos. As Marcas d'água Digitais são utilizadas para proteger o conteúdo multimédia contra a adulteração maliciosa. Com o desenvolvimento de novos Algoritmos Criptográficos, é proporcionada uma maior segurança para transmissão e armazenamento de dados.

A grande maioria das aplicações e ferramentas a ser implementadas no projeto INDECT estão em fase de desenvolvimento por parte dos inúmeros parceiros e centros de investigação europeus. Estas aplicações estão enunciadas no *website* institucional do INDECT. Assim, identificando-as: (i) Reconhecimento de imagens relacionadas com ameaças - nova abordagem para monitorização na análise de vídeo. Deteção de cenários contendo ameaças potenciais. Por exemplo: presença de objetos perigosos (armas), bagagem abandonada, roubos, entre outros. Nesta identificação estão incluídas tecnologias de reconhecimento facial que realizam cruzamento de dados com ferramentas digitais como o Facebook; (ii) Reconhecimento de sons relacionados com ameaças - está atualmente em desenvolvimento um *software* que deteta e monitoriza automaticamente sons como: tiros, explosões, gritos, alarmes e vidros a quebrarem; (iii) Deteção de objetos perigosos - está em desenvolvimento um sistema de análise de algoritmos que deteta em vídeo objetos perigosos (armas) em mãos de pessoas; (iv) Deteção de bagagem abandonada - está igualmente em aperfeiçoamento um sistema de algoritmos que deteta automaticamente em vídeo, bagagem abandonada em terminais de aeroportos e estações ferroviárias; (v) Deteção

de ameaças disponibilizadas a nível informático - aplicação de ferramentas com vista a detetar conteúdos ilegais (pornografia infantil) e ameaças (vírus e *malware*) em redes de computadores; (vi) Proteção dos dados e da privacidade - aplicação de duas ferramentas - Marca d'água Digital e Algoritmos Criptográficos, que visam proteger os conteúdos multimédia e a transmissão e armazenamento de dados.

No que concerne a ameaças disponibilizadas a nível informático (v), nomeadamente conteúdos de pornografia infantil, o INDECT tem vindo a desenvolver uma ferramenta que tem, segundo os coordenadores do projeto, obtido resultados assinaláveis, intitulada de INACT (INDECT Advanced Image Catalog Tool). Esta ferramenta pode ter duas funcionalidades: o INACT Indexer, convertendo ficheiros com conteúdos de pornografia infantil em base de dados; e o INACT Searcher que através da base de dados criada, identifica imagens similares em dispositivos informáticos apreendidos, que possam ser eventualmente usadas como prova de crime.

Segundo o Conselho de Ética do projeto europeu INDECT, este está sujeito a rigorosas normas de funcionalidade, com vista a garantir o cumprimento do regulamento nacional e internacional da privacidade e da proteção de dados. A mesma entidade informa que a utilização da informação recolhida é única e exclusivamente para fins de investigação. Defende ainda que a implementação de ferramentas desenvolvidas pelo INDECT, baseadas em análise de algoritmos avançados, assegura resultados de pesquisa mais seguros, menos subjetivos e com menos erros humanos. Ainda segundo informações disponibilizadas no 2º Relatório Periódico do INDECT, presente no portal CORDIS, todo o funcionamento do projeto de investigação é realizado de forma a assegurar o equilíbrio adequado entre a proteção dos direitos da pessoa humana e a proteção da sociedade.

Contudo, a criação de um projeto europeu de investigação, com as características do INDECT, tem levado ao surgimento de movimentos “Anti-INDECT”, com expressão em vários países europeus, que contestam a crescente política de investimento em vigilância levada a cabo pela União Europeia.

## 4. Opções Metodológicas

Esta dissertação apresenta como estudo de caso o projeto de investigação da União Europeia - INDECT (Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment).

No que concerne à metodologia de análise desenvolvemos uma abordagem qualitativa intensiva.

Uma pesquisa qualitativa (estudo de caso) que se baseia numa análise documental, analisando relatórios e diretivas comunitárias relativas ao projeto INDECT. Do anteriormente referido portal da CORDIS[26] (Community Research and Development Information Service) foram considerados, na investigação documental, os Relatórios Periódicos (1 e 2), assim como um conjunto de artigos académicos, acessíveis diretamente pela plataforma OpenAIRE[27] (Open Access Infraestruture for Research in Europe), nomeadamente artigos de esclarecimento processual das ferramentas INACT, Marcas d'água Digitais e Algoritmos Criptográficos (anteriormente referenciadas no capítulo 3.3. O Caso do INDECT).

O *website* do INDECT, enquanto plataforma digital oficial do projeto, foi adotado na pesquisa documental da dissertação, valorizado pela vasta quantidade de informação que engloba, referente à investigação do INDECT. Enumerando e evidenciando parte da documentação e temas presentes no *website*, considerados na investigação: "Work Package News and Events"[28]; "Public Deliverables"[29]; "Ethical Issues"[30], entre outros.

> "A quantidade de material documental que o investigador poderá estudar é inevitavelmente influenciada pelo tempo de que este dispõe para esta fase da investigação" (Bell, 1997: 106).

A análise dos dados documentais representa, no estudo proposto em dissertação, um método de pesquisa central, pela fonte de dados relevantes que agrega. A abordagem aos referidos dados documentais, aquando da progressão da investigação, clarifica a relevância das fontes e otimiza as escolhas (Bell, 1997).

Da mesma pesquisa qualitativa fazem parte três entrevistas realizadas a quatro representantes de entidades selecionadas pela sua pertinência ao estudo. Procurou-se esclarecer com estes testemunhos, conseguidos em entrevista, os distintos posicionamentos relativamente ao projeto de investigação INDECT, e as opiniões face à atual disseminação de programas e projetos de vigilância, no contexto europeu e mundial.

> "A entrevista a especialista é uma forma específica de entrevista semiestruturada" (Meuser, Nagel, 1991 citado por Flick, 2005: 92).

[26] http://cordis.europa.eu/projects/218086
[27] https://www.openaire.eu/
[28] http://www.indect-project.eu/events
[29] http://www.indect-project.eu/public-deliverables
[30] http://www.indect-project.eu/approach-to-ethical-issues

Ainda segundo os mesmos autores, este tipo de entrevista a um informador privilegiado tem como principal objetivo analisar e comparar o conteúdo dos conhecimentos do perito (Meuser e Nagel, 1991 citados por Flick, 2005).

Uma primeira entrevista é realizada ao coordenador do projeto INDECT - Mikolaj Leszczuk, e a um assistente de coordenação do mesmo projeto - Jan Derkacz. A cargo do coordenador do projeto ficam as respostas às questões estruturais do projeto. Ao assistente de coordenação cabe a resposta às questões de foro ético relativas ao INDECT. A missão do projeto INDECT está descrita no capítulo - 3.3. O Caso do INDECT, deste trabalho. A entrevista tem como objetivo o entendimento das finalidades do projeto e das implicações na privacidade dos cidadãos europeus.

Uma segunda entrevista é realizada a Pedro Heitor, um ativista do movimento STOP INDECT Portugal, com presença na rede social Facebook. Este movimento, segundo o membro entrevistado do STOP INDECT, caracteriza-se por ser *"um movimento livre e sem uma estrutura orgânica definida que visa simplesmente promover a consciencialização e o debate dos cidadãos sobre o projeto INDECT, projeto este que coloca sérias questões éticas e jurídicas que devem ser sujeitas ao escrutínio público por um lado e, por outro, a um controlo rigoroso por parte dos órgãos democráticos da União Europeia".* A entrevista tem essencialmente o objetivo de esclarecer quais as motivações para a criação de um movimento "Anti-INDECT".

Por fim, uma terceira entrevista a ser realizada à presidente da Comissão Nacional de Proteção de Dados (CNPD), Filipa Calvão. Segundo o que está descrito no *website* institucional[31], a CNPD "*é uma entidade administrativa independente com poderes de autoridade e que tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei*". A entrevista tem como objetivo percecionar qual o entendimento da CNPD face a um projeto de investigação da UE, que tem como base a criação de ferramentas de vigilância a implementar no espaço europeu.

Optámos pela realização das entrevistas via correio eletrónico de forma a obter uma mais consistente análise e manter uma coerência processual entre os vários entrevistados. Somente na entrevista à presidente da CNPD existiria a facilidade e disponibilidade para a realização da entrevista presencialmente. Por parte do ativista do movimento STOP INDECT Portugal existiu uma imediata indisponibilidade para um encontro presencial. Por parte do projeto INDECT, e pela sua coordenação estar sediada na Polónia, não foi ponderada a deslocação para uma entrevista presencial.

[31] http://www.cnpd.pt/

## 5. O Projeto INDECT e a sua Fundamentação Teórica

A pesquisa qualitativa intensiva, referente ao estudo de caso do INDECT, como já evidenciado no capítulo anterior, subentende uma análise de documentos estruturais ao projeto de investigação e uma análise a três entrevistas suporte realizadas a representantes de entidades ou grupos pertinentes ao estudo. A análise documental referenciada considera a seguinte pergunta de partida, respeitante ao estudo proposto em dissertação: "*Qual o papel, no contexto da sociedade contemporânea, de programas de investigação, cofinanciados pela União Europeia, especificamente vocacionados para a vigilância dos cidadãos? (O caso do INDECT)*".

Tendo em conta a questão anterior optou-se, no processo da pesquisa documental, identificar *à priori* temáticas que, pela sua relevância, se destacam e se tornam merecedoras de uma atenção e análise privilegiadas. Desta forma, foram identificados os seguintes temas em análise: (1) A criação do projeto INDECT; (2) As implicações do projeto INDECT; e (3) A sociedade vigilante.

Para uma mais eficaz e percetível análise documental, optámos por analisar os temas referidos anteriormente pela seguinte ordem de entrevistados/intervenientes: INDECT, STOP INDECT e Comissão Nacional de Proteção de Dados (CNPD).

Foram incluídos, em anexo (Anexos 1, 2 e 3), os guiões das entrevistas enviados aos entrevistados. O Anexo 1 refere-se ao guião de entrevista ao INDECT, o Anexo 2 ao STOP INDECT e o Anexo 3 à CNPD.

Referente a (1) A criação do projeto INDECT, e como já evidenciado no capítulo - 3.3. O Caso do INDECT, este projeto de investigação cofinanciado pela União Europeia visa, segundo os seus fomentadores, reforçar a segurança dos cidadãos europeus protegendo a sua privacidade. A coordenação do projeto INDECT em entrevista, reportando-se à sua presença na 4ª Conferência Europeia de Investigação de Segurança em Estocolmo, em 2009, enfatizava as mesmas preocupações da União Europeia no que concerne à segurança dos cidadãos. Em 2007 a União Europeia, com o programa de investigação FP7[32], divulgava a admissão de propostas para projetos de investigação, sob o tema da "Segurança". O programa de investigação "FP7 – Security" tinha os seguintes objetivos: (i) Desenvolver tecnologias para garantir a segurança dos cidadãos contra ameaças como o terrorismo, as catástrofes naturais e a criminalidade, respeitando os direitos humanos fundamentais e a privacidade; (ii) Estimular a cooperação entre fornecedores e utilizadores de soluções de segurança civil; (iii) Melhorar a competitividade da indústria europeia de segurança; (iv)

[32] 7th Framework Programme for Research and Technological Development. Programa de 7 anos (2007-2014).

Apresentar resultados para uma investigação orientada para a resolução das lacunas de segurança.

A proposta apresentada pelo projeto INDECT, na especialidade da segurança dos cidadãos em ambiente urbano (FP7-SEC-2007-1), foi avaliada por peritos independentes à União Europeia, no concerne ao mérito científico e às necessidades finais de utilização.

Referente ao primeiro tema em análise, (1) A criação do projeto INDECT, o entrevistado, ativista do movimento STOP INDECT, argumenta que o INDECT, tendo objetivos claros de assegurar a segurança no espaço europeu, faz uso de inovações tecnológicas, como a aplicabilidade de algoritmos avançados, para análise de informações de caráter privado dos cidadãos. Segundo o ativista, os objetivos identificados para o projeto INDECT não dão garantias de uma aplicação futura clara, podendo hipoteticamente ser usado com fins abusivos de monitorização arbitrária/discricionária dos cidadão europeus, para usos militares/paramilitares, ou num cenário extremo a ser utilizado por um Estado Policial.

Ainda alusivo ao tema em análise, (1) A criação do projeto INDECT, a entrevistada, presidente da Comissão Nacional de Proteção de Dados (CNPD), refere que está a par do desenvolvimento do projeto INDECT, assim como das suas especificidades e implicações (desenvolvido mais à frente neste capítulo).

Concernente ao segundo tema em análise, (2) As implicações do projeto INDECT, é igualmente divergente a opinião dos vários entrevistados perante os efeitos decorrentes do desenvolvimento do projeto de investigação referido. Desta forma, a coordenação do projeto INDECT em entrevista, salienta que no decorrer da divulgação das suas investigações foi contatada pelas autoridades policiais de Espanha, Malta, Letónia e Roménia. Evidencia ainda como a Europol[33] louvou o projeto INDECT numa apresentação realizada em abril de 2012. Este reconhecimento é significativo, segundo o entrevistado (coordenador do projeto INDECT), embora segundo o mesmo seja percetível que um projeto de investigação da UE seja valorizado por parte de uma Agência de Aplicação da Lei (*Law Enforcement Agency*) da UE – o consórcio do INDECT. Segundo o mesmo entrevistado a equipa do INDECT, enquanto parte de um projeto de pesquisa e não de um projeto de implementação, desconhece a real e final aplicabilidade das ferramentas desenvolvidas.

Perante a questão da garantia da aplicabilidade das ferramentas desenvolvidas pelo INDECT, para as áreas indicadas no *website* institucional, o coordenador do projeto argumenta que é da responsabilidade das autoridades dos Estados Membros o

[33] A Europol é o serviço europeu de polícia, incumbido do tratamento e intercâmbio de informação criminal.

uso destas ferramentas, tendo em conta o direito dos indivíduos e a proteção de dados pessoais. Adianta ainda que, a utilização destas ferramentas pelos Estados Membros está sujeita à obrigação de respeito pelos direitos fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia[34], pela Convenção Europeia dos Direitos Humanos, e pela legislação da UE face à proteção de dados.

Confrontado pela questão relativa ao projeto INDECT, respeitando a privacidade e proteção de dados dos cidadãos europeus (remetendo em particular aos Artigos 7º e 8º da Carta dos Direitos Fundamentais da União Europeia), o coordenador do INDECT explica que todos os projetos financiados no âmbito do FP7, incluindo o INDECT, são obrigados a cumprir os critérios para o tratamento de dados pessoais, tal como estabelecido no Artigo 8º da Carta dos Direitos Fundamentais da União Europeia, e na Diretiva 95/46/CE, referente ao direito comunitário em matéria de proteção de dados. Segundo o entrevistado esta situação proporciona a todos o direito à proteção de seus dados pessoais. Adianta ainda que, se os dados pessoais são recolhidos, então o processo deverá ser feito de forma justa, para fins específicos e com base no consentimento da pessoa em causa ou em algum fundamento legítimo previsto por lei. Ainda segundo o mesmo, todos têm o direito de acesso aos dados pessoais que foram recolhidos, bem como o direito de ter a respetiva retificação dos mesmos. O cumprimento destas regras está sujeito à supervisão de uma autoridade independente. Ainda segundo o coordenador do INDECT, no processo de investigação do projeto, nenhum dado real (operacional) é usado nem recolhido em gravação. Somente dados experimentais, realizados por voluntários devidamente esclarecidos, são coletados para fins de avaliação.

Alusivo às questões de foro ético, um segundo entrevistado do projeto INDECT, o já referido anteriormente nas Opções Metodológicas, assistente de coordenação do projeto, adianta que a supervisão e fiscalização das questões éticas, aquando da aplicabilidade das ferramentas, cabe à entidade de cada Estado Membro responsável pela proteção de dados. No caso de Portugal será a Comissão Nacional de Proteção de Dados (CNPD). O mesmo entrevistado, assistente de coordenação do INDECT, confrontado com a questão das soluções tecnológicas, envolvendo algoritmos avançados, contribuírem para uma sociedade vigilante, contesta assegurando que as soluções desenvolvidas pelo INDECT, a serem implementadas, iriam cumprir requisitos rigorosos de funcionamento. Finaliza referindo que o INDECT desenvolve ferramentas que privilegiam a privacidade e a proteção de dados. Reporta-se a duas ferramentas especificamente - Marca d'água Digital e Algoritmos Criptográficos - que

[34] http://www.europarl.europa.eu/charter/pdf/text_pt.pdf

visam proteger os conteúdos multimédia e a transmissão e armazenamento de dados (especificações apresentadas no capítulo 3.3. O Caso do INDECT).

Ainda referente ao segundo tema em estudo, (2) As implicações do projeto INDECT, o entrevistado ativista do movimento STOP INDECT, retrata o INDECT como um projeto de monitorização com capacidade de recolha e combinação de dados dos cidadãos (*big data*), provenientes de fóruns, de redes sociais, de *blogs*, de *websites*, de bases de dados públicas (e eventualmente privadas), de transferências eletrónicas de dados e de câmaras de *CCTV* na via pública. O mesmo entrevistado descreve o projeto INDECT como capaz de obter um conjunto ilimitado de informações pessoais dos cidadãos europeus capacitando-o de, através dessa recolha de informações, formular padrões comportamentais, penalizando aqueles que "fogem à normalidade". Procura ainda, segundo declarações realizadas pelo mesmo entrevistado, associar o eventual uso das ferramentas do projeto INDECT, à crescente convulsão social sentida na Europa, controlando e monitorizando formas de expressão democrática popular na *web* e nas ruas europeias.

O entrevistado, ativista do STOP INDECT opta, na questão referente às críticas ao projeto INDECT, em levantar uma série de interrogações: (i) Como será realizada a compilação e o tratamento de dados pessoais? Tendo em consideração o respeito pela Carta dos Direitos Fundamentais da União Europeia, especificamente o Artigo 7º - Respeito pela vida privada e familiar; o Artigo 8º - Proteção de dados pessoais; e o Artigo 11º – Liberdade de expressão e de informação. (ii) Relativamente à capacidade de julgar determinados comportamentos como normais ou anormais, o entrevistado levanta as seguintes questões: Em que termos concretos é feito esse juízo? Como são corrigidos eventuais erros decorrentes desse julgamento? (iii) Referente à fiscalização processual: Que entidade independente externa fiscaliza o INDECT? (como verificámos pelas respostas anteriormente dadas pelo assistente de coordenação do INDECT é a CNPD). (iv) Face à privacidade o entrevistado questiona: Quanto aos sistemas de vigilância, que utilizam algoritmos avançados, como são atenuados os efeitos do uso de tais sistemas, em termos de privacidade e proteção de dados pessoais? Por fim, (v) relativa à informação recolhida pelas ferramentas do INDECT, o entrevistado interpela: Sendo simples, para qualquer governo, autoridade ou órgão de segurança pública, através do seu poder ou através de fraude ou coação, aceder às informações recolhidas e processadas, que mecanismos dentro do INDECT existem para contrariar tal possibilidade?

O entrevistado, ativista do STOP INDECT, identifica a Internet, nomeadamente as redes sociais *online*, como as principais ferramentas de consciencialização da opinião pública relativamente ao INDECT, através da difusão de informação e da

estimulação ao debate. Adianta ainda que já foram realizados alguns fóruns na Internet sobre o tema do INDECT, mas sem grande aderência por parte de interessados. De igual modo foram, segundo o mesmo, realizadas ações de rua nas cidades de Lisboa e Porto, no dia 20 de outubro de 2012, aquando dos protestos a nível europeu contra o projeto INDECT, com vista ao esclarecimento dos fundamentos do projeto.

Face ao tema em análise, (2) As implicações do projeto do INDECT, a entrevistada, presidente da Comissão Nacional de Proteção de Dados (CNPD) salienta que o desenvolvimento de projetos como o INDECT, enquadrando-se numa política europeia de investimento nas questões de segurança e envolvendo inevitavelmente mecanismos de vigilância dos cidadãos, pressupõe obrigatoriamente uma ponderação exaustiva perante os direitos fundamentais. A entrevistada refere que o projeto INDECT, apesar de mencionar o desenvolvimento de algumas ferramentas para proteção da privacidade e dos dados pessoais (Marca d'água Digital e os Algoritmos Criptográficos), assume como seu principal objetivo tornar mais automáticos e inteligentes, o controlo e deteção de ameaças e os processos e procedimentos de pesquisa, seja pela integração de bases de dados, seja pelo cruzamento de informação em ambiente *online* e *offline*, estando assim virado para outros propósitos que se prendem basicamente com o trabalho policial. Adianta ainda que não é por acaso que algumas forças policiais são parceiras do projeto INDECT, fazendo parte do já designado consórcio INDECT. A presidente da CNPD evidencia as preocupações do Grupo de Trabalho de Proteção de Dados da UE – Grupo do Artigo 29.º[35] (no qual a CNPD está representada), face à forma como as investigações do INDECT estão a decorrer, no que concerne ao tratamento de dados pessoais, mas também quanto aos resultados da investigação e à necessidade de estes estarem conformes com os direitos fundamentais, antes de serem aplicados na prática. Desenvolve afirmando que, quanto à aplicação prática futura das ferramentas desenvolvidas pelo INDECT, o seu potencial de vigilância genérica e de análise de risco em tempo real eleva sobremaneira os riscos para a privacidade dos cidadãos.

Na entrevista efetuada, a presidente da CNPD chama a atenção para o desenvolvimento das ferramentas "inteligentes" e automatizadas (que reduzem o risco de erro humano e a apreciação subjetiva – como presente nas diretivas do INDECT), salienta ainda que a programação da "máquina" está sempre sujeita a critérios e parâmetros introduzidos pelo homem, pelo que também fruto de avaliações e juízos de

[35] O Grupo de trabalho foi instituído pelo Artigo 29.º da Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade.

valor. O *profiling*[36], como denomina, assume neste contexto especial relevo, sendo uma questão geradora de apreensão, pelo potencial discriminatório que comporta.

Finalizando, adianta que o Grupo do Artigo 29.º exortou a Comissão Europeia a ponderar previamente o financiamento de projetos que possam, de algum modo, pôr em causa os direitos fundamentais dos cidadãos.

Por último, o tema em análise (3) A sociedade vigilante, enquadra as opiniões dos entrevistados perante a eventualidade de se viver atualmente numa sociedade fomentadora da plena monitorização. Perante as questões da atual disseminação de programas de vigilância desenvolvidos pelos EUA e pela UE, e pelo surgimento de revelações referentes a um programa norte-americano, intitulado de "Prism" que visa a vigilância massificada de cidadãos americanos e europeus, o coordenador do projeto INDECT é perentório em afirmar a não existência de nenhuma relação entre o projeto INDECT e o programa Prism ou quaisquer outros programas e projetos de vigilância desenvolvidos pelos EUA e UE.

Referente ao mesmo tema em análise - (3) A sociedade vigilante - e às mesmas questões relativas à atual disseminação de programas de vigilância desenvolvidos pelos EUA e pela EU, e pelo surgimento de revelações referentes a um programa norte-americano intitulado de "Prism", que subentende a vigilância massificada de cidadãos americanos e europeus, o ativista do movimento STOP INDECT argumenta que dada a ausência de controlo e fiscalização, por órgãos democráticos, de programas e projetos de vigilância quer nos EUA quer na UE, as críticas já apontadas ganham ainda mais consistência, nomeadamente, - "Quem vigia os vigilantes?". O mesmo entrevistado alega que os objetivos de tais programas e projetos não estão totalmente esclarecidos, e que os abusos cometidos sobre os direitos dos cidadãos são frequentes. Assemelha ainda o programa Prism ao projeto INDECT, na medida em que quer um quer outro têm como objetivo assegurar a proteção e segurança dos cidadãos face a uma série de ameaças. Segundo o mesmo, o programa Prism caracteriza-se por ser um programa de mineração de dados[37] (*data mining*) e de vigilância eletrónica em massa, que operava (ou ainda opera) de forma clandestina, sem autorização prévia atribuída por mandado judicial a quaisquer autoridades, para proceder à vigilância eletrónica de particulares.

O entrevistado reitera que apesar das autoridades norte-americanas defenderem que o programa Prism auxiliou na prevenção de atos terroristas, tal facto nunca ficou

[36] Processo de construção e aplicação de perfis gerados por análise de dados informáticos.

[37] Processo de explorar grandes quantidades de dados, procurando padrões consistentes, como regras de associação ou sequências temporais, para detetar relacionamentos sistemáticos entre variáveis, detetando assim novos subconjuntos de dados.

demonstrado. Adianta ainda, que qualquer programa de vigilância exige permanentemente a maior das cautelas e no mínimo uma fiscalização efetiva e constante. Para finalizar declara que se o projeto INDECT operar nos mesmos moldes que o programa Prism, não só estarão a ser violadas todas as disposições legais europeias, no que toca à privacidade e proteção de dados pessoais, mas também estarão em causa a própria integridade e transparência das instituições e autoridades europeias.

A presidente da Comissão Nacional de Proteção de Dados, reportando-se ao tema (3) A sociedade vigilante destaca, no contexto nacional, a atual conjuntura em que as recentes alterações à Lei nº 9/2012 de 23 de fevereiro (Lei da Videovigilância) assumem o Ministério da Administração Interna (MAI) como único organismo de intervenção decisória na implementação de sistemas de videovigilância. Segundo a entrevistada, em termos práticos, esta alteração à lei permite ultrapassar os pareceres negativos da CNPD, que em alguns casos inviabilizaram a instalação de sistemas de videovigilância, podendo de algum modo facilitar a colocação de câmaras na via pública (*CCTV*), cumpridos que estejam os correspondentes requisitos legais.

No que concerne à temática da proteção de dados no quadro europeu, a entrevistada afirma que a proteção de dados pessoais é atualmente, e desde o Tratado de Lisboa em 2007, um direito fundamental da UE. Igualmente evidenciado pela entrevistada foi o papel do Tribunal de Justiça da União Europeia (TJUE) na imposição, a alguns Estados Membros, de melhoramentos ao nível da proteção de dados internos. Perante a questão do surgimento de um futuro regulamento europeu de proteção de dados, a presidente da CNPD esclarece que as alterações, face à atual diretiva europeia de proteção de dados, passam pela aplicabilidade de uma legislação de aplicação direta nos ordenamentos jurídicos dos Estados Membros. Adianta ainda que haverá uma lei igual nos Estados Membros da UE, em matéria de proteção de dados, o que confere segundo a entrevistada, a uma maior harmonização em termos legislativos. Contudo a opinião já veiculada pela CNPD, e reforçada pela presidente deste organismo, salienta que sendo a proteção de dados pessoais transversal a todos os setores da sociedade e, por isso, tendo de ser compatibilizada com outra legislação nacional específica, define que a forma de ato jurídico mais adequada seria a de Diretiva e não a de Regulamento. Salvaguarda no entanto, que ambas as soluções têm vantagens e desvantagens.

Em falta ficou, segunda a mesma, a introdução de normas na proposta de regulamento, relativas ao tratamento de dados pessoais na Internet. Conclui argumentando que o que é proposto é ínfimo, já se encontrando na prática coberto pela atual legislação.

A presidente da CNPD sublinha ainda que a UE tem vindo a investir fortemente na criação de sistemas de informação europeus e no reforço da cooperação policial e judiciária, com o aumento do intercâmbio de informações entre os Estados Membros, mas também com a comunicação de dados para países terceiros e organizações internacionais (exemplo do Acordo TFTP[38] ou PNR[39]) - nestes casos para satisfazer objetivos de outros países e não da UE.

Perante a questão de um eventual relacionamento, incluindo a proposta do regulamento europeu de proteção de dados, com a proliferação, por exemplo, de ferramentas como o Sistema de Informação Schengen de Segunda Geração (SIS II)[40] e o INDECT, a entrevistada desenvolve afirmando que o SIS II representa a evolução de um sistema de controlo fronteiriço para uma ferramenta de natureza mais policial. A sua principal utilização continua a ser o controlo de estrangeiros para efeitos de não admissão no Espaço Schengen. Outras ferramentas – como as desenvolvidas pelo INDECT – destinam-se essencialmente a ser utilizadas para controlo dos cidadãos europeus no interior da UE. A grande distinção entre estes dois exemplos prende-se, segundo a entrevistada, com o facto de, no caso do SIS II serem apenas tratados os dados pessoais de indivíduos determinados sobre os quais recaem medidas concretas, previstas na lei, e recorríveis judicialmente; enquanto num esquema genérico de vigilância para deteção de ameaças serem tratados dados pessoais de um universo indeterminado de pessoas factualmente não suspeitas. Segundo a mesma, essa é uma diferença crucial e que está intimamente ligada ao princípio da proporcionalidade: vigiar uma pessoa (nalguns casos, essa vigilância depende de mandado judicial), porque há indícios concretos e indicações factuais que a tornam suspeita de ter praticado ou estar envolvida num crime, é uma medida adequada; vigiar massivamente pessoas, na hipótese de descobrir indícios que uma delas possa vir a praticar um crime, é claramente uma medida desajustada e desproporcional.

A presidente da CNPD reitera que, como afirmado inequivocamente pelo TJUE, todas as iniciativas europeias têm de passar o teste da necessidade e da proporcionalidade, na perspetiva da proteção de dados e da privacidade.

[38] TFTP (Terrorist Finance Tracking Programme) pressupõe o envio de dados de transferências bancárias da sociedade SWIFT para os EUA.

[39] PNR (Passenger Name Record) pressupõe o envio de dados de passageiros para os EUA, Canadá e Austrália.

[40] Sistema de informação que permite às autoridades nacionais responsáveis pelos controlos fronteiriços e aduaneiros, bem como às autoridades policiais responsáveis pelos controlos na fronteira externa do espaço Schengen e no seu interior, emitir alertas sobre pessoas procuradas ou desaparecidas e objetos como veículos e documentos roubados.

Concernente ainda ao tema (3) A sociedade vigilante, a presidente da CNPD, aquando da interpelação do surgimento de revelações de vigilância massificada de cidadãos americanos e europeus, por parte de entidades como agências de segurança nacional como a NSA (EUA) e a GCHQ (RU), afirma que o que vai sendo tornado público não constituiu uma efetiva revelação para as autoridades de proteção de dados, que há muito tempo vêm chamando a atenção para a interferência abusiva das autoridades norte-americanas nos tratamentos de dados pessoais realizados pelas empresas estabelecidas nos EUA. Segundo a entrevistada, as referidas empresas que incluem muitos dos "gigantes da Internet", proporcionam um conjunto de serviços (ferramentas), que lidam com informação do foro pessoal, disponibilizada voluntariamente e conscientemente, ou não, através de cartões de crédito, de saúde, de cliente, entre outros**.**

A presidente da CNPD finaliza os seus pareceres, face ao tema (3) A sociedade vigilante, referindo que ao nível das Nações Unidas, foram já realizadas algumas iniciativas bastante meritórias, relativamente aos direitos das pessoas no ambiente digital. Refere que estas revelações abusivas, em particular as relativas a alguns países europeus, vieram evidenciar a necessidade da existência de um apertado e efetivo escrutínio democrático referente à atuação dos serviços de informação (agências de segurança nacional), com vista a garantir um rigoroso respeito pela lei e pelos direitos fundamentais. Por último, a entrevistada, evidencia o papel importante de iniciativas como o Projeto Dadus, criado pela CNPD (referenciado no capítulo 3.2. Retrato da Vigilância em Portugal), que têm como missão alertar crianças e jovens para os riscos de uma utilização incorreta das tecnologias de informação, proporcionando esclarecimentos com vista a minimizar riscos e a adotar boas práticas de uso da Internet, bem como prestando esclarecimentos sobre direitos.

Inúmeras e elucidativas conclusões se podem retirar desde já do capítulo - 5. O Projeto INDECT e a sua Fundamentação Teórica. Verificamos, tanto pela análise de dados documentais, como pelos testemunhos obtidos junto aos quatro entrevistados dos três organismos, que a temática proposta a discussão está longe de recolher opiniões consensuais.

Por parte do projeto INDECT, os testemunhos facultados pelos seus dois entrevistados demonstram uma preocupação notória em enquadrar o projeto como pertença de um programa europeu de investigação e desenvolvimento tecnológico (FP7), cumprindo todos os rigorosos critérios processuais de um projeto validado e cofinanciado pela União Europeia. Do discurso empregue pelo consórcio do projeto INDECT, explicitamente demonstrado pela documentação analisada e pelos testemunhos recolhidos em entrevista, fazem parte argumentos explicativos

evidenciando que o projeto INDECT é um projeto de investigação, e não um projeto de implementação. A implementação e utilização das ferramentas desenvolvidas está, segundo os mesmos, dependente do interesse de cada um dos Estados Membros da UE. A serem implementadas, as soluções desenvolvidas pelo INDECT iriam, segundo o coordenador do projeto, cumprir rigorosos requisitos de funcionamento. Igualmente fica esclarecida a missão do projeto que, muito sucintamente, visa reforçar a segurança dos cidadãos europeus protegendo a sua privacidade. Demonstrado fica pelos testemunhos, dos elogios e interesse (segundo admitido pelo entrevistado, percetíveis) ao projeto INDECT, por parte da Europol e autoridades policiais de vários Estados Membros. No que concerne à privacidade e proteção de dados dos cidadãos europeus, a coordenação do projeto INDECT sustenta que todos os projetos financiados no âmbito do FP7 são obrigados a cumprir critérios de tratamento de dados pessoais. Evidente em testemunho por entrevista fica a perentória afirmação da não existência de relação, entre o projeto INDECT e o programa Prism ou quaisquer outros programas e projetos de vigilância desenvolvidos pelos EUA e UE.

Por sua vez o movimento STOP INDECT, através do ativista entrevistado, deixa clara a sua mensagem de que enquanto movimento livre, promove a consciencialização e o debate acerca do projeto INDECT. Segundo o mesmo, o INDECT não dando garantias de uma aplicação futura clara pode, hipoteticamente, ser usado com fins abusivos de monitorização massificada, obtendo um conjunto ilimitado de informações pessoais dos cidadãos europeus, capacitando-o de formular padrões comportamentais, penalizando aqueles que “fogem à normalidade”. Enquanto ativista do movimento STOP INDECT, o entrevistado, questiona os fundamentos e a aplicabilidade do projeto da UE, face à Carta dos Direitos Fundamentais da União Europeia (especificamente os Artigos 7º, 8º e 11º). O STOP INDECT tem a Internet, nomeadamente as redes sociais *online*, como o veículo privilegiado de difusão de informação e de estimulação ao debate face ao INDECT. Relativamente ao tema da sociedade vigilante, o entrevistado relaciona o projeto INDECT com o programa Prism, no que concerne à violação da privacidade e da proteção de dados dos cidadãos.

Ainda referente ao movimento STOP INDECT, à informação presente na página de Facebook do movimento e ao testemunho de um dos seus ativista em entrevista, fica-nos a dúvida do total discernimento, por parte dos seus ativistas, face às especificidades e implicações do projeto INDECT. Como ponto referido, evidenciamos a subentendida ideia que fica do discurso do ativista entrevistado, de que o projeto INDECT é um projeto de implementação da UE e não como realmente é, um projeto de investigação da UE. Esta perceção, que sentimos necessidade de referenciar, é notória em argumentos em que o STOP INDECT incute responsabilidades de

fiscalização processual de uso de ferramentas (relativamente à privacidade e proteção de dados) ao próprio INDECT (projeto de investigação), e não aos Estados Membros (eventualmente interessados e utilizadores das ferramentas desenvolvidas pelo INDECT).

Contrapondo com os pareceres do STOP INDECT, os testemunhos em entrevista facultados pela Comissão Nacional de Proteção de Dados (CNPD), na pessoa da sua presidente, revelam um esclarecido conhecimento do projeto de investigação INDECT, das suas especificidades e implicações. A entrevistada enquadra o projeto como parte da política europeia de investimento nas questões de segurança, envolvendo mecanismos de vigilância de cidadãos, e como tal sujeito a uma atenta avaliação perante os direitos fundamentais. Evidencia ainda a incidência que o projeto INDECT dirige a ferramentas de trabalho policial, de controlo e deteção de ameaças e aos processos e procedimentos de pesquisa, seja pela integração de bases de dados, seja pelo cruzamento de informação em ambiente *online* e *offline*. A referência a esta principal incidência do INDECT, demonstrada pela presidente da CNPD, é de certa forma contraditória com os testemunhos dados em entrevista pelo coordenador do projeto INDECT, que evidencia e focaliza as investigações em ferramentas como a Marca d'água Digital e os Algoritmos Criptográficos (com finalidades menos controversas, focalizadas na proteção da privacidade e dos dados pessoais). Perante a temática da proteção de dados, a entrevistada refere a preocupação do Grupo de Trabalho de Proteção de Dados da UE (Grupo do Artigo 29.º) relativamente aos pressupostos de investigação do INDECT e ao potencial discriminatório que o *profiling* suporta. Perante o tema da sociedade vigilante e dos recentemente divulgados casos, implicando a NSA (EUA) e a GCHQ (RU), sustenta a necessidade de um escrutínio democrático referente à atuação das agências de segurança nacional. Finalizando enaltece o papel da literacia digital e de iniciativas como o Projeto Dadus, enquanto garante de uma maior alfabetização na atual Sociedade em Rede.

## 6. CONCLUSÃO

> "Daí o efeito mais importante do Panótico: induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder. (…) Para isso, é ao mesmo tempo excessivo e muito pouco que o prisioneiro seja observado sem cessar por um vigia: muito pouco, pois o essencial é que ele se saiba vigiado; excessivo, porque ele não tem necessidade de sê-lo efetivamente" (Foucault, 1977: 191).

Retomando os argumentos de Michel Foucault, na sua obra *Vigiar e Punir: História da Violência nas Prisões*, e contrapondo-os aos paradigmas da vigilância na sociedade contemporânea, verificamos efetivamente que a vigilância é disseminada, não se extinguindo em edifícios, fortalezas, escolas ou prisões, que atua e desempenha o seu papel, na administração do poder, em ambientes *online* e *offline*. A "casa de certeza", como Foucault designou o Panótico de Jeremy Bentham (Foucault, 1977), que se representava como um instrumento de domínio delimitado espacialmente, assume na sociedade atual uma configuração radicalmente distinta. A "casa de certeza" é cada vez mais um "espaço" não circunscrito e globalizado.

Igualmente desatualizados estão os argumentos de Foucault que identificam e caraterizam (exclusivamente) a amplitude de ação do Panótico a uma vigilância não necessariamente contínua, no entanto evidente e explícita no exercício do poder. Atualmente, o referido exercício de poder, perpetrado através da vigilância e auxiliado pelos inúmeros avanços tecnológicos, nomeadamente pelo advento da Sociedade em Rede, identifica novas exigências e atua massivamente, interruptamente e por vezes dissimuladamente perante a sociedade. Arriscando uma reformulação na contextualização da vigilância na sociedade contemporânea, com base no Panótico de Foucault: A monitorização é atualmente efetivada de duas formas: Uma primeira, identificada por Foucault e com evidentes propósitos de assegurar poder, onde a vigilância é permanente nos seus efeitos, mesmo que seja descontínua nas suas ações (Foucault, 1977). Uma segunda forma de monitorização, a juntar à identificada por Foucault, que complementa o exercício de poder, robustecendo-o, é efetivada através de uma vigilância massificada das populações por entidades governamentais ou empresariais; que também é contínua para ser objetivamente mais eficaz e por existirem atualmente meios tecnológicos para o fazer; e perpetrada quer com objetivos empresariais, que são de conhecimento generalizado, como é o caso do rastreio de hábitos *online* efetuado por empresas multinacionais; quer com fundamentos de segurança e policiamento (e porque não espionagem) com a vigilância de muitos

milhões de utilizadores de plataformas digitais, como foi denunciado por Edward Snowden, em meados do ano de 2013.

Foucault abordando ainda a vigilância como ferramenta de poder, adianta que:

> "O Panótico funciona como uma espécie de laboratório de poder. Graças a seus mecanismos de observação, ganha em eficácia e em capacidade de penetração no comportamento dos homens: um aumento de saber vem se implantar em todas as frentes do poder, descobrindo objetos que devem ser conhecidos em todas as superfícies onde se exerça" (Foucault, 1977: 194).

A atual Sociedade de Risco, através do Pânico Moral perpetrado por governantes e *media*, salvaguardando os interesses múltiplos de grupos de pressão (*lobby*), legitima a vigilância, robustecendo o poder. O atentado do 11 de setembro de 2001, principiador da denominada Guerra ao Terror, apontado por Ulrich Beck como o vórtice da atual Sociedade de Risco, tem fomentado desde então um conjunto vasto de receios sobrevalorizados (Pânicos Morais), que por sua vez precipitam a tomada de medidas governamentais que muitas vezes colocam em causa direitos fundamentais, como o da privacidade.

A amplitude e profusão dos panóticos na sociedade contemporânea surpreenderia Bentham, que segundo a obra de Foucault (1977), idealizava com uma rede de dispositivos (panóticos) que "estariam em toda a parte e sempre alertas, percorrendo a sociedade sem lacuna nem interrupção" (Foucault, 1977: 197). Novos paradigmas de vigilância emergem, com diferentes configurações e aplicabilidades, viabilizados pelos constantes avanços tecnológicos, atuando tanto no espaço físico, criando ferramentas policiais, como sofisticados *drones* munidos com potentes câmaras de vigilância ou *CCTV*'s fazendo uso de algoritmos avançados; como no espaço virtual, nomeadamente na Sociedade em Rede, onde a amplitude das aplicabilidades é infinitamente maior que no espaço físico.

Episódios como as recentes revelações do mediático *whistleblower*[41] Snowden, ou do menos mediático, mas igualmente denunciador, James Bamford (autor e jornalista) implicando explicitamente a agência de segurança nacional norte-americana (NSA) em crimes de vigilância massificada; ou ainda do controverso Julian Assange, que com a Wikileaks expõe periodicamente centenas de documentos *online* - *The Spy Files*[42] - referentes à indústria mundial da vigilância massificada, surgem junto à opinião pública e trazem à discussão os limites da vigilância. O debate em torno da

[41] Denunciador é uma pessoa que expõe uma má conduta, suposta atividade desonesta ou ilegal que ocorre numa organização perante a sociedade civil e as autoridades públicas.
[42] https://www.wikileaks.org/the-spyfiles.html

controversa temática adensa-se, torna-se altamente mediático e é discutido por entre os vários quadrantes da sociedade. A título de curiosidade, mas revelador da pertinência do tema, logo após as revelações da existência do programa Prism, por parte de Snowden, a já referida obra *1984* de George Orwell, datada de 1949, passou a integrar provisoriamente o Top 100 de vendas da Amazon, com um aumento de 7,000% nas vendas (Moss, 2011).

No "caso português", como referenciado por Catarina Frois (2008), não existindo uma real ameaça terrorista ou criminal como nos EUA ou Reino Unido, a modernização e o combate ao atraso dos serviços públicos e estatais, surgem como fundamentos para muita da implementação de sistemas inovadores frequentemente associados à monitorização governamental. São exemplo as implementações de sistemas de videovigilância na via pública, por parte do Programa Nacional de Videovigilância, e a base de dados de perfis de ADN para fins de identificação civil e criminal (Machado, Frois, 2014). É neste contexto, de busca de integração e pertença, que Portugal assina o controverso acordo referente à *Terrorist Watchlist*[43], que essencialmente determina, como forma de combate ao terrorismo, a obrigatoriedade de comunicação aos EUA, por parte das autoridades portuguesas, de quaisquer indícios de atividades terroristas em território português.

Num outro domínio, com aplicabilidade distinta, surge a vigilância centralizada no consumidor e nos seus hábitos de consumo, perpetrada essencialmente por entidades empresariais multinacionais. A designada por Zygmund Bauman de "Vigilância Líquida" (Bauman, Lyon: 2013), como parte de uma "Modernidade Líquida"[44] (Bauman, 2000) pretende espelhar a orientação da vigilância numa atual modernidade fluída, inquietante e imprevisível. Esta "Vigilância Líquida" assume uma especial relevância na atual Sociedade em Rede, com o apogeu da Web 2.0. Igualmente representativas desta mesma fluída vigilância surgem as *cookie*[45], que permitem identificar historiais de pesquisa dos utilizadores (consumidores) na Internet. Roger Clarke identifica esta como uma das práticas de *dataveillance*[46] (Clarke, 1999).

Tendo abordado, em dissertação, uma multiplicidade de aplicabilidades da vigilância na atualidade, é com a vertente da vigilância governamental, com fins de

[43] Entre a República Portuguesa e os EUA para a Troca de Informação de Rastreio do Terrorismo, assinado em Washington em 24 de julho de 2012, aprovado pela Resolução da Assembleia da República n.º 51/2013, em 15 de fevereiro de 2013.

[44] Terminologia introduzida por Zygmund Bauman (2000) e refere-se à época atual em que vivemos. É o conjunto de relações e instituições, além de sua lógica de operações, que se impõe e que dão base para a contemporaneidade. Época de liquidez, de fluidez, de volatilidade, de incerteza e insegurança.

[45] Ficheiro de texto que é depositado no disco rígido do computador, quando se entra num *website*, criando um número de identificação único para aquele computador.

[46] Terminologia introduzida por Roger Clarke e que se refere à vigilância das atividades de indivíduos estudando os trilhos de dados criados por uso de cartão de crédito, telemóvel, e Internet.

controlo de segurança e policiamento, mais propriamente com o programa de investigação da União Europeia INDECT, que efetuaremos as mais elaboradas apreciações conclusivas. Após reflexão ao estudo de caso do INDECT, é com algumas interrogações que assistimos ao desenvolvimento de projetos de investigação, cofinanciados e apoiados pela União Europeia, suscitadores de incertezas face ao efetivo respeito pela privacidade dos cidadãos europeus.

Não tendo considerado, intencionalmente, o escrutínio da opinião pública no estudo levado a cabo, não existe efetivamente conclusão a tirar acerca do conhecimento, por parte da sociedade portuguesa, da existência do INDECT, das suas implicações e especificações. Contudo, a incidência do estudo efetuado é reveladora de um desconhecimento aprofundado, por parte do movimento STOP INDECT, ao momento o mais notório crítico ao projeto, de algumas particularidades do INDECT, nomeadamente no que se refere ao campo de ação (ser um projeto de investigação e não de implementação como sugerido pelo ativista do movimento STOP INDECT).

Igualmente conclusivo com o estudo do INDECT, e como já evidenciado anteriormente, é que existem duas opiniões face ao INDECT, por vezes extremadas. Um dos considerados na investigação, o movimento STOP INDECT, é claramente contra o projeto, recorrendo por vezes a uma menos rigorosa objetividade na sua análise crítica. Por sua vez e por outro lado, o INDECT, com o seu grupo de investigação e consórcio, vale-se de argumentos justificativos e legitimativos para as investigações propostas, não declarando explicitamente a sua efetiva missão e objetivos.

Das opiniões fundamentadas pelos três implicados na análise do estudo de caso - INDECT, STOP INDECT e CNPD - sobressai a opinião da Comissão Nacional de Proteção de Dados (CNPD), pelo conhecimento concreto do âmbito do projeto de investigação, das suas implicações e especificações. Sobressai igualmente pelo facto de não partilhar opinião com nenhuma das duas fações, nem consórcio e nem movimento, assumindo o seu papel de entidade independente, com atribuições genéricas de controlar e fiscalizar o processamento de dados pessoais, realizando discernidas considerações face à rigorosa aplicabilidade da lei.

Finalizado, a 30 de junho de 2014, o período de investigação do projeto INDECT, segue-se a divulgação por parte do consórcio INDECT, dos resultados junto a entidades governamentais competentes dos Estados Membros da UE. Partilhando da opinião veiculada pela CNPD, torna-se primordial neste momento o discernimento das referenciadas entidades governamentais competentes, perante à aplicabilidade das ferramentas propostas, com vista a assegurar a privacidade e proteção de dados dos cidadãos europeus.

"Para onde vamos a partir daqui?" (Rule, 2007: 190).

Reproduzindo o título interrogativo do capítulo conclusivo da obra de James Rule, *Privacy in Peril* (2007), mas com enfoque na vigilância (e forçosamente na privacidade) enunciamos três acontecimentos ou casos que poderão indiciar algumas alterações no panorama atual da vigilância, nomeadamente na proteção de dados pessoais, em ambiente digital. Não sendo a temática predominante da dissertação, esta referente a projetos de investigação como o INDECT, consideramos no entanto relevante identifica-los. O primeiro caso prende-se com uma recente decisão (de 13 de maio de 2014) do Tribunal de Justiça da União Europeia (TJUE), e comunicada por parte da empresa multinacional de serviços *online* Google, do reconhecimento por parte da UE do direito a ser esquecido na Internet. Face ao decretado pelo TJUE, a Google disponibilizou de imediato, para os 28 países da UE (mais Islândia, Liechtenstein, Noruega e Suíça), um formulário *online*[47] para a solicitação de remoção de dados pessoais dos utilizadores. O segundo caso que gostaríamos de evidenciar prende-se com o surgimento da organização Europe vs Facebook[48], fundada por Max Schrems, e que em meados de 2013 contava já com 22 queixas e com inúmeros processos em tribunal, contra o Facebook (Anjos, 2013). A razão por detrás de tais ações prende-se com a acusação de violação das regras europeias da privacidade. Por fim o terceiro caso, comunicado pelos *media* no início de setembro de 2014, reporta-se também ele à rede social Facebook e à disponibilização de uma opção, um "*checkup* de privacidade", sensibilizando e permitindo os utilizadores (mais de 1 bilião) a rever e a configurar os seus dados pessoais na aplicação (Guynn, 2014).

Considerando a interrogação colocada anteriormente, surgem importantes sinais reveladores da pertinência de vigiar a vigilância, de a estudar e às suas implicações, de a controlar e fiscalizar. Enumeramos, a título exemplificativo, a entidade Surveillance Studies Network[49] (SSN), com o seu jornal *online* Surveillance and Society[50], e o programa de investigação europeu Living in Surveillance Societies[51] (LISS), evidenciando o relevante papel que realizam no âmbito dos estudos de vigilância. Assinalamos igualmente, na última década, o acréscimo da publicação de artigos e obras, no campo dos estudos de vigilância (Haggerty, Lyon, Ball, 2012).

Referente ao controlo e fiscalização dos limites da vigilância consideramos importante, a um nível supranacional, identificar e valorizar os pareceres de órgãos

[47] https://support.google.com/legal/contact/lr_eudpa?product=websearch
[48] http://europe-v-facebook.org/EN/en.html
[49] http://www.surveillance-studies.net/
[50] http://www.surveillance-and-society.org/
[51] http://www.liss-cost.eu/

consultivos europeus independentes, como o já referenciado Grupo do Artigo 29.º, com vista a apreciar rigorosamente as implicações do financiamento de projetos, que de algum modo possam pôr em causa os direitos fundamentais dos cidadãos. Por outro lado, a um nível nacional, consideramos importante valorizar o papel de entidades como a CNPD, repondo nas suas competências, por exemplo, poderes de atribuição de pareces vinculativo face à instalação de câmaras de vigilância no espaço público.

Como reflexão final apraz-nos dizer que encaramos o estímulo à literacia digital como uma medida primordial, no que concerne à proteção de dados pessoais dos indivíduos, à conservação da privacidade das comunidades e por consequente ao combate à vigilância.

Para terminar, cumpre-nos adiantar a finalidade da presente dissertação de mestrado em abrir pistas e linhas de investigação futuras, na área dos estudos de vigilância.

## Bibliografia


Albrechtslund, A. (2008), *Online Social Networking as Participatory Surveillance*, First Monday 13(3).

Andrejevic, M. (2002), "The Work of Being Watched: Interactive Media and the Exploitation of Self-Disclosure", *Critical Studies in Media Communication*, 19 (2), pp. 230-248.

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

Andrejevic, M. (2007), *iSpy: Surveillance and Power in the Interactive Era (Culture America)*, University Press of Kansas.

Anjos, M. (2013), "Privacidade", *Revista do Expresso*, 2125, pp. 30-39.

Bauman, Z. (2000), *Liquid Modernity*, Cambridge, UK, Polity Press.

Bauman, Z. and Lyon, D. (2013), *Liquid Surveillance: A Conversation*, Cambridge, UK, Polity Press.

Beck, U. (2002), "The Terrorist Threat – World Risk Society Revisited", *Theory, Culture & Society 2002* (Sage), Vol. 19 (4), pp. 39-55.

Bell, J. (1997), *Como Realizar um Projeto de Investigação*, Coleção Trajetos, Lisboa, Gradiva Publicações S.A..

Borges, J.e Oliveira, L. (2011), "Competências Infocomunicacionais em Ambientes Digitais", *Observatório (OBS*)* Journal, vol.5 - nº4 (2011), pp. 291-326.

Buck, A. (2012), "Examining Digital Literacy Practices on Social Network Sites", *Research in the Teaching of English*, Volume 47, Number 1, August, pp. 9-38.

Cardoso, G., Nascimento, S., Morgado, A. e Espanha, R. (2005), *Democracia Digital – Eleitos e Eleitores na Era da Informação*, Oeiras, Celta Editora.

Castells, M. (2001), *The Internet Galaxy: Reflections on the Internet, Business, and Society*, Oxford University Press.

Castells, M. e Cardoso, G. (org.) (2005), *A Sociedade em Rede: do Conhecimento à Ação Política*; Conferência. Belém (Por), Imprensa Nacional.

Clarke, R. (1999), "Internet Privacy Concerns Confirm the Case for Intervention", *Magazine Communications of the ACM,* Volume 42*,* Issue 2*,* New York*,* USA.

Cohen, S. (1972), *Folk Devils and Moral Panics*, MacGibbon and Kee, Ltd.

Cottrill, C. (2011), "Location Privacy: Who Protects?" *Urisa Journal*, pp. 49-59.

Deleuze, G. (1992), *Conversações: 1972-1990*, Paris, Les Éditions de Minuit.

Deleuze, G. (2005 [1988]), *Foucault*, São Paulo, Brasil, Editora Brasiliense S.A..

Estêvão, T. (2014), "O Novo Paradigma da Vigilância na Sociedade Contemporânea – "Who Watches the Watchers", *Observatório (OBS*)*, Vol.8, nº 2, [online] retirado de: http://obs.obercom.pt/index.php/obs/article/view/787

Flick, U. (2005), *Métodos Qualitativos na Investigação Científica*, Lisboa, Monitor – Projetos e Edições, Lda.

Fonio, C. (2008), "Vigilância e Identidade: Para uma Nova Antropologia da Pessoa", *A Sociedade Vigilante – Ensaios Sobre Identificação, Vigilância e Privacidade*, (org. Catarina Frois), Lisboa, Imprensa de Ciências Sociais.

Foucault, M. (1999 [1977]), *Vigiar e Punir – Nascimento de uma Prisão*, Editora Vozes, Petrópolis, Brasil.

Frois, C. (2008), "Bases de Dados Pessoais e Vigilância em Portugal: Análise de um Processo em Transição" em *A Sociedade Vigilante - Ensaios Sobre Identificação, Vigilância e Privacidade* (org. Catarina Frois), Lisboa, Imprensa de Ciências Sociais.

Frois, C. (2011), *Vigilância e Poder*, Lisboa, Editora Mundos Sociais.

Frois, C. (2013), *Peripheral Vision - Politics, Technology and Surveillance*, London and New York, Berghahn Books.

Fuchs, C. (2008), *Internet and Society: Social Theory in the Information Age*, New York: Routledge.

Fuchs, C. (2011), *New Media, Web 2.0 and Surveillance*, Sociology Compass 5/2.

Fuchs, C., Boersma, K, Albrechtslund, A. and Sandoval, M. (2011), *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*, New York and London, Routledge.

Gates, K. (2012), "The Globalization of Homeland Security", ", in Haggerty, K., Lyon, D., *Routledge Handbook of Surveillance Studies*, (ed. Kirstie Ball) London and New York, Routledge.

Giddens, A. (1985), *The Nation-State and Violence*, Cambridge, England, Polity Press.

Greenwald, G. (2014), *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, New York, USA, Metropolitan Books.

Guynn, J. (2014), "Facebook Rolling Out Privacy Checkup for Users", *USA TODAY* [online] retirado de: http://www.usatoday.com/story/tech/2014/09/04/facebook-privacy-checkup-tool/15067743/ [acedido: 7 setembro 2014].

Haggerty, K., Lyon D. and Ball, K. (2012), "Introducing Surveillance Studies", in Haggerty, K., Lyon, D., (ed. Kirstie Ball), *Routledge Handbook of Surveillance Studies*, London and New York, Routledge.

Harding, L. (2014), *The Snowden Files – The Inside Story of the World's Most Wanted Man*, New York, USA, Vintage Books.

Koskela, H. (2004), "Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism", *Surveillance & Society* 2 (2/3), pp. 199-215.

Levin, T. (2010), *Surveillance, Aesthesis, Literacy - 25: An Anthology for the 25th Anniversary of BIT Teatergarasjen*, Published Nordic Culture Point, Arts Council Norway.

Lyon, D. (1994), *The Electronic Eye – The Rise of Surveillance Society*, Minneapolis, USA, Polity Press.

Lyon, D. (1998), "The World Wide Web of Surveillance: The Internet and Off-World Power" – *Flows, Information, Communication & Society* 1.1 (Spring 1998), pp. 91-105.

Lyon, D. (2001), *The Surveillance Society – Monitoring Everyday Life*, Buckingham, England, Open University Press.

Lyon, D. (2003), "Surveillance Technology and Surveillance Society", in *Modernity and Technology*, (ed. Thomas J. Misa, Phlip Brey and Andrew Feenberg), pp. 161-184, Cambridge: MIT Press.

Lyon, D. (2004), *Identity Cards: Social Sorting by Database*, Oxford Internet Institute. Internet issue brief 3: pp. 1-14.

Lyon, D. (2007), *Surveillance Studies – An Overview*, Cambridge, England, Polity Press.

Machado, H. e Silva, S. (2008), "Confiança, Voluntariedade e Supressão dos Riscos: Expectativas, Incertezas e Governação das Aplicações Forenses de Informação Genética" em *A Sociedade Vigilante - Ensaios Sobre Identificação, Vigilância e Privacidade* (org. Catarina Frois), Lisboa, Imprensa de Ciências Sociais.

Machado, H. and Frois, C. (2014), "Aspiring to Modernization: Historical Evolution and Current Trends of State Surveillance in Portugal" in *Histories of State Surveillance in Europe and Beyond*, (Ed. Kees Boersma, Rosamunde Van Brakel, Chiara Fonio and Pieter Wagenaar), New York and London, Routledge.

Mann, S. (2003), "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments", *Surveillance & Society* 1(3): pp. 331-355.

Marx, G. T. (2002), "What's New About the New Surveillance? Classifying for Change and Continuity", *Surveillance & Society* 1 (1): 9–29.

McCloskey, H.J. (1985), "Privacy and the Right to Privacy", In: Purtill, R.L. (Ed.), *Moral Dilemmas: Readings in Ethics and Social Philosophy*, Wadsworth, Belmont, CA, pp. 342–357.

Meuser, M and Nagel, U. (1991), "Expertlnneninterviews: Vielfach Erprobt, Wenig Bedacht. Ein Beitrag zur Qualitativen Methodendiskussion", in D. Garz and K. Kraimer (eds), *Qualitativ-Empirische Sozial Forschung Opladen*: Westdeutscher Verlag, pp. 441-68.

Moss, S. (2011), "George Orwell Back in Fashion as Prism Stokes Paranoia About Big Brother", *The Guardian* [online] retirado de: http://www.theguardian.com/books/booksblog/2013/jun/11/george-orwell-prism-big-brother-1984 [acedido: 22 agosto 2014].

Motta, F. e Alcadipani, R. (2004), "O Pensamento de Michel Foucault na Teoria das Organizações", R. Adm., São Paulo, v.39, n.2, pp. 117-128.

Norris, C., McCahill, M. and Wood, D. (2004), "The Growth of CCTV: A Global Perspective on the International Diffusion of Video Surveillance in Public Accessible Space", *Surveillance & Society*, 2 (2-3), pp.110-135.

O'Hara, K. e Shadbolt, N. (2009), *O Espião na Máquina do Café*, Lisboa, Portugal, Plátano Editora.

Orwell, G. (1999 [1949]), *1984 - Mil Novecentos e Oitenta e Quatro*, Lisboa, Antígona.

Papacharisse, Z. and Gibson, P. (2011), "Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites", *Privacy Online: Theoretical Approaches and Research Perspectives on the Role of Privacy in the Social Web*.

Pidd, H. (2011), "Facebook Facial Recognition Software Violates Privacy Laws, says Germany", *The Guardian* [online] retirado de:

http://www.theguardian.com/technology/2011/aug/03/facebook-facial-recognition-privacy-germany [acedido: 14 abril 2014].

Qiu, J. (2007), "The Wireless Leash: Mobile Messaging Service as a Means of Control", *International Journal of Communication* 1, pp. 74-91.

Rothe, D. and Muzzatti, S. (2004), "Enemies Everywhere: Terrorism, Moral Panic, and US Civil Society", *Critical Criminology* (12), pp. 327-350.

Rule, J. (2007), *Privacy in Peril*, New York, USA, Oxford University Press.

Salter, M. (2008), "The Global Airport: Managing Space, Speed, and Security", *Politics at the Airport* (ed. Mark Salter), Minneapolis, University of Minnesota Press.

Scheneider, C. and Trottier, D. (2012), "The 2011 Vancouver Riot and the Role of Facebook in Crowd-Sourced Policing", *BC Studies*, nº 175, pp. 57-72.

Staples, W. (2000), *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, New York, USA, Rowman and Littlefield.

Tavani, H. (2008), "Informational Privacy: Concepts, Theories, and Controversies", in *Handbook of Information and Computer Ethics*, (ed. Kenneth Himma and Herman Tavani), pp. 131-165, New Jersey, John Wiley & Sons, Inc.

Thompson, K. (1998), *Moral Panics*, New York and London, Routledge.

Traynor, I. (2013), "EU Threatens to Suspend Deal with US on Tracking Terrorists' Funding", *The Guardian* [online] retirado de: http://www.theguardian.com/world/2013/sep/24/eu-threat-us-data-sharing-terrorist-funding [acedido: 21 junho 2014].

Trottier, D. (2012), "Policing Social Media", *Canadian Sociological Association*, pp. 411-425.

Trottier, D. (2013), "Crowdsourcing CCTV Surveillance on the Internet", *Information, Communication & Society*, DOI:10.1080/1369118X.2013.808359.

Turow, J. (2005), "Audience Construction and Culture Production: Marketing Surveillance in the Digital Age". T*he ANNALS of the American Academy of Political and Social Science* 597 (1), pp. 103-121.

Turow, J. (2006), "Cracking the Consumer Code: Advertising, Anxiety and Surveillance", in the Digital Age. In the *New Politics of Surveillance and Visibility*", (ed. Kevin Hagerty and Richard V. Ericson), pp. 279-307, Toronto: University of Toronto Press.

Warren, S. and Brandeis, L. (1890), "The Right to Privacy - Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890*)", The Harvard Law Review Association*, pp. 193-220.

Welinder, Y. (2012), "A Face Tells More Than a Thousand Posts: Developing Face Recognition Privacy in Social Networks", *Harvard Journal of Law & Technology*, Volume 26 - 1.

Westin, A. (1967), *Privacy and Freedom*, Atheneum, New York.

Whitaker, R. (1999), *The End of Privacy: How Total Surveillance Is Becoming a Reality*, New York: New Press.

## Anexos

**Anexo 1** (Guião de entrevista ao INDECT)

1) What do you consider the main reasons for the creation of a European research program as INDECT?

2) According to information collected in the EU CORDIS website, the period of the research project INDECT ends June 30, 2014. Which is the development of the project after its end date?

3) Which use, until the moment, the various EU member states have made from the technological tools developed by INDECT?

4) What are your expectations regarding the future adoption of these tools?

5) How do you see the current spread of surveillance programs and projects developed by the USA and EU?

6) How do you see the emergence of revelations concerning a U.S. program called PRISM and mass surveillance of Americans and Europeans?

7) There are some groups on the Internet, especially in social networks (e.g. Stop Indect), who argue that an EU research project, with these characteristics, enables the European states to take advantage of surveillance tools, violating citizens' privacy. To what extent is guaranteed the exclusive applicability of the tools, developed by INDECT, to the areas indicated on the website?

8) In its opinion on what terms is that development projects like INDECT guarantee and are not antagonistic with respect for privacy and protection of personal data of European citizens - in particular, from Articles 7 and 8 of the Charter of Fundamental Rights of the European Union?

9) It is widely evidenced in the institutional website of INDECT, the Board of Ethics and the ethical concerns and solutions with the research project. At the same time is not clear the ethical concerns with putting these solutions into the field. Who oversees the inspection, on the various member states, of the applicability of these solutions?

10) One of the main features of INDECT, present on his mission, is the development of solutions using advanced algorithms. How far is that this set of technological solutions, which arise under the guise of making our society safer, does not make our society a highly vigilant society?

**Anexo 2 (**Guião de entrevista ao STOP INDECT)

1) Qual o papel do STOP INDECT?

2) Quais considera serem as principais razões para a criação de um programa de investigação europeu como o INDECT?

3) Quais as principais críticas que fazem ao INDECT?

4) Como vê a atual disseminação de programas e projetos de vigilância desenvolvidos pelos EUA e UE?

5) Como vê o surgimento de revelações referentes a um programa norte-americano intitulado de PRISM e à vigilância massificada de cidadãos americanos e europeus?

6) Os movimentos anti INDECT, visíveis na Internet e de diversas proveniências, têm uma presença evidente dos Anonymous. O mesmo se passa em Portugal?

7) STOP INDECT está presente na Internet através de sites, blogs e nas redes sociais em ferramentas como o Facebook e Twitter. Que ações de consciencialização, face o INDECT, são realizadas pelo STOP INDECT em Portugal?

8) Quais considera serem as principais consequências, ao nível da privacidade no contexto dos cidadãos europeus, com a implementação de sistemas de vigilância utilizando algoritmos avançados, como no caso do INDECT?

9) No contexto nacional verificaram-se alterações na Lei da videovigilância (Lei nº 9/2012 de 23 de fevereiro). A prevenção de atos terroristas surge como um dos justificativos para a implementação de sistemas de videovigilância. Igualmente verifica-se uma passagem do poder vinculativo, na definição de locais na via pública sujeitos a videovigilância, da Comissão Nacional de Proteção de Dados para o Ministério da Administração Interna. Perante estas mudanças, quais as suas expetativas na adoção pelo governo português, dos sistemas de videovigilância utilizando algoritmos avançados?

10) No site institucional do INDECT existe uma evidente preocupação com as questões éticas em que está envolto o projeto de investigação. Quais são, na sua opinião, as principais lacunas da Comissão de Ética do INDECT?

**Anexo 3** (Guião de entrevista à CNPD)

1) Tem conhecimento de projetos de investigação, cofinanciados pela União Europeia, que desenvolvam soluções de apoio à decisão humana, com vista a proteger o cidadão em ambiente urbano, como é o caso do INDECT?

2) Na sua opinião em que termos é que o desenvolvimento de projetos como o INDECT, asseguram e não são antagónicos com o respeito pela privacidade e proteção de dados pessoais dos cidadãos europeus - em especial, face aos artigos 7º e 8º da Carta dos Direitos Fundamentais da União Europeia?

3) No contexto nacional verificaram-se alterações na Lei da videovigilância (Lei nº 9/2012 de 23 de fevereiro). A prevenção de atos terroristas surge como um dos justificativos para a implementação de sistemas de videovigilância. Igualmente verifica-se uma passagem do poder vinculativo, na definição de locais na via pública sujeitos a videovigilância, da Comissão Nacional de Proteção de Dados para o Ministério da Administração Interna. Na sua opinião estas alterações na Lei poderão viabilizar e facilitar a implementação da videovigilância na via pública?

4) Como vê as atuais políticas europeias de proteção de dados?

5) Considera que a mudança de uma diretiva europeia de proteção de dados, para um regulamento europeu de proteção de dados implementará mais medidas de proteção da privacidade dos cidadãos europeus?

6) Em traços gerais que alterações significativas estão atualmente presentes nesta proposta de passagem a um regulamento europeu de proteção de dados?

7) A par da transição para um regulamento europeu de proteção de dados, como vê a atual importância que a União Europeia tem vindo a dedicar a ferramentas de controlo fronteiriço como o SIS II (Sistema de Informação Schengen de segunda geração) e a projetos de investigação como o INDECT?

8) Em que medida não serão as duas ultimas situações reportadas, que em última análise fomentam a vigilância no espaço europeu, antagónicas a uma regulamentação europeia de proteção de dados?

9) Como vê o surgimento de revelações referentes à vigilância massificada de cidadãos americanos e europeus, por parte de entidades como a norte americana NSA e a sua congénere britânica GCHQ?

10) No ano de 2008 a CNPD criou o Projeto Dadus que visava facultar a população estudantil do 2º e 3º Ciclos do Ensino Básico, de esclarecimentos relativos à proteção de dados pessoais na Internet. Em que medida estes mesmos esclarecimentos não deveriam ser promovidos junto a uma população adulta e idosa?