TÉCNICO LISBOA

FACULDADE DE DIREITO
UNIVERSIDADE DE LISBOA

Os Direitos de Personalidade na Sociedade de Informação:

Os cidadãos perante os desafios da privacidade

Ricardo Miguel Ribeiro da Mata

Dissertação para a obtenção do Grau de Mestre em Segurança de Informação e Direito no Ciberespaço

Orientador: Professor Doutor Eduardo Vera Cruz

Co-orientador: Professor Doutor Carlos Caleiro

Júri

Professora Ana Fouto

Lisboa, 31 de outubro de 2019

Agradecimentos

Um trabalho de mestrado é uma jornada longa e por vezes penosa, portanto gostaria de agradecer a um conjunto de pessoas que eu acredito que sem eles não seria possível concluir esta etapa da minha vida.

Ao meu orientador, *Professor Doutor Eduardo Vera-Cruz*, pelo privilégio que me deu de ter feito parte desta última etapa académica, ao qual agradeço a sua inspiração e assertividade em apontar as direções a seguir, ficando a expetativa que a amizade se mantenha para o futuro.

Ao meu co-orientador, *Professor Doutor Carlos Caleiro*, pela disponibilidade que sempre demonstrou na elaboração deste trabalho e de todo o acompanhamento ao longo dos últimos dois anos

Aos meus pais, que como sempre o fizeram ao longo da minha vida me apoiaram imenso durante esta caminhada. Obrigado também pelo ânimo que me foram transmitindo nos momentos em que mais precisei, sem vocês seria impossível ter concluído este desafio. Acima de tudo, espero recompensar-vos com orgulho o resto da vida.

À minha namorada, que me motivou desde o primeiro minuto, me ajudou em tudo mesmo quando nada lhe era pedido e me deu na cabeça quando tal era necessário.

Aos meus amigos, que estiveram sempre ao meu lado e me ajudaram a relaxar quando o stress já era demasiado.

Ao meu cão que, embora seja um animal não racional, era por vezes um poço de abrigo quando mais eu precisava e me ajudava a desligar do mundo sempre, sem protestar.

Um obrigado a todos, esta dissertação é minha, mas também é vossa.

Resumo

Dado o crescimento de casos de violação de dados pessoais e, pouco a pouco, a consciencialização do cidadão comum sobre esse assunto, sentimos que era interessante realizar uma pesquisa da legislação vigente, não apenas em Portugal, mas também na Europa, e tentar descobrir, com recurso a um questionário, se os portugueses se encontram cientes da maneira como a privacidade é tratada em todo o mundo e se eles se importam com o facto de os seus dados pessoais serem usados sem escrúpulos pelas empresas e também pelo governo. Atualmente, encontramo-nos num momento de consciencialização da sociedade (sendo que aqueles responsáveis por gerir as grandes empresas e, portanto, por controlarem as informações numa escala enorme são os mais importantes para isso), devido ao facto de surgirem cada vez mais casos do uso indevido de dados, causando uma preocupação maior nos cidadãos. O crescente uso das redes sociais na nossa rotina diária e os perigos que o uso excessivo e desinformado implica, serão também uma questão de análise.

Depois de analisarmos o estado atual da legislação, com foco especial no novo regulamento europeu de dados, o RGPD (Regulamento Geral de Proteção de Dados), que é a mudança mais importante no modo como se lida com os dados pessoais nos últimos 20 anos, tentaremos entender como é que o cidadão comum se sente relativamente à maneira como os seus dados são tratados atualmente de acordo com as normas em vigor e a sua predisposição para alterar a maneira como lidam com seus dados pessoais nas suas vidas. No final, deixaremos algumas recomendações sobre como a nossa privacidade pode ser mais respeitada diariamente sem que isso comprometa a segurança nacional.

Palavras-chave: Privacidade; Segurança; Direitos de Personalidade; Vigilância; Ciberespaço.

Abstract

Given the growth of cases of violation of personal data and, little by little, the awareness of the ordinary citizen regarding this subject, we felt that it was interesting to carry out a research of the current legislation not only in Portugal, but also in Europe, and try to figure out, using a questionnaire, if the Portuguese are aware of the way privacy is handled worldwide and if they care about their personal data being used unscrupulous by companies and also the government. We are now in a time of raising awareness in the society (being that those who are managing the big companies and therefore controlling information in an enormous scale are the more important ones to do that) due to the fact that more and more cases of data misusing have arisen, causing a bigger concern in the citizens. The increasing use of the social media in our daily routine and the dangers that the excessive and uninformed use entails will also be a matter of analysis.

After analysing the current state of the legislation, with special focus on the new European data regulation, the GDPR (General Data Protection Regulation) which is the most important change in data protection regulation in the last 20 years, and try to understand how the ordinary citizen feels about how the data is being managed and their willingness to improve the way they handle their personal data in their daily lives, we will leave some recommendations on how we can improve our privacy without compromising the national security.

Keywords: Privacy; Security; Personality Rights; Surveillance; Cyberspace.

Índice

Lista de figuras

Lista de abreviaturas

ACLU - União Americana pelas Liberdades Civis

ANACOM – Autoridade Nacional de Comunicações

BDSG – Bundesdatenschutzgesetz

BFDI – Federal Commissioner for Data Protection and Freedom of Information

CC – Código Civil

CEDH – Convenção Europeia dos Direitos do Homem

CEO – Chief Executive Officer

CNPD – Comissão Nacional de Proteção de Dados

CRP – Constituição da República Portuguesa

DPA – Data Protection Act

DSK – Data Protection Conference

DUDH – Declaração Universal dos Direitos Humanos

UE – União Europeia

FDPA – Federal Data Protection Act

GPS – Global Positioning System

IP – Internet Protocol

IoT – Internet of Things

NSA – Agência de Segurança Nacional

ONG – Organização não Governamental

PIDCP – Pacto Internacional sobre os Direitos Civis e Políticos

RFID – Radio Frequency Identification

RGPD – Regulamento Geral de Proteção de Dados

TFUE – Tratado sobre o Funcionamento da União Europeia

TJUE – Tribunal de Justiça da União Europeia

TUE - Tratado da União Europeia

VPN - Virtual Private Network

WSN - Wireless Sensor Network

WWW – World Wide Web

Introdução

"Na Internet, se estiver a consumir ou a usar algo de graça, tenha a certeza: você é o produto." – Rafael Esberard

É cada vez mais reconhecido pela sociedade aquilo que são os impactos das tecnologias, particularmente o seu uso desmesurado na vida de cada um de nós. A permanente revolução tecnológica em que vivemos começou a surgir por volta do ano de 1975 e, com o passar dos anos, aumentou também a velocidade das mudanças, levantando a questão, quando é que vai parar? O ritmo alucinante da transformação preocupa-nos e deixa-nos perplexos, confusos perante um turbilhão de mudanças que, quando começamos a entender, deixamos de as conseguir sentir, pois já passaram. Não temos ainda respostas para muitas questões, mas também é certo que não podemos olhar para a modernização da sociedade como algo exclusivamente negativo, porque tal não seria verdade. São inegáveis as vantagens que a mesma trouxe ao nosso quotidiano, porém com vantagens é habitual virem desvantagens, e essas estão pouco a pouco a ser descobertas, colocando em causa se as vantagens são justificadas.

O facto é que estamos a aprender a viver numa dimensão de tempo nova e a adaptação está a ocorrer através de sucessivas crises de crescimento. Vivemos na chamada Sociedade da Informação e é importante apropriarmo-nos de uma importante consequência do significado desta expressão. A Informação é criada a partir de um conjunto de dados, portanto os dados, enquanto indício ou registo que permitem identificar alguma característica de uma entidade ou evento, estão na essência deste novo e vertiginoso mundo com que nos confrontamos. Essa é uma tomada de consciência importante, nuclear, diríamos mesmo, pois são os dados inerentes a cada um de nós que, todos juntos, moldam o presente, e a forma como os tratamos tem mais consequências do que poderemos ser levados a pensar. A verdade é que não atendemos como devíamos em relação aos nossos dados, ou pelo menos não parece que lhes damos a devida importância. Os cidadãos disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. Com a rápida evolução tecnológica e a globalização surgiram novos desafios em matéria de proteção de dados pessoais, pois não podemos esquecer que a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental, adquirido já há bastante tempo, mas que agora manifesta outra premência. Viveremos assim hoje numa sociedade da informação onde a importância dos dados pessoais não é devidamente percecionada pelos cidadãos?

A contínua expansão tecnológica desmedida motiva a preocupação de muitos de nós que assistimos apenas à vontade das empresas em querer crescer, principalmente notória e monetariamente e, ao contrário destes intervenientes, conseguimos (ou interessa-nos) ver o outro lado da moeda. Este grupo de pessoas que procura remar para o lado contrário tem, de facto, o objetivo de mostrar que é possível habitarmos num lugar que não necessita de uma vigilância constante como se

verifica atualmente. Para além disso, é possível constatar que não se verifica a existência de práticas comuns de segurança digital pela generalidade das pessoas, inclusive aqueles que nasceram e cresceram juntamente com a tecnologia, colocando assim a segurança dos seus dados e por conseguinte, da sua privacidade, e dos outros que os rodeiam em sério risco. Estas foram algumas das motivações que desencadearam a escolha do tema desta dissertação, as consequências resultantes de uma vigilância constante que quebre as barreiras da ética e da moral, sendo que o propósito do trabalho passa igualmente por aí, perceber em que situação nos encontramos exatamente, não só a nível legislativo como também do conhecimento geral dos cidadãos, de modo a tentar perceber se os nossos direitos de personalidade estão de facto a ser violados e se existe alternativa à situação que vivenciamos.

Numa primeira análise pode efetivamente parecer que os cidadãos são displicentes na facilidade com que disponibilizam as suas informações a terceiros, sem considerarem as consequências que daí podem advir, no entanto, este tema partilha da mesma transformação vertiginosa que caracteriza os dias de hoje e ao momento presente poderá já ter ocorrido mudanças nos comportamentos, ou pelo menos uma maior consciência dos factos e essa é uma das motivações para a elaboração deste trabalho. No entanto antes de podermos concluir o que quer que seja procuraremos realizar uma reflexão em torno dos grandes eixos teóricos do tema da privacidade. Assim, numa primeira instância iremos abordar os direitos de personalidade desde a sua origem que data mais manifestamente a partir do pós 2ª Guerra Mundial, até à atualidade em que hoje nos encontramos, e como estes se encontram protegidos pela legislação nacional e europeia. Dada a contínua expansão e desenvolvimento da sociedade de informação e sendo a privacidade o direito de personalidade que mais relevância tem de analisar no contexto deste trabalho, procuraremos enquadrá-la juridicamente recorrendo a documentos como a Constituição da República Portuguesa, a Declaração Universal dos Direitos Humanos (DUDH) e o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP). Outro e mais recente poderoso instrumento de defesa dos dados pessoais é o Regulamento Geral de Proteção de Dados (RGPD) que veio trazer novas exigências relativamente a este tema, especialmente pela introdução de coimas elevadas, esperando-se assim, que consiga proporcionar um novo rumo relativamente ao modo como se lida com os dados pessoais.

Num outro capítulo iremos tentar tomar o pulso a estado da arte em matéria de proteção de dados noutros países. Olhar para os outros, para a sua forma de fazer é sempre um exercício que nos ajuda a conhecer-nos melhor as nós próprios, e eventualmente a seguirmos as melhores práticas e, se for caso disso, a valorizarmos as nossas. Através da análise da legislação Portuguesa, Europeia e recorrendo também a casos fora da Europa, iremos tentar perceber se as mais recentes atualizações das leis garantem a proteção dos dados pessoais e da privacidade de todos nós, ou se ainda há um longo caminho a percorrer relativamente a esse aspeto.

Após a análise da privacidade como um direito fundamental que deve ser respeitado, importa ainda analisar as situações em que essa privacidade é colocada em risco pelas nossas ações, mais concretamente pelo uso negligente das contas de redes sociais que possuímos onde colocamos

quantidades enormes de informação pessoal, sem noção do risco que representa para a nossa privacidade.

As redes sociais são aplicações típicas daquilo que se convencionou chamar de Web 2.0. A Web 2.0 é a segunda geração de serviços online e caracteriza-se por potencializar as formas de publicação, partilha e organização de informações, além de ampliar os espaços para a interação entre os participantes do processo. Embora em rigor tenham sido criadas redes sociais mais cedo, foi a partir de 2004 que as mesmas iniciaram a sua disseminação, nunca mais parando o crescimento do número de utilizadores. Com a massificação vieram as oportunidades de negócio para os fornecedores dos serviços e os riscos para os utilizadores. Cada vez são oferecidos mais e mais atraentes serviços, com políticas de privacidade cada vez mais difusas, deixando em aberto um vasto leque de ações que os fornecedores de serviços podem executar com os nossos dados. O contrato, na realidade, é um exemplo disso mesmo, cedemos os nossos dados em troca da utilização gratuita dos serviços das aplicações. O que à partida pode parecer uma relação normal, pode também constituir uma situação de abuso desses dados e são esses contextos de riscos e ameaças perante a exposição online que são abordados no capítulo.

Visto que não é apenas por essa via que a nossa privacidade pode ser colocada em risco, importa observar a ação daqueles que têm a capacidade de nos vigiar quase (ou mesmo) constantemente, ou seja, o Estado e muitas empresas, comparando esta realidade às prisões idealizadas há mais de 230 anos recorrendo ao mecanismo de controlo intitulado de Panótico. De maneiras mais ou menos evidentes, é cada vez mais do conhecimento geral que os nossos dados se encontram dispersos pelas mais variadíssimas bases de dados, passíveis mesmo de serem utilizados sem o nosso consentimento. Essa consciencialização é talvez resultado dos recentes acontecimentos a que temos assistido, como é o caso do escândalo, amplamente mediatizado e documentado pela Netflix, intitulado de “Nada é privado – o escândalo da Cambridge Analytica” em que se mostra como foi desmascarada a empresa que, através de estratégias de manipulação de ideias políticas com recurso a dados de utilizadores oriundos da rede social Facebook, terá sido a impulsionadora dos resultados ocorridos nas eleições de 2016, que resultaram na eleição do presidente Donald Trump.

Porque de dados e do seu valor e impacto para as nossas vidas trata este trabalho, julgou-se relevante tentar obter uma visão atual dos cidadãos em relação ao tema. Iremos assim recorrer a um estudo de caso, onde se procuraremos perceber se, de facto, existe um sentimento de alarme na generalidade das pessoas quando se fala na questão da falta de privacidade das mesmas, no mesmo sentido, iremos tentar perceber se essas se encontram conscientes do desrespeito à sua privacidade da qual muito provavelmente são vítimas no espaço digital mas também no mundo físico e, por último, tentaremos compreender se essa falta de privacidade é motivo de incómodo para os inquiridos.

Importa ainda assinalar que a principal limitação verificada na investigação para a realização do presente trabalho é a fraca bibliografia nacional disponível quer em formato físico, quer em formato digital, pelo que, a procurar por monografias e/ou artigos em revistas tornou-se necessário, visto que são igualmente as mais atualizadas.

1. Os direitos da personalidade

O homem é o lobo do homem (*Homo homini lupus*), foi uma célebre expressão utilizada por Thomas Hobbes[1] no ano de 1651 com o intuito de justificar a existência do Estado como o único poder com capacidade de controlar os instintos egoístas das pessoas. Pouco mais de 100 anos depois, deu-se nas ruas de Paris a Revolução Francesa, marcando o início da Idade Contemporânea, e igualmente o início do direito contemporâneo. Este encontrava-se sobre uma influência pesada do liberalismo económico, tendo servido como uma espécie de ferramenta que permitia a existência de abusos de monarcas e outros privilegiados da nobreza. Após alguns séculos desta prática recorrente, a burguesia olhava para o Estado como algo que necessitava de ser contido, pois a sua interferência na vida da sociedade "representava um obstáculo ao livre desenvolvimento das relações económicas"[2]. Aos olhos da nova ordem jurídica competia minimizar-se o papel do Estado, estando este somente encarregue de preservar a segurança nas relações sociais. O fundamento do projeto liberal foi espelhado no artigo 4.º da Declaração dos Direitos do Homem e do Cidadão, "a liberdade consiste em poder fazer tudo que não prejudique o próximo". Foi a partir desse momento que o Homem se tornou livre, mais livre do que alguma vez foi na história civilizacional.

Como é costume verificar-se no comportamento do ser humano, fez-se um uso excessivo da liberdade, principalmente após a Revolução Industrial. Este abuso refletia-se principalmente na desigualdade económica e social que se começou a sentir, no sentido em que os mais fracos eram, de certo modo, engolidos pela liberdade dos mais fortes. Esta realidade deu azo a que fosse preciso mais do que apenas proteger o homem do Estado e do próprio homem, era necessário evitar que este abrisse mão dos seus direitos essenciais[3]. Foi nesse contexto histórico, na segunda metade do século XIX, que as primeiras conceções dos direitos da personalidade começaram a surgir. A expressão foi então concebida por jusnaturalistas franceses e alemães para representar os tais direitos inerentes ao homem, reconhecidos como preexistentes ao seu reconhecimento por parte do Estado.

"Os direitos de personalidade dão conteúdo essencial à personalidade e por isso são qualificados como direitos essenciais"[4] e, apesar de os fundamentos para a existência destes datar desde a altura do mundo grego e romano, foi no pós 2ª Guerra Mundial que os direitos da

[1] Thomas Hobbes (1588-1679), foi o responsável por divulgar esta frase "O homem é o lobo do homem", inserida no seu livro Leviatã. A frase original, traduzida para o latim como "homo homini lupus", pertence ao dramaturgo romano Plautus (254-184 a.C.).
[2] Schreiber A. (2013). *Direitos da Personalidade*. 2ª Edição Revista e Atualizada. São Paulo: Editora Atlas S.A., p. 2-4.
[3] "*Muitos juristas passariam, então, a defender a criação de uma nova categoria que fosse capaz de assegurar, no campo do próprio direito privado, a proteção daqueles direitos imprescindíveis ao ser humano, direitos que não se limitavam a uma liberdade ilusória e vazia, direitos superiores à própria liberdade, direitos a salvo da vontade do seu titular, direitos indisponíveis, direitos inalienáveis, direitos inatos* - Schreiber A. (2013). *Direitos da Personalidade*. 2ª Edição Revista e Atualizada. São Paulo: Editora Atlas S.A., p. 4.
[4] Mazur, M. (2012). *Direitos da Personalidade – A dicotomia entre os direitos de personalidade e os direitos fundamentais*. São Paulo: Atlas, p. 7.

personalidade se começaram a manifestar de uma maneira mais resoluta, tal como diz Rabindranath Valentino Aleixo Capelo de Sousa[5]. As disposições jurídicas de maior relevância, bem como os direitos de personalidade mais estudados, evidenciam perspetivas de análise extremamente semelhantes, sendo o direito à vida o ponto mais pacífico.

Na sociedade da informação e da tecnologia em que vivemos nos dias de hoje, os direitos da personalidade, e numa sociedade mais atual, o direito à educação, constituem ambos configurações de promoção do ser humano, sendo que o conhecimento é cada vez mais um sinónimo de poder, mas ao mesmo tempo de sobrevivência digna. A importância de existir uma regulamentação que defenda este tipo de direitos é importante visto que se relaciona diretamente com os aspetos mais importantes da vida de uma pessoa, sendo a dignidade humana[6] uma das mais fulcrais a serem protegidas. Portanto, "a existência de um *direito geral da personalidade* é defendida sob o fundamento de que, dada a variedade de tipos de violações aos direitos de personalidade, é necessária a proteção ampla dos indivíduos, por meio de uma espécie de direito-quadro (*Rahmenrecht*) de caráter aberto, que permita abarcar hipóteses não previamente reguladas em tipos legais específicos, algo que se torna ainda mais evidente quando se observam problemas ligados à privacidade e às liberdades comunicativas."[7]

Para facilitar a compreensão acerca do que são os direitos de personalidade, mas também perceber a relação inerente com os direitos humanos, é indispensável entender como se integram e o que são os denominados direitos fundamentais, que segundo Jorge Reis Novais "[s]er um direito fundamental significa, em Estado constitucional de Direito, ter uma importância, dignidade e força constitucionalmente reconhecidas que, no domínio das relações gerais entre o Estado e o indivíduo, elevam o bem, a posição ou a situação por ele tutelada à qualidade de limite jurídico-constitucional à atuação dos poderes públicos"[8], e que no ordenamento jurídico moderno, consente numa primeira instância, a existência objetiva dos direitos humanos e da personalidade. Na sua origem, os direitos fundamentais procuraram representar uma barreira face ao poder, com grande foque nos Estados Unidos da América, país em que o Estado foi sempre considerado uma ameaça. Neste processo, forjou-se a disciplina constitucional e, de acordo com José de Oliveira Ascensão "nem mesmo a

[5] Sousa, R. V. A. C. D. (1995). *O direito geral de personalidade (Doctoral dissertation)*, p. 84 e ss.

[6] "Tomando-se como base a jurisprudência e a dogmática da Alemanha, fonte de inspiração do desenvolvimento da doutrina dos direitos da personalidade, é correto dizer que a dignidade humana é inviolável e que a todos os poderes estatais impõe sua proteção", Miranda, Rodrigues Junior e Fruet. (2012) *Direitos da Personalidade – Principais problemas dos direitos da personalidade e estado-da-arte da matéria no direito comparado*. São Paulo: Atlas, p. 1-23.

[7] Miranda, J., Rodrigues Junior, O., Fruet, G. (2012). *Direitos da Personalidade – Principais problemas dos direitos da personalidade e estado-da-arte da matéria no direito comparado*. São Paulo: Atlas.

[8] Professor Doutor Jorge Reis Novais (ICJP/FDUL), in *III Seminário Luso-Brasileiro de Direito na Faculdade de Direito da Universidade de Lisboa*, realizado pelo Instituto de Ciências Jurídico-Políticas (ICJP) e coordenado pelo Instituto Brasiliense de Direito Público (IDP), 7 a 9 de abril de 2015.

evolução posterior, que ampliou os direitos fundamentais a novas zonas, particularmente no Direito Continental europeu, apagou aquela marca de origem na caracterização dos direitos fundamentais."[9]

Foi a 7 de fevereiro de 1992 que os membros da Comunidade Europeia, em Maastricht, assinaram o Tratado da União Europeia, TUE (ou Tratado de Maastricht), onde foi consagrado o respeito dos direitos do Homem, pois "o respeito dos direitos do homem, ou seja, do ser humano enquanto tal, constitui um dos elementos essenciais da identidade europeia. Para a cultura política ocidental não há democracia sem respeito dos direitos da pessoa enquanto tal"[10]. É evidente que quando se refere a direitos fundamentais, o homem é o foco central e unitário desta discussão, estes que existem apenas tomando como ponto de partida a existência de uma Lei Fundamental, isto é, a existência de uma Constituição. O desenvolvimento da personalidade livre, que se encontra protegido pelo artigo 1.º da Constituição da República Portuguesa[11], é "a designação geral encontrada tardiamente para a autonomia do indivíduo que é garantida para áreas de proteção específicas nos direitos de liberdade especiais"[12], consistindo deste modo, uma base para um "direito geral de liberdade"[13]. Na sociedade moderna em que vivemos, podemos identificar o ponto marcante da definição dos direitos humanos, ou ainda, dos direitos do homem, como sendo a Revolução Francesa e a consequente criação da Declaração Universal dos Direitos do Homem e do Cidadão, publicada pela primeira vez em 26 de agosto de 1789. Em relação aos direitos da personalidade, segundo Sílvio Romero Beltrão "estes exprimem aspetos que não podem deixar de ser conhecidos sem afetar a própria personalidade humana"[14], dizendo ainda que os mesmos direitos, como primeiro conceito análogo dos direitos fundamentais, são posições jurídicas do homem que o mesmo adquire somente pelo simples facto de nascer e viver, tal como se encontra descrito no artigo 66.º, n.º 1 do Código Civil. O artigo 70.º do Código Civil, prevê um direito geral à personalidade e prescreve a proteção desse direito[15]. Em termos legais, outros artigos do mesmo código fazem o elenco de certos aspetos fragmentários da personalidade, tal como o direito ao nome (artigo 72.º) ou o direito à imagem (artigo 79.º). Para além destes, existem seis outros direitos que, apesar de não terem sido explicitamente previstos, cobrem igual importância, são eles: o direito à vida (artigo 24.º da atual Constituição), à

[9] de Oliveira Ascensão, J. (2002). *A Reserva da Intimidade da Vida Privada e Familiar,* Vol. XLIII – n.º 1. Coimbra Editora, p. 10.

[10] Martins, A. M. G. (2015). *A Carta dos Direitos Fundamentais da União Europeia e os direitos sociais*. Revista Direito Mackenzie, 3(2), p. 56.

[11] "Portugal é uma República soberana, baseada na dignidade da pessoa humana e na vontade popular e empenhada na construção de uma sociedade livre, justa e solidária."

[12] Horst Dreier, in Grundgesetz-Kommentar (org. por Horst Dreier), Tübingen, 1996, anot. 5 ao artigo 2.º.

[13] "(…) mesmo aspetos não previstos por lei são englobados nos direitos da personalidade, enquanto necessários para exprimir e assegurar a dignidade da pessoa. (…) Por este seu caráter essencial, os direitos de personalidade têm prioridade em relação a quaisquer outras categorias de direitos.", de Oliveira Ascensão, J. (2002). *A Reserva da Intimidade da Vida Privada e Familiar*, Vol. XLIII – n.º 1. Coimbra Editora, p. 10.

[14] Beltrão, S. R. (2005). *Direitos da Personalidade – De Acordo com o Novo Código Civil*. São Paulo (SP): Atlas, p. 47.

[15] 1- A lei protege os indivíduos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física ou moral.

2- Independentemente da responsabilidade civil a que haja lugar, a pessoa ameaçada ou ofendida pode requerer as providências adequadas às circunstâncias do caso, com o fim de evitar a consumação da ameaça ou atenuar os efeitos da ofensa já cometida.

integridade pessoal (artigo 25.º), à liberdade (artigo 27.º), à inviolabilidade do domicílio e da correspondência (artigo 34.º)[16], à identidade pessoal e à criação pessoal (artigo 33.º). Em Portugal, "as normas sobre direitos de personalidade, que foram introduzidas no Código Civil Português – num período em que, apesar da relativamente extensa proclamação de direitos e garantias individuais no artigo 8.º da Constituição de 1933, a prática não era democrática -, ganharam *nova coloração e relevância* à luz dos "direitos, liberdade e garantias pessoais" consagrados em 1976, servindo o catálogo destes para densificar o disposto no artigo 70.º, nº 1, quanto aos aspetos da personalidade que são objeto de proteção pela lei contra qualquer ofensa ou ameaça de ofensa."[17] Os direitos de personalidade permitem que o cidadão consiga ver preservada a potencialidade de realização dos seus desejos, isto sem que perca a perspetiva de que, ao viver em sociedade, em especial na sociedade de informação em que vivemos, está inserido num campo normativo que tem como um dos seus principais exercícios harmonizar os desejos adversos próprios da existência humana.

O direito de privacidade pode-se dividir no direito à publicidade e no direito à privacidade. Pelo primeiro entende-se o direito de manter o conteúdo de alguém privado de ser explorado comercialmente sem o devido consentimento do proprietário do mesmo (indo de encontro aos artigo 11.º e artigo 13.º, mais tarde transcritos para artigo 15.º e artigo 17.º, da Diretiva sobre os Direitos de Autor no Mercado Único Digital, que dizem respeito à proteção de publicações de imprensa para utilizações digitais e à criação de um mecanismo capaz de controlar o material carregado nas plataformas digitais por parte dos utilizadores). Pelo direito à privacidade compreende-se o direito a ser deixado só e de não ter a sua personalidade representada publicamente sem a devida autorização.[18]

Os direitos de personalidade constituem deste modo o direito a defendermos os direitos da nossa própria existência, sendo que são subjetivos, na qualidade de normas jurídicas possibilitando ao indivíduo o aproveitamento direto de certos bens, universais, visto que pertencem a toda e qualquer pessoa a partir do momento em que nasce, privados, no sentido em que satisfazem as necessidade pessoais individuais no que toca a relações particulares, não patrimoniais, visto que em nenhum momento possuem uma utilidade do âmbito económico, absolutos, pois cada indivíduo estabelece relações entre ele e todos os sujeitos, assumindo o dever jurídico de não os lesar, inatos, visto serem fulcrais em relação à pessoa, indisponíveis, no sentido em que a essencialidade do seu objeto, que se encontra unido ao sujeito originário por meio de um nexo orgânico, tornando-os deste modo inseparáveis, e por último, perpétuos, porque são adquiridos desde o primeiro dia de vida, até ao

[16] Pertencendo neste caso aspetos como a intimidade da vida privada e a honra.
[17] Pinto, P. M. (2018). *Direitos de Personalidade e Direitos Fundamentais*. GESTLEGAL, p. 332.
[18] Parreira, R., & Caçador, F. (2019). *Direito de Autor: Artigos 11 e 13 (agora artigos 15 e 17) foram aprovados*. Disponível em: https://tek.sapo.pt/noticias/internet/artigos/artigos-11-e-13-agora-artigos-15-e-17-foram-aprovados [Acedido a 12 de abril de 2019].

último. Comparando com os direitos fundamentais, estes têm em comum com os de personalidade as características de serem não patrimoniais, perpétuos e indisponíveis.[19]

Concluindo, o conceito de direitos de personalidade é, evidentemente, distinto do de direitos fundamentais, sendo importante que tal diferença seja evidenciada. Os direitos de personalidade focam-se exclusivamente no Homem em si, não tendo qualquer relação com o poder. Muitos dos direitos fundamentais não são direitos de personalidade (possam ser eles direitos familiares, políticos, sociais, etc.), contudo existem direitos de personalidade que do mesmo modo não são direitos fundamentais, "*por serem irrelevantes pelo prisma das posições sociais asseguradas, que continua a estar na essência dos direitos fundamentais"*[20]*.*

Os direitos fundamentais podem então ser entendidos como "*os direitos básicos quer dos portugueses quer dos estrangeiros ou apátridas que se encontrem ou residem em Portugal (…) e abrangendo as suas diversas espécies de direitos, liberdades e garantias pessoais, de direitos, liberdades e garantias de participação política, de direitos económicos, sociais e culturais*", e dado isto pode-se igualmente concluir que "*embora muitos e diversos direitos de personalidade sejam também constitucionalmente reconhecidos como direitos fundamentais, nem todos os direitos de personalidade constituem direitos fundamentais e, ao invés, nem todos os direitos fundamentais são direitos de personalidade".*[21]

[19] Mazur, M. (2012). *Direitos da Personalidade – A dicotomia entre os direitos de personalidade e os direitos fundamentais*. São Paulo: Atlas, p. 12.
[20] de Oliveira Ascensão, J. (2002). *A Reserva da Intimidade da Vida Privada e Familiar,* Vol. XLIII – n.º 1. Coimbra Editora, p. 10.
[21] Sousa, R. V. A. C. D. (1995). *O direito geral de personalidade (Doctoral dissertation)*, Coimbra: Coimbra Editora, p. 581.

1.1. Enquadramento jurídico da privacidade: do conceito à sua abrangência

A informação é um gatilho para a ação, para a mudança. Toda a informação que sobre nós é acumulada, nos mais variados locais por onde deixamos rasto, só é importante porque vai permitir a quem a domina a impelirem-nos a fazer algo, seja isso votar num partido, comer melhor, praticar desporto, comprar um determinado artigo ou envolver-nos numa determinada causa. É por isso que a informação tem hoje um valor inestimável, essa relação da informação com a ação vincula a expressão "sociedade da informação"[22]. É por isso também que a privacidade dos dados é hoje de imensa importância, devendo ser considerado um direito fundamental. No contexto da abordagem inerente a este trabalho importa entender como o direito de privacidade é um direito de personalidade o que, por sua vez, lhe confere a importância e a legitimidade que hoje, mais que nunca, importa defender.

O direito de privacidade, mais concretamente o direito à reserva sobre a intimidade da vida privada, encontra-se presente na lei portuguesa, especificamente no artigo 80.º do Código Civil[23]. Segundo José de Oliveira Ascensão, a privacidade chega-nos em duas vertentes distintas: "*A privacy, em contraposição à publicidade ou ao setor público da vida"* e "*o direito à reserva ou a intimidade da vida privada, como um direito de personalidade entre outros".* No primeiro ponto, a questão centra-se na esfera social da existência humana, tornando o conceito vastamente extenso, abarcando dentro de si diversos direitos autonomizados como direitos da personalidade, podendo mesmo dizer que "*a privacy acaba por ser o conteúdo do direito de personalidade – quase como um megadireito que esgote toda a categoria".* No segundo ponto, a privacidade é vista mais como um direito defensivo, coexistindo com outros semelhantes (direito à imagem, à inviolabilidade do domicílio, etc), "*é o direito da personalidade, de origem alemã, destinado a cobrir todos os espaços de defesa da personalidade não especificamente previstos na lei".*

Como já vimos anteriormente, os direitos fundamentais tiveram, na sua origem, o propósito de assegurar o direito das pessoas sob as barreiras do poder. Segundo Jorge Miranda, os direitos fundamentais são "os direitos ou as posições jurídicas ativas das pessoas enquanto tais, individual ou institucionalmente consideradas, assentes na Constituição, seja na Constituição formal seja na Constituição material".[24] Analisando a doutrina portuguesa, os direitos fundamentais encontram-se sujeitos a diferentes classificações, dependendo do autor em questão.[25] Contudo, importa ressalvar,

[22] De acordo com Luís Manuel Borges Gouveia, "A Sociedade da informação está baseada nas tecnologias de informação e comunicação que envolvem a aquisição, o armazenamento, o processamento e a distribuição da informação por meios eletrónicos, como a rádio, a televisão, telefone e computadores, entre outros. Estas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, económicos e políticos, criando uma nova comunidade local e global: Manuel Borges Gouveia, L. (2004). Sociedade de Informação - Notas de contribuição para uma definição operacional. Disponível em: http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf [Acedido a 3 de fevereiro de 2019].

[23] Artigo 80.º - Direito à reserva sobre a intimidade da vida privada
1. Todos devem guardar reserva quanto à intimidade da vida privada de outrem.
2. A extensão da reserva é definida conforme a natureza do caso e a condição das pessoas.

[24] Miranda, J. (2004). *Manual de direito constitucional*. Coimbra Editora, p. 7.

[25] Jorge Miranda identifica quatro diferentes categorias de direitos fundamentais, são elas: individuais e institucionais, comum e particular, liberdades e garantias e direitos, liberdades e garantias e direitos sociais.

tendo em conta os direitos fundamentais presentes na Constituição e o tema deste trabalho, o artigo 26.º - Outros direitos pessoais - e 27.º - Direito à liberdade e à segurança - da mesma.

No primeiro, é importante referir os 2 primeiros pontos, são eles:

> *1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação.*
>
> *2. A lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.*

O nº 1 do artigo 26.º da Constituição menciona uma série de direitos que devem ser respeitados no dia-a-dia da vida na comunidade, sendo de especial importância referir o direito à reserva da intimidade da vida privada e familiar, algo que tem sido cada vez mais colocado em risco na sociedade de informação em que vivemos atualmente. Previsto no nº 2 do mesmo artigo, encontram-se as garantias providenciadas pela lei para prevenir a obtenção indiscriminada de informações de cariz pessoal, algo que se tornou cada vez mais necessário e que por vezes tende a não ser cumprido.

No artigo 27.º é importante realçar os pontos 1, 2, 4 e 5:

> *1. Todos têm direito à liberdade e à segurança.*
>
> *2. Ninguém pode ser total ou parcialmente privado da liberdade, a não ser em consequência de sentença judicial condenatória pela prática de ato punido por lei com pena de prisão ou de aplicação judicial de medida de segurança.*
>
> *4. Toda a pessoa privada da liberdade deve ser informada imediatamente e de forma compreensível das razões da sua prisão ou detenção e dos seus direitos.*
>
> *5. A privação da liberdade contra o disposto na Constituição e na lei constitui o Estado no dever de indemnizar o lesado nos termos que a lei estabelecer.*

Dado o crescimento da importância atribuída à privacidade, em particular à proteção da mesma, a Constituição da República Portuguesa consagrou o direito à privacidade como um direito fundamental, sendo que antes já era considerado um direito de personalidade[26]. A nível internacional,

[26] Nas palavras de Otto Von Gierke os direitos de personalidade são: "os direitos que concedem ao seu sujeito um domínio sobre uma parte da sua própria esfera de personalidade. Com este nome eles caraterizam-se como direitos "sobre a própria pessoa" distinguindo-se com isso, através da referência à especialidade do seu objeto, de todos os outros direitos… Os direitos de personalidade distinguem-se, como direitos privados especiais, do direito geral da personalidade, que consiste na pretensão geral, conferida pela ordem jurídica, de valer como pessoa. O direito de personalidade é um direito subjetivo e deve ser observado por todos." - Patrícia Cardoso Dias, Mestre em Direito, *Direitos Fundamentais versus Direitos de Personalidade*, Direito e Economia.

a privacidade encontra-se protegida por dois instrumentos fundamentais, são eles a Declaração Universal dos Direitos Humanos (DUDH)[27] e o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP)[28].

Tal como é referido no artigo 12.º da DUDH: "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo o ser humano tem direito à proteção da lei contra tais interferências ou ataques." Já o artigo 17.º do PIDCP é atualmente a disposição internacional mais significativa no que respeita à privacidade, referindo o seguinte:

"1. Ninguém será objeto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação.

2. Toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados."

A tarefa de monitorização e implementação do PIDCP passa pela responsabilidade do Comité dos Direitos Humanos. No mesmo encontram-se presentes Comentários Gerais respeitantes a assuntos específicos relativamente ao Pacto, como é o caso do Comentário Geral nº 16, em relação ao direito ao respeito da privacidade, família, domicílio e correspondência e à proteção da honra e reputação (artigo 17.º), de 1988, e o Comentário Geral nº 19, sobre a proteção da família, direito ao casamento e igualdade dos cônjuges (artigo 23.º), de 1990, ambos de extrema relevância no que toca ao tema da proteção da privacidade.

Indo de encontro ao especificado no Comentário Geral nº 16, também o artigo 17.º assegura a proteção do direito de todos os indivíduos contra as interferências na sua privacidade, arbitrárias ou ilegais. De acordo com o Comité dos Direitos Humanos, aos direitos anteriormente referidos têm de lhes ser concedida a garantia da proteção contra interferências tanto do Estado, como também contra violações por parte de outras pessoas, sejam singulares ou jurídicas. Nas disposições do artigo 17.º do PIDCP, o direito à privacidade pode dividir-se em vários pontos, o direito à privacidade, identidade, integridade, intimidade, autonomia, comunicação e sexualidade. Tal como consta no comentário geral

---

Jorge Miranda considera que os direitos fundamentais são entendidos como "os direitos ou as posições jurídicas subjetivas das pessoas enquanto tais, individual ou institucionalmente consideradas, assentes na Constituição.", Miranda, J. (1999). *Direitos Fundamentais: introdução geral.* Lisboa: Apontamentos das aulas, p. 11.

[27] "É inevitável que um documento como a Declaração Universal dos Direitos Humanos levante questões sobre a possibilidade de existirem valores universais. Este questionamento começou antes do documento ter sido concluído, continua até aos dias de hoje, e provavelmente nunca acabará", Johannes Morsink, *The Universal Declaration of Human Rights – origins, drafting and intent,* University of Pennsylvania Press, Philadelphia.

[28] "O Pacto Internacional sobre os Direitos Civis e Políticos foi adotado pelas Nações Unidas em 1966, e entrou em vigor após receber o número necessário de certificações em 1976. É provavelmente o tratado dos direitos humanos mais importante do mundo, visto que possui uma cobertura universal, contém um largo número de direitos e pretendo aplicá-los a todas as classes de pessoas.", Joseph, S., & Castan, M. (2013). *The international covenant on civil and political rights: cases, materials, and commentary*. Oxford University Press.

nº 16 sobre o artigo 17.º, nº 8, "o cumprimento do artigo 17.º exige que a integridade e a confidencialidade da correspondência sejam garantidas *de jure* e *de facto*[29]"[30].

O direito à privacidade, em sentido absoluto, tal como presente no artigo 12.º da DUDH, assegura a proteção do campo específico da existência individual, não interferindo na esfera privada de terceiros, podendo igualmente ser compreendido como o elemento que não se apresenta em qualquer uma das categorias a seguir mencionadas. A identidade inclui características pessoais, tais como o nome, a aparência, a indumentária, o cabelo, o género, o código genético, assim como as crenças religiosas, fazendo uma distinção perante os demais. A integridade pessoal é um conceito mais amplo, que engloba tanto a integridade moral como a física, um direito que se encontra previsto na maioria dos países do mundo e encontra-se também protegida pelo artigo 17.º do PIDCP. Por exemplo, nos casos em que um profissional de uma organização (seja um médico, um empresário, etc.) aceda a dados pessoais de um cliente sem o consentimento do mesmo, tal comportamento é considerado uma infração ao direito à privacidade. A intimidade encontra-se assegurada pela proteção ao domicílio e à correspondência, assim como através da proteção de dados. Uma pessoa encontra-se protegida contra a publicação, sem consentimento prévio, das suas características pessoais. A autonomia engloba a área de realização pessoal dos seres humanos. É o direito ao seu próprio corpo, abrangendo o direito a agir contra o próprio corpo, incluindo até o direito a cometer suicídio. A área da comunicação abrange a interação com outras pessoas e concede, além da proteção especial da família, um direito a desenvolver relacionamentos com outras pessoas. A autonomia sexual é uma parte especial e particularmente importante do direito à privacidade. Toda e qualquer regulação dos comportamentos sexuais constitui uma interferência no direito à privacidade. Apenas é consentida a interferência se for incondicionalmente necessária à proteção das pessoas afetadas, como é o caso das crianças.[31] Por último, no que toca a casos considerados especialmente vulneráveis, as pessoas com deficiência, por exemplo, que necessitem de cuidados especiais são, muitas vezes, suscetíveis de sofrerem interferências nos seus direitos à privacidade, como sucede em situações em que se encontram em instalações fechadas. Já as pessoas afetadas por doenças ou os idosos a viverem em hospitais, lares ou clínicas acarretam um risco de verem o direito à sua privacidade ser colocado em causa, por se encontrarem numa situação de "impotência", sem que disponham da capacidade de controlar quem e como acedem aos seus dados pessoais. Por último, também as crianças são suscetíveis de sofrer infrações nos seus direitos à privacidade se revelarem informações pessoais em redes sociais ou simplesmente na rede, pois embora existam mecanismos de proteção, são muitas vezes contornados pelas próprias crianças sem que estas se apercebam dos perigos que as suas ações despoletam.[32]

[29] Em Português: "de direito e de fato".
[30] Gomes, C. M. & Moreira, V. (2014). *Compreender os Direitos Humanos, Manuel de Educação para os Direitos Humanos*. Coimbra Editora, p. 395.
[31] Manfred Nowak. 2005. CCPR Commentary, artigo 17.º CCPR.
[32] Gomes, C. M. & Moreira, V. (2014). *Compreender os Direitos Humanos, Manuel de Educação para os Direitos Humanos.* Coimbra Editora, p. 388-389.

No código do trabalho[33] é igualmente referida a privacidade, mais concretamente, neste caso, a intimidade da vida privada que se encontra prevista no artigo 16.º da Lei 7/2009, referindo que

> "*1 - O empregador e o trabalhador devem respeitar os direitos de personalidade da contraparte, cabendo-lhes, designadamente, guardar reserva quanto à intimidade da vida privada.*
>
> *2 - O direito à reserva da intimidade da vida privada abrange quer o acesso, quer a divulgação de aspetos atinentes à esfera íntima e pessoal das partes, nomeadamente relacionados com a vida familiar, afetiva e sexual, com o estado de saúde e com as convicções políticas e religiosas*."[34]

Do mesmo modo, encontra-se prevista no artigo 18.º da Constituição da República Portuguesa a reserva da intimidade da vida privada, mais concretamente no n.º 2 do mesmo, mencionando que

> "*A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição.*"

Indo ao encontro deste tema da intimidade da vida privada, importa referir como uma das correntes mais divulgadas neste âmbito, a teoria das três esferas, que tem origem na literatura alemã. Esta foi responsável por possuir um papel elementar na construção e delimitação do campo de ação de proteção do direito à reserva da intimidade da vida privada. Segundo esta mesma teoria, este direito de personalidade abarca uma esfera íntima, onde se encontram abrangidas informações de tal forma reservadas que, em regra, nunca serão acessíveis a terceiro. Esta tese, como é possível deduzir pelo nome, faz a distinção de três esferas concêntricas, cujo ponto primordial é a própria pessoa. Cada uma destas esferas engloba um determinado conjunto de dados, com a particularidade de que a acessibilidade dos mesmos aumenta à medida que nos afastamos do centro, ou seja, da pessoa, e a sensibilidade dos mesmos vai aumentando à medida que caminhamos em direção ao centro. Quanto mais próximo nos encontrarmos do centro, mais íntima a informação é, sendo que neste caso estamos a referir-nos à primeira esfera. A segunda esfera, pode já ser revelada à família e amigos por exemplo, mesmo tratando-se de informação privada. Por último, a esfera mais distante do centro, engloba factos que podem ser do conhecimento de qualquer um, sendo então factos públicos.[35]

Quando se fala no tópico da privacidade encontra-se subjacente o respeito, não só pelas pessoas, pelos seus ideais, mas cada vez mais pelas suas comunicações, sendo este último

---

[33] Lei n.º 7/2009 de 12 de fevereiro.

[34] "O artigo 16.º do CT refere o direito à reserva da intimidade da vida privada, que se analisa na proibição tanto do acesso de estranhos a informações sobre a vida privada como da divulgação de informações que alguém tenha sobre ela", Abrantes, José João (2014). *Direitos Fundamentais da Pessoa Humana no Trabalho, em especial a reserva da intimidade da vida privada*, Almedina.

[35] Desenvolvida por diversos autores, mais concretamente por Rita Amaral Cabral, "*O Direito à intimidade da Vida Privada"* e por Ricardo Leite Pinto, "*Liberdade de Imprensa e Vida Privada"*.

considerado um direito fundamental reconhecido na Carta dos Direitos Fundamentais da União Europeia. Tal acontece devido à possibilidade de o conteúdo destas comunicações eletrónicas poder revelar informações extremamente sensíveis acerca dos utilizadores abrangidos na comunicação. Da mesma forma, os metadados (descrições de dados armazenados em bancos de dados, ou como é comumente definido "dados sobre dados a partir de um dicionário digital de dados")[36] provenientes de comunicações eletrónicas podem, de igual modo, revelar informações extremamente sensíveis e pessoais, tal como categoricamente reconhecido pelo TJUE (Tribunal de Justiça da União Europeia). No mesmo sentido, a larga maioria dos Estados-Membros reconhece a necessidade assegurar a proteção das comunicações como um direito constitucional diferenciado. De maneira a assegurar o cumprimento do direito referido anteriormente de uma maneira uniforme por parte de todos os Estados-Membros, criando possíveis restrições sobre os fluxos de dados pessoais além-fronteiras e não pessoais, respeitante à utilização de serviços de comunicações eletrónicas, a União Europeia criou regras nesse sentido, estipuladas no RGPD. Visto que a Internet e as tecnologias digitais no geral não conhecem fronteiras, a dimensão do problema estende-se para além de um único Estado-Membro, sendo que estes possuem uma maior dificuldade em resolver de uma maneira eficaz as contrariedades no contexto atual, individualmente, recomendando-se que os países não se isolem e cooperem entre si. Por último, com o intuito de manter a coerência com o Regulamento Geral de Proteção de Dados, é imprescindível rever a Diretiva Privacidade e Comunicações Eletrónicas, que estipula regras para assegurar a segurança no que toca ao tratamento de dados pessoais, à notificação da violação de dados pessoais e à confidencialidade das comunicações e adotar medidas para articular as duas ferramentas.[37]

1.2. O RGPD como instrumento de defesa para os dados individuais

A entrada em vigor em Portugal do Regulamento Geral de Proteção de Dados[38] procurou cimentar mais solidamente as questões relacionadas com a proteção da informação pessoal, recorrendo às coimas como o seu principal mecanismo de controlo da violação dos direitos. As sanções, nos casos menos graves poderão chegar aos 10 milhões de euros ou a 2% do volume de negócios anual a nível mundial, consoante o valor que for mais elevado e, nos casos mais graves, duplica-se os valores anteriormente referidos, ou seja, 20 milhões de euros ou 4% do volume de negócios anual a nível mundial. As coimas, no primeiro caso, referem-se a falhas no cumprimento de

[36]de Souza, T. B., Catarino, M. E., & dos Santos, P. C. (2012). *Metadados: catalogando dados na Internet. Transinformação*, 9(2), p. 93.

[37] Proposta de REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas e que revoga a Diretiva 2002/58/CE (Regulamento relativo à privacidade e às comunicações eletrónicas).

[38] O Regulamento Geral de Proteção de Dados (RGPD) entrou em vigor em 25 de maio de 2018 e substituiu a diretiva e lei de proteção de dados, passando a existir um conjunto único de regras de proteção de dados para todas as instituições e empresas ativas na UE, independentemente da sua localização.

exigências técnicas ou organizacionais, como por exemplo, falta de certificações ou falha na comunicação de violações das suas bases de dados. As mais graves, aplicam-se a violações dos princípios básicos relacionados com a segurança dos dados, como o desrespeito pelo consentimento que o utilizador deu, a transferência de dados pessoais para outras organizações ou países que não garantam o nível de proteção de dados desejado.[39] O regulamento não vem acrescentar muitas mais normas para além daquelas que já existiam, a grande diferença passa sim, pela instituição deste sistema de penalizações claramente descrito, como forma de assegurar o cumprimento das mesmas[40] sendo que uma empresa ou organização tem permissão para recolher ou reutilizar informação pessoal nos seguintes cenários:

- Se tiverem uma ligação contratual com alguém (por exemplo, um contrato de fornecimento de bens ou serviços, ou um contrato de trabalho);
- Se estiverem a cumprir uma obrigação legal (por exemplo, aquando do processamento de informação de um sujeito);
- Quando o processamento de informação vai de encontro aos interesses essenciais de um sujeito (por exemplo, quando esta prática pode ajudar na proteção da vida do mesmo);
- Para completar uma tarefa pública (neste caso é mais relacionado com tarefas de administrações públicas tais como hospitais, escolas e câmaras);
- Quando existirem interesses legítimos (por exemplo, se o banco usar a informação pessoal de um cliente para avaliar se o mesmo está em condições para ter uma conta poupança).

Apesar do cuidado do normativo em tipificar os cenários, estes ainda abrangem um grande universo de situações em que os nossos dados podem ser solicitados, mas é enfatizado que quando uma organização requer o nosso consentimento para o tratamento de dados é necessário que concordemos com isso, usualmente através da assinatura de um formulário disponibilizado pela mesma.[41] Se por acaso fornecermos o nosso consentimento em determinada altura a uma organização para esta lidar com os nossos dados pessoais, esta permissão pode ser retirada a qualquer altura,

[39] Jornal Oficial da União Europeia. (2016). REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

[40] Zerlang, J. (2017). *GDPR: a milestone in convergence for cyber-security and compliance*. Network Security, 2017(6), p. 8-11.

[41] Proteção de dados e privacidade em linha (publicado em https://europa.eu), "Quando uma empresa ou organização pede o consentimento do titular dos dados, este tem de dar o seu acordo de forma explícita, por exemplo, assinando um formulário de consentimento ou assinalando a opção «sim» num formulário de escolha sim/não numa página Web."

fazendo com que a partir desse momento a organização não possa mais utilizar a nossa informação pessoal.[42]

Talvez a questão mais abordada no que toca ao tratamento de dados e à privacidade com a entrada em vigor do RGDP é o direito ao esquecimento[43], e por este entenda-se que, se a nossa informação pessoal deixar de ser necessária ou caso esteja a ser usada à margem da lei, então podemos pedir para que a mesma seja eliminada. Estas regras aplicam-se igualmente a motores de busca, tal como o Google, uma vez que estes são considerados controladores de informação[44]. No caso de uma organização ter disponibilizado online a nossa informação pessoal e mais tarde pedirmos para a mesma ser eliminada, a organização tem a obrigação de comunicar todos os sítios onde a informação terá sido partilhada e pedir ainda que todos os dados sejam eliminados.

No entanto, em 1976, no artigo 35.º da Constituição da República Portuguesa - utilização da informática - já se encontra descrito em modos bastante práticos e sucintos como se deve lidar com a questão dos dados no mundo informático, bem como os direitos que estes (os indivíduos) possuem quando disponibilizam os seus dados para tratamento, como vem descrito no ponto 1 do presente artigo: "todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos previstos na lei." A mesma lei, no nº 2 do mesmo artigo, diz garantir a proteção dos dados pessoais dos cidadãos. Já no nº 3 estão descritas as características que não podem ser usadas no tratamento de dados, salvo exceções em que o titular dá o seu consentimento, sendo elas "convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica", no sentido de se fazer um esforço para não existirem situações de discriminação ou situações em que os dados não servem como modo de identificar individualmente alguém. A exceção ao referido anteriormente encontra-se descrito nº 4 do artigo 35.º dizendo que "é proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei."[45] Descrito como sendo o direito que protege os cidadãos dos perigos consequentes do uso da informática, segundo Castro, é um direito fundamental, embora se assuma como direito-garantia da reserva de intimidade da vida privada. A entrar em rota de colisão com os artigos acima mencionados, encontra-se o direito à liberdade de

[42] Proteção de dados e privacidade em linha (publicado em https://europa.eu), "Se tiver dado consentimento a uma empresa ou organização para utilizar os seus dados pessoais, pode, a qualquer momento, contactar o responsável pelo tratamento dos dados (a pessoa ou organismo que trata os seus dados pessoais) e retirar o seu consentimento. Assim que tiver retirado o seu consentimento, a empresa ou organização deixa de poder utilizar os seus dados pessoais."

[43] Artigo 17.º UE Regulamento Geral sobre a Proteção de Dados, "Direito ao apagamento dos dados (direito a ser esquecido)"

[44] São assim chamados visto que estes retêm grande maioria da informação disponível no meio digital e que dão primazia àquelas cujos donos pagarem mais para as publicitarem, o que acaba por se tornar perigoso.

[45] No Artigo 35.º da Constituição da República Portuguesa, é igualmente nota de destaque os pontos:

5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

expressão previsto no artigo 37.º da CRP que, devido aos avanços tecnológicos, permite e facilita que todos os utilizadores da rede possam divulgar e difundir o seu pensamento, opiniões e informações no espaço virtual.[46]

A missão, muito complicada, diga-se, de assegurar a proteção dos dados dos cidadãos, não pode ser levada a cabo se não existir uma articulação entre várias entidades, tanto a nível nacional como a nível europeu. Para esse efeito, foram institucionalizados mecanismos de controlo e de fiscalização da parte nacional do Sistema de Informação Schengen, para preservação da ordem e segurança públicas, bem como a segurança do Estado. E como se encontra referido na Lei n.º 2/94 de 19 de Fevereiro, artigo 5.º[47]: "É criado o Centro de Dados que serve o Sistema de Informação Schengen, o qual fica dependente do Serviço de Estrangeiros e Fronteiras e a funcionar sob orientação de um responsável nomeado por despacho do Ministro da Administração Interna." Com a criação deste centro de dados procurou-se facilitar o controlo da utilização de dados integrados no sistema de modo a certificar-se que tal não atente contra os direitos das pessoas, reforçando-se a noção de que os "direitos de acesso, de retificação e de supressão de dados são exercidos pelos detentores de um interesse direto, pessoal e legítimo, de acordo com as disposições da Convenção de Aplicação, junto da autoridade nacional de controlo"[48].

A antiga lei da proteção de dados pessoais, a Lei nº 67/98 de 26 de outubro, teve como atribuição transpor a diretiva nº 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995 relativa à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Apesar de já não se encontrar ativa por força da implementação do Regulamento Geral de Proteção de dados, a lei em questão tinha determinadas normas a cumprir que ainda hoje se mantêm como é o caso do artigo 5.º da mesma onde se encontra descrito o que se deve ter em conta no momento em que se pretende proceder ao tratamento de dados pessoais de outros, devendo estes ser:

> a) *Tratados de forma lícita e com respeito pelo princípio da boa fé*, ou seja, o tratamento de dados pessoais deve atender às exigências legais a que no caso esteja adstrito;
>
> b) *Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades*, isto é, os dados recolhidos podem apenas ser utilizados para os objetivos inicialmente acordados com o portador dos mesmos e funcionários de uma empresa não podem aceder a dados que tenham um nível de acesso superior aos deles;

[46] Canotilho, J. J. Gomes e Vital Moreira (2007). Constituição da República Portuguesa Anotada, 1, 4.
[47] "Estabelece os mecanismos de controlo e fiscalização do Sistema de Informação Schengen".
[48] Artigo 6.º, Lei n.º 2/94 de 19 de fevereiro.

c) *Adequados, pertinentes e não excessivos relativamente às finalidades para que são recolhidos e posteriormente tratados*, indo de encontro ao ponto anterior;

d) *Exatos e, se necessário, atualizados, devendo ser tomadas as medidas adequadas para assegurar que sejam apagados ou retificados os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente*, por outras palavras, todos os dados pessoais podem ter um prazo de validade, fazendo com que todos eles devam ser revistos periodicamente com o objetivo de verificar se continuam a espelhar a realidade, fazendo as retificações necessárias;

e) *Conservados de forma a permitir a identificação dos seus titulares apenas durante o período necessário para a prossecução das finalidades da recolha ou do tratamento posterior*[49], ou seja, deve-se procurar ter os dados organizados para uma fácil consulta, bem como toda e qualquer informação de como e até quando se deve proceder com o tratamento dos dados.

Relativamente a dados sensíveis, como descrito no nº 7 do referido artigo 5.º, o tratamento dos mesmo é proibido, podendo somente ser realizado em casos em que seja indispensável ao exercício das atribuições legais ou estatutárias do responsável dos dados, ou em casos em que o portador tiver dado o seu consentimento para tal. Ao longo da pesquisa e aprofundamento do tema, facilmente se conclui aquilo que deve ser a prática tanto das empresas/organizações, como dos portadores dos dados. Para que todas as leis sejam cumpridas, sabendo que no que toca ao meio cibernético o cenário é mais traiçoeiro e bastante mais fácil de escapar impune no que toca a práticas maliciosas, é importante que exista sobretudo respeito e conhecimento informado. Respeito por parte daqueles cuja atividade exige que se proceda ao tratamento de dados de outros, não procurando fazer uso de mecanismos (por vezes ilícitos) para usufruto próprio, colocando em causa aqueles que em determinado momento lhes confiaram informações pessoais. Já aqueles cujos dados serão tratados devem procurar aprofundar o seu conhecimento relativamente à maneira como a sua informação será processada, para não correrem o risco de, por um lado, confiarem os seus dados a entidades mal-intencionadas e, por outro, confiarem os seus dados a entidades sem más intenções, mas que irão retirar proveito próprio recorrendo a esses mesmos dados. Com isto, torna-se necessário entender aquilo que os cidadãos sentem relativamente à sua privacidade e à utilização dos seus dados pessoais, portanto, achou-se essencial a realização de um questionário de modo a averiguar essa questão. Neste questionário procurámos numa primeira instância perceber se os cidadãos (maiores de idade) se encontram alarmados com os ataques às suas informações privadas. Num segundo plano, procurámos averiguar se os inquiridos se encontram conscientes da falta de privacidade que, muito provavelmente, são vítimas. E por último, perceber se essa falta de privacidade é um motivo de incómodo para eles,

[49] Lei nº 67/98 de 26 de outubro, CAPÍTULO II, Tratamento de dados pessoais, SECÇÃO I, Qualidade dos dados e legitimidade do seu tratamento, Artigo 5.º Qualidade dos dados.

tentando perceber no fundo, qual o valor que atribuem aos seus próprios dados. Tudo isto será analisado mais à frente no trabalho.

2. Uma análise comparativa das legislações de proteção de dados em alguns países Europeus

Seja em que aspeto for, não existem países iguais, e apesar dos esforços realizados por parte da União Europeia para aproximar os Estados-Membros uns dos outros, a realidade é notoriamente diferente, verificando-se exatamente isso no que toca à legislação de proteção de dados nos diferentes países. É certo que o Regulamento Geral de Proteção de Dados surgiu com o objetivo de colocar os países pertencentes à União Europeia no mesmo patamar nesse aspeto, porém, há países que já se encontravam mais desenvolvidos fazendo com que a adoção das medidas impostas pelo regulamento fossem relativamente simples de adotar, sendo que, no outro lado da moeda, encontram-se países como Portugal, onde mesmo depois da entrada em vigor do RGPD, continuam a persistir dificuldades em grande parte dos setores para conseguirem implementarem a legislação devidamente[50], sendo que já foram quatro o número de multas em Portugal devido ao não cumprimento das regras impostas pelo regulamento, uma delas ao hospital público do Barreiro no valor de 400000€, tendo as restantes sido aplicadas a empresas[51]. No entanto, até hoje, a maior multa registada foi em França, imposta a uma multinacional (Google) que usava indevidamente os dados pessoais dos cidadãos com o intuito de segmentar publicidade sem que existisse qualquer consentimento expresso dos titulares do mesmo, no valor de 50 milhões de euros (4% da faturação anual da empresa).[52] O jurista Alexandre Sousa Pinheiro afirmava que a maior dificuldade à aplicação do RGPD em Portugal era a ausência de legislação nacional, existindo por parte das empresas e entidades públicas uma procura em escapar às coimas, em vez de procurarem uma execução correta das exigências impostas pelo regulamento, algo que não ajudava ao bom funcionamento do mesmo.[53] Porém, a 14 de junho de 2019 foi (finalmente) aprovada na Assembleia da República a lei n.º 120/XIII de execução relativa ao regulamento, que era necessária visto que em determinados aspetos como a idade do consentimento para o tratamento de dados ou as coimas a aplicar a instituições privadas, necessitava da lei nacional.[54]

[50] Tal como afirma Jesualdo Fernandes, professor de sistemas de informação do ISEG, numa conferência promovida pela Moneris.

[51] As três outras empresas a sofrerem coimas, duas das quais são lojas que não indicavam a videovigilância dos clientes. O valor total é de 424 mil euros e à TSF a CNPD adianta que há cada vez mais queixas relacionadas com a captação de imagens de vídeo por câmaras de segurança, sobretudo de vizinhos e trabalhadores preocupados com as imagens gravadas. – Parreira, R., & Caçador, F. (2019). RGPD: *Um ano depois só há 4 multas. Videovigilância concentra principais queixas*. Disponível em: https://tek.sapo.pt/noticias/internet/artigos/rgpd-um-ano-depois-so-ha-4-multas-videovigilancia-concentra-principais-queixas [Acedido a 14 de maio de 2019]

[52] Nunes, F. (2019). *Já houve quatro multas em Portugal por causa do RGPD*. Disponível em: https://eco.sapo.pt/2019/05/17/ja-houve-quatro-multas-em-portugal-por-causa-do-rgpd-uma-foi-ao-hospital-do-barreiro-e-tres-a-empresas-privadas/ [Acedido a 2 de junho de 2019].

[53] Machado, M. (2019). RGPD. Um ano depois, os nossos dados já são privados? – Observador. Disponível em: https://observador.pt/2019/05/25/rgpd-um-ano-depois-os-nossos-dados-ja-sao-privados/ [Acedido a 14 de junho de 2019].

[54] Machado, M. (2019). *Portugal aprova lei de proteção de dados um ano depois do RGPD – Observador*. Disponível em: https://observador.pt/2019/06/14/portugal-aprova-lei-de-protecao-de-dados-um-ano-depois-do-rgpd/ [Acedido a 27 de março de 2019].

No documento em questão são apresentadas restrições à videovigilância em território nacional, mais concretamente no nº 2 do artigo 19.º referindo que as câmaras de vídeo não podem incidir sobre: “

a) Vias públicas, propriedades limítrofes ou outros locais que não sejam do domínio exclusivo do responsável, exceto no que seja estritamente necessário para cobrir os acessos ao imóvel;
b) A zona de digitação de códigos de caixas multibanco ou outros terminais de pagamento ATM;
c) O interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a privacidade, designadamente instalações sanitárias, zonas de espera e provadores de vestuário;
d) O interior de áreas reservadas aos trabalhadores, designadamente zonas de
e) refeição, vestiários, ginásios, instalações sanitárias e zonas exclusivamente afetas ao seu descanso.”

No nº 3 do presente artigo, é referido ainda que as câmaras de videovigilância podem apenas incidir sobre os perímetros externos, locais de acesso e espaços cujos bens e equipamentos requeiram especial proteção, em estabelecimentos de ensino. Por último, no nº 4 encontra-se descrito que em situações em que a videovigilância é admitida, é proibida a captação de som, com a exceção em que as instalações vigiadas se encontrem encerradas ou em casos em que a CNPD tenha autorizado previamente. Porém, no nº 1 deste mesmo artigo é descrito que “sem prejuízo das disposições legais específicas que imponham a sua utilização, nomeadamente por razões de segurança pública, os sistemas de videovigilância cuja finalidade seja a proteção de pessoas e bens asseguram os requisitos previstos no artigo 31.º da Lei n.º 34/2013, de 16 de maio”, sendo o mencionado anteriormente no artigo 2º os limites definidos à utilização desta prática. O referido no nº 1 pode desta forma ser um terreno aberto para que os limites sejam ultrapassados em determinadas circunstâncias.[55]

Como referido anteriormente, todos os países e, por conseguinte, todas as suas leis, são distintos, mesmo aqueles que pertencem a uma união formal como a União Europeia. O caso alemão é interessante de se analisar, pois foi em Hessen, Alemanha, que surgiu a primeira lei de proteção de dados no mundo chamada de Datenschutzgesetzgebung no ano de 1970, sendo que, em 1977, é que foi implementada a primeira lei de proteção de dados federal denominada de Bundesdatenschutzgesetz (BDSG). Esta lei foi continuamente alterada até que, em 2001, as provisões da Diretiva 95/46/EC de Proteção de Dados da União Europeia de outubro de 1995 foram finalmente

[55] App.parlamento.pt. (2019). TEXTO DE SUBSTITUIÇÃO DA PROPOSTA DE LEI N.º 120/XIII/3.ª ASSEGURA A EXECUÇÃO, NA ORDEM JURÍDICA NACIONAL, DO REGULAMENTO (UE) 2016/679, RELATIVO À PROTEÇÃO DAS PESSOAS SINGULARES NO QUE DIZ RESPEITO AO TRATAMENTO DE DADOS PESSOAIS E À LIVRE CIRCULAÇÃO DESSES DADOS. [online] Disponível em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679626d56304c334e706447567a4c31684a53556c4d5a5763765130394e4c7a464451554e45544563765247396a6457316c626e527663306c7561574e7059585270646d4644623231706333e6862793969595752685954493324e43316a5a5745324c54526c4e4441744f475a6b4e5331684e445a6859324535593255334e6a51756347526d&fich=badaa264-cea6-4e40-8fd5-a46aca9ce764.pdf&Inline=true [Acedido a 28 de março de 2019].

implementadas na lei nacional, contendo uma série de alterações, em particular dizendo respeito a atividades de negócio. O Tribunal Federal Alemão aprovou em 2017 a nova Lei de Proteção de Dados (FDPA) e com as atualizações da lei nacional, surgiu um novo BDSG que vem complementar o Regulamento Geral de Proteção de Dados e facilitar a sua implementação no país. O propósito deste no BDSG, que entrou em vigor em simultâneo com o RGPD a 25 de maio de 2018, é fazer uso das numerosas cláusulas abertas presentes no regulamento que permitem aos Estados-Membros realizar alterações, sejam elas de especificação ou restrição, aos requerimentos de processamento de dados pessoais.[56] A Alemanha não tem uma Autoridade destinada à proteção de dados, como existe em Portugal a Comissão Nacional de Proteção de Dados, tem por sua vez diversas autoridades em todos os 16 Estados Alemães, responsáveis por assegurar que as leis estão a ser cumpridas. Apesar de não ter essa entidade nacional a regular o cumprimento das normas, existe sim uma Autoridade de Proteção de Dados reguladora dos serviços de telecomunicações, que representa o país no Conselho Europeu de Proteção de Dados, denominado de Comissário Federal para Proteção de Dados e Liberdade de Informação (BFDI). Visto que existe um vasto número de autoridades relacionadas com a proteção de dados e da privacidade dos cidadãos, foi criado um comité para assegurar que todos estes têm a mesma abordagem no que toca a este assunto de extrema sensibilidade, denominado de "Conferência de Proteção de Dados" (DSK). O BDSG possui regras adicionais ao RGPD relativamente ao processamento de categorias especiais de dados pessoais. Contrariamente ao artigo 9.º do RGPD, o processamento dos dados referidos anteriormente é permitido por órgãos públicos e privados em determinados casos. Para além disso, na secção 23 do novo BDSG encontram-se determinados os casos em que os encarregados detêm permissão para processar dados para uma finalidade distinta daquela para a qual os dados foram inicialmente coletados. Fazendo uso da cláusula que se encontra no artigo 88.º do RGPD, na secção 26 do BDSG encontram-se igualmente descritas regras especiais relativas ao processamento de dados para fins relacionados com o emprego, onde o legislador alemão estabeleceu um regime próprio de proteção de dados para funcionários.[57] Importa assinalar que no documento da lei alemã, à semelhança do caso português, se encontram previstos limites à vídeo vigilância em espaços públicos, mais concretamente na secção 4 do 2º capítulo, onde consta que "monitorizar as áreas acessíveis ao público com dispositivos ótico-eletrónicos (videovigilância) serão apenas permitidos na medida do necessário."[58]

No Reino Unido existem outras particularidades algo distintas das verificadas anteriormente. Semelhante ao caso Alemão, no dia da entrada em vigor do Regulamento Geral de Proteção de Dados, foi preparada uma nova lei nacional de proteção de dados, o DPA (Data Protection Act), que contém

[56] Zrinski, T. (2019). *EU GDPR vs. German Bundesdatenschutzgesetz (BDSG)*. Disponível em: https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-vs-german-bundesdatenschutzgesetz-similarities-and-differences/ [Acedido a 14 março de 2019].

[57] Law in Germany - DLA Piper Global Data Protection Laws of the World. (2019). Disponível em: https://www.dlapiperdataprotection.com/index.html?t=law&c=DE&c2= [Acedido a 29 de março de 2019].

[58] Iapp.org. (2017). Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680. [online] Disponível em: https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf [Acedido a 29 de março de 2019].

não só derrogações e isenções no que toca ao espectro que o RGPD engloba em determinadas áreas onde estas são permitidas, mas também:

- Permite a aplicação contínua do RGPD na legislação nacional do Reino Unido quando o mesmo sair da União Europeia (caso tal se venha a verificar);
- A criação de um regime de proteção de dados especificamente no que toca ao processamento de dados pessoais, tendo origem na parte 3 do DPA que transpõe a Diretiva de Aplicação da Lei ((EU) 2016/680) para a lei do Reino Unido;
- A parte 4 deste documento atualiza o regime de proteção de dados para o processamento da segurança nacional; e
- As partes 5 e 6 do DPA definem o intuito do mandato do Comissário da Informação, bem como os seus poderes de execução e, simultaneamente, cria uma série de infrações criminais relacionadas com o processamento de dados pessoais.

No artigo 9.º nº 2 do RGPD encontram-se previstas uma série de exceções no processamento legal de categorias especiais de dados pessoais, sendo que algumas dessas carecem de uma base na legislação dos Estados-Membros. As partes 1 e 2 presentes no Anexo 1 do DPA facultam várias dessas bases na forma de condições, que na verdade fornecem margens específicas para a legalização do processamento de certos tipos de dados de categorias especiais por parte do Reino Unido, sendo que algumas dessas condições são semelhantes à lei anterior do país, enquanto outras são novas. Nos casos em que um encarregado deseje fazer uso de uma das condições do DPA para realizar o processamento legal de dados considerados especiais, de uma condenação criminal ou de ofensas, é exigido que conste um documento político adequado e que sejam aplicadas as salvaguardas adicionais de modo a justificar o processamento desejado. O documento político anteriormente referido tem como objetivo estabelecer como é que o regulador procura cumprir cada um dos princípios de proteção de dados presentes no artigo 5.º do RGPD. No artigo 8.º nº 1 do RGPD encontra-se estipulado que uma criança só pode fornecer o seu próprio consentimento ao processamento relativamente aos serviços da sociedade da informação, quando a mesma tiver mais do que 16 anos de idade, a não ser que a lei do Estado-Membro aplique uma idade menor. O DPA reduz a idade do consentimento para esses fins para 13 anos no Reino Unido.[59]

A França adaptou a sua legislação doméstica ao GDPR com a promulgação da Lei nº 2018-493, de 20 de junho de 2018, relativa à proteção de dados pessoais, que atualiza principalmente a antiga Lei nº 78-17, de 6 de janeiro de 1978, sobre tecnologia da informação, arquivos de dados e liberdades civis. Para além disso, o Despacho nº 2018-1125, de 12 de dezembro de 2018, adotado nos termos do artigo 32.º da Lei nº 2018-493, atualiza a legislação francesa relacionada com a proteção dos dados pessoais, procurando "simplificar a

[59] Law in United Kingdom - DLA Piper Global Data Protection Laws of the World. (2019). Disponível em: https://www.dlapiperdataprotection.com/index.html?t=law&c=GB&c2= [Acedido a 29 de março de 2019].

implementação e as correções formais necessárias para garantir a coerência com a lei de proteção de dados da UE".

Atualmente, a lei estabelece que ela se aplica quando o controlador de dados se encontra estabelecido em França ou fora da União Europeia e utiliza meios de processamento localizados no território francês. O escopo territorial da Lei francesa encontra-se em conformidade com o artigo 3.º do RGPD, sendo que, essa mesmo, tem aplicação a qualquer processamento de dados pessoais no contexto das atividades de um estabelecimento sob a jurisdição de um regulador na França, independentemente do mesmo ocorrer em território francês ou não. Além disso, as regras francesas adotadas com base na margem de manobra permitida que os Estados-Membros possuam pelo RGPD, serão apenas aplicáveis na medida em que o titular dos dados resida em França, inclusive quando o responsável pelo tratamento destes não estiver estabelecido no país, existindo casos excecionais, como é o caso dos fins jornalísticos ou dos fins de expressão académica, artística ou literária. Para as atividades referidas, são aplicáveis as regras do Estado-Membro onde o controlador de dados se encontra estabelecido.[60]

Os países analisados, e comparando com a realidade portuguesa, já possuíam uma base de leis mais avançada que a nossa, fazendo com que se encontrassem devidamente preparados para o dia em que o RGPD entrasse em vigor, sendo a prova maior disso o conjunto de leis nacionais que entraram em vigor exatamente no mesmo dia que o regulamento, sendo que no caso português essas mesmas leis só começaram a ser discutidas em parlamento bastantes meses depois e a aplicação das mesmas arrastou-se até 14 de junho de 2019[61]. Portugal ainda hoje se encontra algo perdido no que toca ao cumprimento das normas impostas pelo Regulamento Geral de Proteção de Dados, o que mostra a necessidade geral da existência de um maior planeamento e ação em todos os setores. Apesar da introdução destas novas regulamentações na União Europeia, não existe uma grande coesão entre os Estados-Membros a esse nível, fazendo com que estes se encontrem algo isolados no combate às ameaças de segurança, quer por parte de outros países, quer por ameaças internas. Por conseguinte, esta situação origina uma diferenciação notória entre os países, havendo aqueles que se encontram mais avançados e outros que estão algo atrasados nesta matéria, sendo que, infelizmente, Portugal se insere neste segundo leque.

[60] Law in France - DLA Piper Global Data Protection Laws of the World. (2019). Disponível em: https://www.dlapiperdataprotection.com/index.html?t=law&c=FR&c2= [Acedido a 29 de março de 2019].
[61] Machado, M. (2019). *Portugal aprova lei de proteção de dados um ano depois do RGPD – Observador.* Disponível em: https://observador.pt/2019/06/14/portugal-aprova-lei-de-protecao-de-dados-um-ano-depois-do-rgpd/ [Acedido a 27 de maio de 2019].

3. A Internet e as Redes Sociais como zonas de risco para a privacidade

3.1. A privacidade na Internet

Num panorama em que a informação é universalmente acessível, como é que controlamos a nossa privacidade online? No mundo em que vivemos nada é grátis, pois seja no mundo online ou offline, existe, por exemplo, uma troca de valores em aplicações e serviços grátis, a nossa informação é coletada, armazenada e partilhada por empresas, e na verdade nós concordámos com essas diretrizes quando clicamos no botão do rato a aceitar as políticas de privacidade. Por muito que pensemos que detemos o controlo da nossa privacidade, a realidade é oposta, uma vez que, por exemplo, a Google faz um scan de todas as contas do Gmail[62] e a Apple sabe a localização de todos os utilizadores de iPhones, mesmo que a localização esteja desligada.[63] No entanto, o problema não são estas grandes empresas que em princípio são confiáveis - estes exemplos servem apenas para demonstrar a facilidade com que se retiram, diariamente, informações pessoais de cada um - o problema está no desconhecido, no vilão que ninguém conhece fazendo ameaças anónimas, nas empresas que ninguém conhece ou numa pessoa desconhecida que possui imensa informação sobre cada um de nós. Tudo o que fazemos online pode deixar uma impressão digital com consequências imprevisíveis, sendo fundamental a tentativa de preservação da nossa privacidade.

Procurando regulamentar e proteger a privacidade na internet, podemos assinalar como um acontecimento de referência, neste caso no Brasil, o ato conhecido como o Marco Civil da Internet. Trata-se de uma lei que entrou em vigor a 23 de junho de 2014 e que regulamenta a utilização da internet, instaurando princípios e garantias que converte a rede livre e democrática no Brasil, disciplinando o comportamento dos indivíduos no mundo virtual. Por exemplo, em situações em que um utilizador realiza uma pesquisa online num motor de busca, essa mesma informação pode vir a ser utilizada comercialmente em futuros acessos do mesmo de forma a "bombardear" o autor da pesquisa com publicidade exaustiva relativamente àquilo que foi pesquisado. No entanto, depois da entrada em vigor do Marco Civil da Internet, de acordo com o artigo 7.º do mesmo, são definidos os direitos assegurados aos utilizadores da rede, com destaque para o ponto VII que diz ser verificada a garantia do "não fornecimento a terceiros dos seus dados pessoais, inclusive registos de conexão, e de acesso

[62] MacMillan, D. (2018). *Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail*. Disponível em: https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442 [Acedido a 10 de julho de 2019].

[63] "With the advent of wearable technology such as Fitbits and smart watches equipped with heart rate monitors, Dr. Tynan says technology is now also being used to track not just our movements, but also our emotions. "You can detect whether somebody is excited, or down – all different trends during the day. This is all sold under the guise of cool things we can do, but the information they collect becomes a pot of gold for government, companies and hackers to mine and potentially do some nasty things with." – Shute, J. (2019). *Can anyone escape Britain's surveillance state?* Disponível em: https://www.telegraph.co.uk/technology/news/11831533/Can-anyone-escape-Britains-surveillance-state.html [Acedido a 23 de junho de 2019].

a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei" e para o ponto X que admite a garantia da "exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação da internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registos previstas nesta Lei", a utilização desses dados pessoais só poderá então ocorrer se for concedido o consentimento livre, expresso e informado por parte dos portadores desses dados, podendo ser revogado a qualquer altura.[64]

O princípio da neutralidade da rede encontra-se presente no artigo 9.º da Lei 12965/14 (Marco Civil da Internet) que diz que "o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonómica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação". Isto quer dizer que os fornecedores de conexão à internet (em Portugal a autoridade reguladora das comunicações postais e das comunicações eletrónicas é a ANACOM (Autoridade Nacional de Comunicações)) são os responsáveis pela ligação do mundo físico ao espaço cibernético, sendo portanto imperativo que sejam neutros, não promovendo o acesso de determinados utilizadores a certos sítios, fazendo com que os provedores tirassem proveito próprio dessa prática. Se estes forem capazes de manipular o acesso dos utilizadores a determinados sítios, a natureza plural da internet acabará por ser comprometida. No entanto, esta neutralidade da rede poderá ser quebrada em situações excecionais, como em questões técnicas relacionadas com a qualidade de um serviço e a serviços de emergência, casos que se encontram especificados pelo Presidente da República.[65]

O documento citado até aqui vem alterar o paradigma no que toca a duas questões principais. Em primeiro lugar, o artigo 19.º do mesmo vem responsabilizar apenas os fornecedores de aplicações por conteúdos gerados por terceiros, apenas se, após ordem judicial, os mesmos não retirarem esse mesmo conteúdo ofensivo. Logo, a jurisprudência do Supremo Tribunal de Justiça terá necessariamente de sofrer alterações, pois passa a ser necessária uma ordem judicial para que seja retirado o conteúdo. Numa segunda instância, o artigo 21.º veio valorizar a tutela da privacidade estabelecendo que todo e qualquer conteúdo que envolva cenas de nudez ou de sexo deverão ser retirados pelo fornecedor da aplicação após pedido extrajudicial da vítima.[66]

[64] Nos pontos I, II, III, VII e VIII do artigo7.º, o direito a isolar-se do contato com outras pessoas, bem como o direito de impedir que terceiros tenham acesso a informações acerca de sua pessoa (Amaral, 2008, p. 306), encontram-se previstos ao elencarem-se como direitos dos utilizadores da internet a inviolabilidade da intimidade e da vida privada, a preservação do sigilo das comunicações privadas pela rede, transmitidas ou armazenadas; o não fornecimento de dados pessoais coletados pela internet a terceiros sem prévio consentimento do utilizador, além de estabelecer o dever de informar os mesmos acerca da coleta de dados sobre si, quando houver justificação para tal.

[65] Pontieri, A. (2019). Marco civil da internet, neutralidade de rede e liberdade de expressão. [online] Jus.com.br. Disponível em: https://jus.com.br/artigos/70495/marco-civil-da-internet-neutralidade-de-rede-e-liberdade-de-expressao [Acedido a 10 de maio de 2019].

[66] Flumignan, W. (2018). *Responsabilidade civil dos provedores no Marco Civil da Internet* (Lei n. 12.965/14). Universidade de São Paulo, p. 17.

Sintetizando, os três princípios que se destacam no Marco Civil da Internet são a neutralidade, a privacidade e o registo dos acessos. No que toca à neutralidade da rede, o consumidor deve pagar de acordo com o volume e velocidade que deseja, fazendo com que a rede seja um ambiente igualitário para os utilizadores. Sendo assim, a Lei proíbe a venda de pacotes de internet limitados pelo tipo de conteúdo, origem, destino, aplicação ou serviço, proíbe também a redução de banda dos utilizadores que atingirem os limites de consumo, previamente estabelecidos pela operadora. O princípio da privacidade veio garantir o sigilo e inviolabilidade das comunicações dos utilizadores. Segundo a Lei, a quebra do sigilo mediante ordem judicial só deve acontecer em situações em que as informações possam colaborar na identificação de utilizadores envolvidos em ações ilícitas. Aqui também consta a responsabilidade do provedor no que toca ao sigilo das informações dos utilizadores. Por último, o princípio do registo de acessos veio estabelecer que é responsabilidade do provedor de serviço a guarda dos dados de conexão, devendo este armazenar os registos pelo menos durante 1 ano.

Na União Europeia, a Diretiva relativa à Privacidade e às Comunicações Eletrónicas assegura "*a proteção dos direitos e liberdades fundamentais, nomeadamente o respeito pela vida privada, a confidencialidade das comunicações e a proteção dos dados pessoais no setor das comunicações eletrónicas. Assegura igualmente a livre circulação de dados, equipamentos e serviços de comunicações eletrónicas na União*"[67]. Do mesmo modo foi criada com o intuito de "*estabelecer regras para garantir a segurança no que diz respeito ao tratamento de dados pessoais, à notificação da violação de dados pessoais e à confidencialidade das comunicações. Proíbe, além disso, as comunicações não solicitadas nos casos em que o utilizador não tenha dado o seu consentimento"*[68]*.* O Regulamento do Parlamento Europeu e do Conselho relativo ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrónicas tem como bases jurídicas pertinentes o artigo 16.º e o artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE). O artigo 16.º do TFUE introduz uma base jurídica particular no que toca à adoção de regras respeitantes à proteção de pessoas singulares respeitante ao tratamento de dados pessoais pelas instituições da União.[69] Já o artigo 114.º do Tratado estabelece a base jurídica no que diz respeito a medidas de apropriação que procuram estabelecer o mercado interno, realçando igualmente um forte objetivo de assegurar um nível de proteção elevado, com ênfase nos consumidores.

[67] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas).

[68] Este ponto encontra-se previsto no artigo 5.º, nº 1 "*Os Estados-Membros garantirão, através da sua legislação nacional, a confidencialidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas publicamente disponíveis. Proibirão, nomeadamente, a escuta, a instalação de dispositivos de escuta, o armazenamento ou outras formas de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por pessoas que não os utilizadores, sem o consentimento dos utilizadores em causa (…)*"

[69] Milt, K. (2019). PROTEÇÃO DOS DADOS PESSOAIS. [online] Europarl.europa.eu. Disponível em: http://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf [Acedido a 12 de julho de 2019].

3.2. Riscos e ameaças da exposição online

A questão da privacidade afeta-nos em todos os aspetos da nossa vida e muitas vezes deixamos de a ter sem que nos apercebamos de tal. À medida que a Internet se tornou parte das nossas vidas, muitos de nós utilizamo-la para substituir ferramentas que estão presentes na nossa vida há muito anos, como é o caso dos diários, que foram sendo substituídos por blogs online onde partilhamos os nossos sentimentos, opiniões, etc., para toda e qualquer pessoa poder aceder e opinar, a menos que, claro, sejam colocados em privado. Caso tal não seja feito, quem expõe assim as informações privadas na Internet corre sérios riscos de atrair ações indesejadas, reveladoras de más intenções, tornando-se mais perigoso do que parecia à primeira vista. Mesmo quem coloca informações em privado pode ser alvo de ataques cibernéticos (*snooping* ou *spywares*, por exemplo) que, no caso de o computador não se encontrar bem protegido, podem ser acedidas por terceiros. Dado isso, os utilizadores devem evitar dar informações pessoais ou o email a sites suspeitos de publicidade, e certificar-se que o seu computador se encontra protegido com programas especificamente desenhados para precaver esse tipo de violações de privacidade.

Na *World Wide Web* (WWW)[70] encontram-se disponibilizados infinitos conjuntos de documentos e materiais interligados, disponibilizados para terceiros acederem aos mesmos. É um inesgotável recurso de informação, passível de gerar conhecimento, quando usado adequadamente. Porém, diversos problemas surgem na navegação online, problemas esses que retiram o âmbito privado na rede. Os chamados *clickstreams* (sequências de cliques), dizem respeito ao trajeto percorrido (sítios onde entrou e hiperligações seguidas) por quem navega na WWW e contêm relevância pois revelam interesses pessoais e padrões, deixando assim de serem somente dados de tráfego, mas sim dados de conteúdo.[71] Estes caminhos ficam registados no computador pessoal que, associado através do IP do mesmo, possibilita que seja traçado um perfil do utilizador. Gravemente ameaçadores à privacidade dos utilizadores são os *cookies* e o *spyware*, isto devido à sua característica distintiva, invisibilidade. Os *cookies* são porções de informação que se encontram regularmente associados a um identificador único, armazenados nos computadores dos utilizadores (até 2009, antes da chegada de uma diretiva da União Europeia, estes pedaços de informação eram armazenados sem o conhecimento ou consentimento dos utilizadores)[72], que memoriza informação com base no comportamento de navegação do mesmo.[73] O *spyware* é um tipo de *malware*[74] que, sem

[70] A WWW foi idealizada por Tim Berners-Lee, investigador do CERN na Suíça e coordenada em conjunto com Robert Cailliau, e cujo propósito inicial era a partilha de arquivos.

[71] Taniguchi, D. (2009). U.S. Patent No. 7,587,486. Washington, DC: U.S. Patent and Trademark Office.

[72] Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., & Weippl, E. (2019). *Measuring Cookies and Web Privacy in a Post-GDPR World. In International Conference on Passive and Active Network Measurement*, p. 258-270.

[73] Mazouchi, A., Chokhawala, A., & Kusam, A. (2019). U.S. Patent Application Nº. 15/788,466.

[74] Um m*alware* pode ser entendido por: "um pedaço de código que altera o comportamento do núcleo do sistema operativo ou de algumas aplicações com poucas defesas de segurança, sem o consentimento do utilizador e de forma a que seja impossível de detetar essas alterações usando características documentadas do sistema operacional ou da aplicação" - Rutkowska, J. (2006). *Introducing stealth malware taxonomy*. COSEINC Advanced Malware Labs, 1-9, p. 2.

o consentimento do indivíduo, recolhe informações sobre seus hábitos online, histórico de navegação ou informações pessoais (como números de cartão de crédito), e geralmente usa a internet para passar estas informações a terceiros sem o conhecimento do próprio.[75] Sem dúvida que as ferramentas que utilizamos trazem vantagens no dia-a-dia de um utilizador tais como permitir um login automático, armazenar preferências, manter o controlo de artigos adicionados nos carrinhos de compras e registar a atividade do utilizador, e é neste último ponto que a situação se inverte e se torna algo mais sensível pois este registo de atividade invade de certa forma a privacidade dos utilizadores. Segundo Luciano *et all*, "*todos os fornecedores dos serviços de redes sociais e e-mail gratuito utilizam cookies para coleta de dados. Estes cookies coletam informações além das necessárias para utilização destes serviços. A partir destas podem-se conhecer as preferências dos utilizadores, as quais podem ser utilizadas, por exemplo, para direcionar publicidade indesejada e sites de comércio eletrónico oferecendo produtos que atendam ao perfil do utilizador*". Mas, ainda de acordo com os mesmos autores, o uso "*indevido de informações: as informações divulgadas podem ser utilizadas para ataques de força bruta, que consiste em utilizar um algoritmo para analisar as informações com o objetivo, por exemplo, de descobrir as senhas, criação de perfil falso de utilizador, golpes de engenharia social e responder questões de segurança para recuperação de senhas*."[76]

Estas ameaças poderão ser categorizadas, como ameaças externas, no sentido em que existe uma ação de um agente externo à nossa vontade que deliberadamente nos viola a privacidade. No entanto com a disseminação massiva das redes sociais, naquilo que se convencionou chamar a Web 2.0, as ameaças à privacidade podem advir do próprio sujeito, por desconhecimento das condições de prestação de certos serviços que subscreva.

De acordo com Doneda[77], "as redes sociais são representativas de uma interação social que nos leva a pensar num conceito de rede mesmo anterior à famosa web. Entendemos atualmente como rede social um serviço prestado através da Internet que possibilita aos seus utilizadores criar um perfil público contendo dados pessoais e possibilitando ferramentas que permitem a interação com outros utilizadores partilhando interesses, ideais e preferências em comum (um clube de futebol, uma igreja, uma sala de aula, uma empresa). As redes sociais são assim consideradas como um espaço sem fronteiras com liberdade de entrada e circulação" consequentemente um espaço de risco de divulgação dessas interações. Importa então, equacionar a exposição no equilíbrio entre os direitos dos consumidores e os respetivos deveres nos dois sentidos, isto é, os deveres que têm para consigo próprios e com os outros utilizadores, e os deveres para com as empresas que disponibilizam os serviços dos quais os consumidores fazem uso. Presente na Lei n.º 24/96, de 31 de julho, que

[75] Harkin, D., Molnar, A., & Vowles, E. (2019). *The commodification of mobile phone surveillance: An analysis of the consumer spyware industry*. Crime, Media, Culture, p. 6.
[76] SILVA, V. R. B., LUCIANO, E. M., & WIEDENHÖFT, G. C. (2016). *AMEAÇAS POTENCIAIS À PRIVACIDADE DAS ORGANIZAÇÕES CAUSADAS PELO COMPORTAMENTO INSEGURO DE USUÁRIOS: UMA ANÁLISE SEGUNDO O FAIR INFORMATION PRINCIPLES*, p. 12.
[77] Doneda, D. (2012). *Reflexões sobre proteção de dados pessoais em redes sociais*. Revista da rede académica internacional de proteção de dados pessoais, 1, p. 1-12.

estabelece os direitos e deveres dos consumidores, encontram-se, essencialmente, os seguintes direitos e deveres:

- Direito à Qualidade de Bens e Serviços – estabelece que os produtos e serviços devem satisfazer os propósitos a que se destinam;
- Direito à Proteção da Saúde e à Segurança Física – direito a que os bens ou serviços que adquirirem não coloquem em risco a sua saúde e segurança física;
- Direito à Formação e à Educação – direito a conhecer os direitos enquanto consumidor, sendo o Estado responsável por garantir esse conhecimento;
- Direito à Informação – direito a que a informação chegue até si de forma clara e objetiva, enquanto consumidor, sendo que os fornecedores têm a obrigação de disponibilizar todas as informações sobre as características dos produtos que vendem;
- Direito à Proteção dos Interesses Económicos – direito a ter os interesses económicos garantidos;
- Direito à Prevenção e Reparação de Danos – direito à reparação de um dano causado por alguma entidade;
- Direito à Proteção Jurídica e a uma Justiça Acessível e Pronta – direito a recorrer à justiça como meio de defender os direitos;
- Direito à Participação por via representativa – direito a ser representado por associações e a que estas sejam consultadas, na defesa dos interesses dos consumidores (DECO, por exemplo).

- Dever da Solidariedade – dever a juntar-se a outros consumidores na defesa dos interesses e direitos;
- Dever da Consciência Crítica – dever a estar atento à qualidade e preço dos produtos e dos serviços que as empresas fornecem;
- Dever de Agir – dever de agir em situações em que os consumidores se sintam enganados;
- Dever da Preocupação Social – dever de ter consciência do impacto que determinado consumo causa noutras pessoas;
- Dever de Consciência Ambiental - dever de ter responsabilidade ambientar, de modo a preservar os recursos naturais. [78]

O problema agrava-se tendo em conta que não temos de estar atentos somente à invasão da nossa privacidade por parte de hackers, os governos são igualmente responsáveis por desrespeitarem o nosso espaço privado, sendo a única diferença o facto de não quererem com isso prejudicar os cidadãos para proveito próprio, ao contrário dos hackers. No entanto, não deve ser por essa razão que devemos ficar mais descansados e preocuparmo-nos apenas com quem procura fazer-nos mal

[78] Pgdlisboa.pt. (1996). Lei nº 24/96, de 31 de julho - LEI DE DEFESA DO CONSUMIDOR. [online] Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=726&tabela=leis [Acedido a 17 de abril de 2019].

diretamente. No livro[79] Edward Snowden "Sem Esconderijo", Gleen Greenwald revelou que a Agência de Segurança Nacional (NSA) não realiza apenas a vigilância em massa acerca de cidadãos americanos, mas também sobre estrangeiros, que podem abarcar aliados próximos. Na maioria dos casos, esta vigilância constante levada a cabo pelos países incidindo diretamente sobre os próprios cidadãos, recorrendo maioritariamente ao uso indiscriminado de metadados[80], é justificada pela necessidade de controlar pessoas potencialmente perigosas dentro de cada país. Esta prática de justificar um comportamento que influencia todos os indivíduos por causa de uma minoria potencialmente perigosa torna-se muito perigosa pois a partir daí facilmente se entra numa espiral de comportamentos pouco éticos, justificados por razões adjacentes à maioria das pessoas. Tendo os governos praticamente toda e qualquer ferramenta à sua disposição para fazerem com elas o que bem entenderem, neste caso concreto, numa tentativa de conseguirem tornar a sociedade num lugar mais seguro, a tecnologia à qual recorrem cada vez mais (dado o aumento exponencial de utilizadores do mesmo nos últimos anos), é sem dúvida o telemóvel. O uso do telemóvel como uma ferramenta de vigilância foi, inclusive, o epicentro de um caso muito antecipado ligado à privacidade no Tribunal Supremo dos Estados Unidos da América, no *Carpenter v. United States*,[81] mais concretamente o uso da funcionalidade de GPS presente nos smartphones. Este caso surgiu em dezembro de 2010 na altura em que uma série de assaltos tiveram lugar nos estados de Michigan e Ohio, curiosamente, de telemóveis. No decurso das investigações, a polícia prendeu quatro homens, incluindo Timothy Carpenter, que foi mais tarde declarado culpado por uma série de assaltos tendo sido sentenciado a 116 anos de prisão. O modo como os agentes da autoridade conseguiram ligar o autor dos crimes aos mesmos, foi através da obtenção de informação de localização do seu próprio telemóvel durante 100 dias, sem que houvesse um mandato. Antes do seu julgamento, Carpenter argumentou que a obtenção desses registos constituía uma violação da Quarta Emenda, e, portanto, a polícia era obrigada a ter um mandato, tendo o Supremo Tribunal concordado em ouvir o caso anos mais tarde. A sentença emitida foi que para aceder à informação de localização de um telemóvel, que é gerada automaticamente sempre que estes se conectam com uma antena, com a informação a ficar armazenada durante anos, era obrigatório que a polícia tivesse um mandato, embora tenha deixado a porta aberta para que os agentes da autoridade possam obter certas e determinadas informações em algumas situações. Esta decisão do tribunal representou uma vitória para os defensores da privacidade digital que, pode originar repercussões para todo o tipo de informação na posse de terceiros, o que inclui mensagens privadas, emails, informação de navegação online e registos bancários. "*Today's decision rightly recognizes the need to protect the highly sensitive location data from our cell phones, but it also provides a path forward for safeguarding other sensitive digital information in future cases -*

[79]Greenwald, G. (2014). *Edward Snowden Sem esconderijo*, p. 32.

[80] Metadados são dados sobre os dados. Os metadados descrevem o que são esses mesmos dados: eles fornecem informações sobre esses dados. Estes oferecem uma maneira de classificar, organizar e caracterizar dados ou conteúdo.

[81] Supremecourt.gov. (2017). SUPREME COURT OF THE UNITED STATES - CARPENTER v. UNITED STATES. [online] Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf [Acedido a 12 de julho de 2019].

from our emails, smart-home appliances, and technology that is yet to be invented,"[82] declarou o advogado Nathan Freed Wessler, da ACLU.

O mundo virtual tornou-se um local propício para o antissocial criar o caos. Notícias de casos de fraudes, ofensas, agressões, violação à privacidade, divulgação de informações confidenciais, etc., são cada vez mais frequentes nesta era digital. Numa primeira instância, podemos classificar esses comportamentos como o exercício do direito à liberdade de expressão e/ou manifestação de uma mera opinião, porém, não podemos deixar de calcular as possíveis consequências visto que são motivadoras de danos aos direitos de personalidade. A partilha de informação pessoal dos utilizadores da rede, em particular das redes sociais, leva-nos a refletir acerca do conceito atual de privacidade, sendo importante reter que a abertura do utilizador à rede social permite o uso, no entanto, não pode legitimar o abuso. Por uma rede social pode-se entender um serviço que permite aos utilizadores da mesma a criação de um perfil público que contém dados pessoais e ferramentas que proporcionam interações com outros utilizadores. De acordo com Doneda[83], *as redes sociais são assim consideradas como um espaço sem fronteiras com liberdade de entrada e circulação.* Esta visão dos criadores das redes sociais é ao mesmo tempo um palco que permite a difusão de mensagens políticas, onde por vezes se pode tornar perigoso, ou originar revoluções, por exemplo a "Primavera Árabe" fez uso desta tecnologia para originar ondas revolucionárias de protestos e manifestações que tomaram lugar no Médio Oriente e no Norte de África contra as ditaduras presentes nos países em questão, originando manifestações, greves e comícios, tendo sido através das redes sociais que todas estes atos de revolta se iniciaram.[84] As redes sociais introduziram velocidade e interatividade que faltavam nas técnicas convencionais de mobilização, que geralmente incluem o uso de folhetos, cartazes e faxes. Por exemplo, as redes sociais permitiram que ativistas egípcios a residirem dentro e fora do país acompanhassem os eventos no Egito, participassem nos grupos nas redes sociais bem como nas discussões presentes nestas.[85] Como se percebe, o nível de popularidade destas redes acrescentando ao facto de serem gratuitas, faz com que sejam os locais ideais para a disseminação de mensagens seja de que tipo forem. Como seria expectável, as marcas e empresas não deixaram passar a oportunidade de divulgar os seus produtos e de criar os seus próprios perfis para autopromoção.

---

[82] Tradução: A decisão tomada hoje reconhece a necessidade de proteger os dados de localização altamente confidenciais dos nossos telemóveis, mas também fornece um caminho para a proteção de outras informações digitais sensíveis em situações futuras – desde os nossos e-mails, eletrodomésticos inteligentes e tecnologia que ainda será inventada.

[83] Doneda, D. (2012). *Reflexões sobre proteção de dados pessoais em redes sociais*. Revista da rede académica internacional de proteção de dados pessoais, 1, p. 1-12.

[84] April 2008 marked the first Egyptian instigated cyberactivism attempt, in which activists created a Facebook page to join textile workers in Mahalla on a general strike. Although the Facebook page attracted 70,000 supporters, the strike was harshly defeated by state security forces (ibid.). The experience and knowledge gained in these early social media trials, however, proved useful in the 2011 protests and subsequent revolution. – Eltantawy, N. and Wiest, J. (2011). Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory. [online] Research Gate. Disponível em: https://www.researchgate.net/publication/285908894_Social_Media_in_the_Egyptian_Revolution_Reconsidering_Resource_Mobilization_Theory [Acedido a 11 de junho de 2019].

[85] Eltantawy, N., & Wiest, J. B. (2011). *The Arab spring| Social media in the Egyptian revolution: reconsidering resource mobilization theory*. International journal of communication, 5, 18. p. 1210.

Na ótica empresarial, as redes sociais podem ajudar a determinar o potencial de um certo serviço ou produto. Porém, para além das vantagens óbvias que as redes sociais trazem para a generalidade da população, as desvantagens (e os perigos) são motivo de preocupação. A criação de perfis falsos é possivelmente a prática mais comum relativamente a más práticas nas redes sociais. Com isto, podem existir dois objetivos principais: o utilizador mal-intencionado tem como propósito abordar terceiros, fazendo-se passar por uma pessoa fictícia, ou cria um perfil falso de uma pessoa real, utilizando dados dessa mesma pessoa. A criação de perfis falsos é, infelizmente, uma prática que tem vindo a crescer, tendo sido registado na rede social *Facebook* mais de 76 milhões de contas falsas. Uma pessoa pode ser levada a crer que um mero perfil falso numa rede social não causa grande transtorno para os outros, mas como exemplo a demonstrar o contrário, no Tribunal da Relação de Guimarães, o réu foi condenado pelo crime de difamação agravada acrescido de uma indemnização civil à lesada, devido à criação de um perfil falso na rede social Hi5. Mais grave que as falsificações de perfis, são as situações em que pessoas, ao fazerem-se passar por outros, conseguem enganar terceiros, sendo o exemplo mais crítico a pedofilia. Quando se lida com crianças é de facto quando o tema fica realmente mais sensível e preocupante e nas redes sociais não é exceção, elas constituem um alvo fácil para pessoas mal-intencionadas. Dada a abertura da sociedade às novas tecnologias, bem como facilidade de acesso de cada vez mais pessoas às mesmas, é encarado como normal o uso de smartphones, tablets, computadores, etc. por parte das crianças. Este crescimento não foi acompanhado pelo conhecimento dos perigos presentes na internet, portanto, muitas vezes os jovens definem os seus perfis públicos tornando todas as suas informações (muitas vezes privadas) acessíveis por outros e vulneráveis.

Numa outra dimensão a chamada Internet das Coisas (IoT) supõe a interconexão de bilhões de coisas inteligentes ao nosso redor que possuem a capacidade de coletar, armazenar, processar e comunicar informações sobre si mesmas e sobre o seu ambiente físico. Atualmente, as organizações, o Estado e nós enquanto indivíduos, necessitamos da Internet como principal auxiliar na realização de tarefas do quotidiano, significando que a sociedade no geral se encontra cada vez mais depende da tecnologia. Os sistemas de IoT fornecem serviços avançados sempre inovadores, com base na aquisição de dados cada vez mais refinados num ambiente densamente povoado por aparelhos inteligentes. Exemplos desses sistemas são os cuidados de saúde generalizados, sistemas avançados de gestão de edifícios, serviços de cidades inteligentes, vigilância pública e a tal aquisição de dados mais apurada. No entanto, a coleta, o processamento e a disseminação de dados cada vez mais invisíveis, densos e difundidos no meio da vida privada das pessoas, suscitam sérias preocupações relativas à sua privacidade, sendo que a ignorância relativamente ao resultado desses problemas pode originar consequências indesejadas, por exemplo, a não aceitação e falha de novos serviços, danos à reputação ou processos jurídicos dispendiosos. A sociedade de informação depende, naturalmente, dos sistemas de informação, onde prevalece a partilha e o acesso facilitado à informação. O acesso simplificado, porém, entra em colisão com a privacidade, sendo que a mesma tem sido um tópico de pesquisa importante em diferentes áreas de tecnologia que são importantes facilitadores da visão da IoT, por exemplo, a identificação por radiofrequência (RFID), as redes de sensores sem fio (WSNs), a

personalização da Web e as aplicações e plataformas móveis. Apesar das contribuições consideráveis das comunidades em questão, falta uma visão holística dos problemas de privacidade, visto tratar-se de um conceito em evolução que compreende um número crescente de tecnologias e exibe uma variedade de recursos constantemente em mudança.

É, pois, inegável que vivemos numa sociedade cada vez mais dependente da tecnologia. Essa tecnologia, que resulta numa diminuição da nossa privacidade, consequência da constante vigilância a que somos sujeitos, origina uma dupla relação entre essa vigilância e a sociedade. Primeiro, a introdução de novas tecnologias de vigilância têm inegavelmente, um grande impacto social, podendo este ser um impacto positivo. E antes de se pensar que a vigilância ou a invasão à privacidade começa apenas agora a ganhar exposição, a título de exemplo, em Lancaster, o assédio racista a dois comerciantes locais levou o Conselho da Cidade a proceder à instalação de três câmaras de vigilância que são diariamente controladas por uma sede policial local (*Guardian*, 3 de abril de 1999). Além disso, a "outra face" da vigilância, no entanto, surge da sua capacidade de reforçar as divisões sociais já existentes na sociedade, no que se refere à idade, etnia, género e classe. O departamento de polícia de Washington DC, por exemplo, admitiu que recolhe rotineiramente amostras de urina para averiguar se as policias femininas estão grávidas sem o conhecimento ou consentimento das mesmas. Embora a vigilância tenha sempre um impacto social, é ao mesmo tempo moldada pelas relações sociais e práticas culturais existentes. Nas sociedades modernas industriais, por exemplo, os processos de vigilância foram na altura moldados pela "Competição militar entre os estados-nação, racionalização expressa na burocracia e nos imperativos de classe do capitalismo" (Lyon, 2001: 118). Mais recentemente, alguns sociólogos argumentaram que o surgimento de uma sociedade de consumo está a alterar o paradigma dos processos de vigilância.[86]

3.3. Do Panótico ao 1984: um estado de constante vigilância

"A configuração da segurança na Comunidade Internacional, apesar do caráter acentuadamente intuitivo do conceito, tem sido alvo de intensos debates e conceções doutrinárias, que têm como ponto focal a colocação da segurança no centro da discussão das relações internacionais conflituais. A tradição tem entendido a segurança internacional no sentido da violação dos direitos e dos bens coletivos dos Estados, estes entendidos a partir dos seus elementos constitutivos, realçando-se sobretudo o elemento territorial – a integridade territorial – e o elemento funcional – o poder público soberano de que disfrutam, nas suas aceções interna e internacional. A rutura da segurança internacional tem o significado da postergação destes direitos e princípios fundamentais da inserção internacional dos Estados, pondo em crise a sua própria existência no seio da Comunidade

[86] McCahill, M. (2013). *The surveillance web*. Willan, p. 11-12.

Internacional."[87] A verdade é que a (video)vigilância tem vindo a crescer substancialmente à medida que avançamos no século XXI, tendo ganho novos propósitos no seu uso, também devido à mais fácil integração entre aparelhos de monitorização, de controlo de acesso e alarmes, sendo que, atualmente, são muitas vezes usados para:

- Monitorização de tráfego;
- Observar o comportamento de prisioneiros;
- Manter perímetros de segurança controláveis;
- Segurança doméstica;
- Transportes públicos;
- Prevenção de crime;
- Proteção escolar;
- Eventos desportivos;
- Monitorizar empregados; entre muitos outros.

A verdade é que a existência de tais mecanismos de videovigilância pode garantir, ou pelo menos ajudar a garantir, uma cidade, uma sociedade, um país, um mundo mais seguro. Porém, é inegável o risco de diminuição da privacidade quando estamos na presença de câmaras de vigilância, principalmente quando presenciamos o avanço exponencial da tecnologia, permitindo inclusive descobrir a identidade das pessoas que aparecem nas câmaras através de softwares de reconhecimento fácil que cruzam os dados com muitos outros sistemas. A entrada em vigor do RGPD veio procurar reforçar as leis da privacidade dos dados no espaço europeu, proteção essa que inclui a videovigilância. "Em Portugal e quanto à videovigilância, este facto[88] assume especial relevância, dado que, a Lei de Segurança Privada[89] estabelecia os requisitos a respeitar na instalação e exploração de um sistema de videovigilância. Contudo, sendo que a videovigilância não é um recurso exclusivo da segurança privada, tais requisitos não se impunham se a videovigilância fosse explorada fora do contexto da segurança privada. E é precisamente neste ponto que o controlo prévio exercido pela CNPD (Comissão Nacional de Proteção de Dados) se revelou fundamental, pois permitiu que a Comissão estabelecesse as condições de exploração do sistema, especialmente quanto ao prazo máximo de gravação das imagens (geralmente 30 dias), a finalidade (usualmente, a proteção de pessoas e bens), os destinatários dos dados (em regra, apenas órgãos de polícia criminal e

[87] Gouveia, J. B. (2013). *Direito Internacional da Segurança*. Leya, p. 11
[88] Neste caso, a autora (Lurdes Dias Alves) refere-se ao facto de o tratamento de dados pessoais, que inclui a videovigilância, deixar de ter obrigatoriedade de autorização prévia.
[89] Lei 34/2013, de 16 de maio.

autoridades judiciárias, para utilização em processos crime) e o direito de informação (através da afixação em local visível da informação sobre a existência de videovigilância)."[90] Tornou-se pois evidente a importância da criação de uma legislação, sem colocar em causa a aplicabilidade do Regulamento Geral de Proteção de Dados, ajude a fixar e a regular os limites do uso da videovigilância.

A imagem de pessoas, (neste caso recolhidas através de ferramentas de videovigilância) não começou por ser salvaguardada pela recente legislação de proteção de dados pessoais, pois já o era antes, desde logo, pela CRP, artigo 26.º, n.º 1, afirmando que o direito à imagem e à reserva da intimidade da vida privada é reconhecido a todos. Na mesma linha, a imagem das pessoas é igualmente protegida no Código Civil, artigo 79.º, afirmando que "o retrato de uma pessoa não pode ser exposto, reproduzido ou lançado no comércio sem o consentimento dela". No Código Penal, o artigo 199.º, está prevista a punição daqueles que fotografem ou filmem terceiros, mesmo que se trate de eventos em que estes tenham participado"[91]. Por todas estas preocupações de salvaguarda, é facilmente compreensível a sensibilidade do tema e que a videovigilância, é suscetível de colocar em causa o direito à imagem e à reserva da vida privada de pessoas, ao recolher imagens das mesmas.

Todos os problemas acima referidos sucedem essencialmente devido à complexa interligação entre os direitos fundamentais e alguns direitos pessoais, com os direitos à liberdade de expressão e à informação. O direito ao bom nome e reputação encontra-se previsto no artigo 72.º do CC, sendo fundamentalmente o direito a não ser ofendido ou lesado na sua honra, dignidade ou consideração social mediante acusação causada por outros. Este direito é facilmente colocado em causa em situações como as abordadas anteriormente, como é a criação de um perfil falso. O direito à imagem está previsto no artigo 79.º do CC e abrange o direito a definir a sua autoexposição (não ser fotografado, não ver o seu retrato exposto em público sem o seu consentimento, entre outros). O direito em questão é considerado um direito de personalidade que se encontra ligado ao direito à reserva da intimidade da vida privada, sendo "em primeiro lugar, o direito ao resguardo, isto é, o direito de privacidade" (Pereira, 2004). Reconhecido no artigo 8.º da Convenção Europeia dos Direitos do Homem (CEDH) encontra-se o direito à reserva da intimidade da vida privada e familiar, consagrado no artigo 26.º, nº 1 e nº 2 da CRP, sendo analisado maioritariamente em dois direitos menores: o direito a que as informações que tenha sobre a vida privada de outros não sejam divulgadas por ninguém e o direito a impedir o acesso de desconhecidos a informações privadas e familiares. O grande problema passa por circunscrever as fronteiras entre o domínio da vida privada e familiar que desfruta de reserva de intimidade. Estas fronteiras devem ser traçadas de acordo com os conceitos de privacidade e dignidade humana, tendo em conta o respeito dos comportamentos, o respeito do anonimato e o respeito da vida em relação[92]. A reserva do indivíduo sobre a sua privacidade, intimidade e imagem

[90] Lurdes Dias Alves, *A videovigilância e a compreensão da privacidade.*

[91] Para estas as regras existem exceções, como aquela prevista no n.º 2 do artigo 79.º do CC, onde se encontra previsto que "Não é necessário o consentimento da pessoa retratada quando assim o justifiquem a sua notoriedade, o cargo que desempenhe, exigências de polícia ou de justiça, finalidades científicas, didáticas ou culturais, ou quando a reprodução da imagem vier enquadrada na de lugares públicos, ou na de factos de interesse público ou que hajam decorrido publicamente."

[92] Canotilho, J. J. Gomes e Vital Moreira (2007). Constituição da República Portuguesa Anotada, 1, 4.

está atualmente protegida pela cláusula geral presente nos artigos 79.º e 80.º do Código Civil, bem como na ordem jurídica internacional e na Constituição da República Portuguesa. De acordo com José Eduardo Figueiredo Dias, ao tutelar os bens jurídicos da privacidade e intimidade está-se, simultaneamente, a assegurar a proteção um direito de personalidade, devendo ser considerado com um fortalecimento do princípio da dignidade do Homem.[93]

O filósofo e jurista inglês Jeremy Bentham, em 1785, concebeu aos seus olhos a prisão ideal, fazendo uso de um mecanismo designado de *Panótico*[94]. Este mecanismo de vigilância consistia num edifício em forma de anel em que no centro do mesmo se encontrava um pátio com uma torre de vigia nela inserida, onde se situava por sua vez um guarda prisional. O propósito desta torre era proporcionar a ilusão e a incerteza aos reclusos de que estavam constantemente a ser vigiados, quando na verdade não sabiam se de facto era isso que sucedia, pois não conseguiam ver o interior da torre devido aos holofotes da mesma estarem constantemente apontados para as celas. Assim, o propósito do *Panótico* passa por "(…) induzir no detido um estado consciente e permanente de visibilidade que assegura o funcionamento autoritário do poder. Fazer com que a vigilância seja permanente nos seus efeitos (...) que a perfeição do poder tenta tornar inútil a atualidade do seu exercício"[95]. A verdade é que não existiu qualquer prisão que tenha adotado este mecanismo exatamente como o desenhado na teoria, dada a complexidade e o elevado custo do mesmo, no entanto, sucederam casos de prisões algo semelhantes à desenhada por Jeremy Bentham, tendo resultado muito bem, fazendo com que o número de tentativas de fugas das prisões tenha diminuído substancialmente. O único estabelecimento prisional que adotou o mecanismo quase igual ao *Panótico* foi uma prisão em Cuba, na década de 1920, famosa pela corrupção e crueldade, que se encontra atualmente abandonada. Na altura em que não existiam formas de vigilância digitais, este conceito tinha potencial para se tornar numa maneira muito eficaz de garantir a segurança de um estabelecimento de um elevado grau de importância como é uma prisão. Atualmente, com a evolução da tecnologia, vivemos num contexto com claras analogias, embora de uma forma muito menos evidente e sobretudo mais simples de executar, sendo vulgarmente intitulado como o *Big Brother.* Numa referência à obra seminal de George Orwell, que descreve uma sociedade pautada por um vastíssimo sistema de fiscalização em que passaram a assentar as "democracias", a vigilância permite reunir nos mesmos instrumentos e nos mesmos gestos o trabalho e a fiscalização exercida sobre o cidadão. Assim, "o uso de CCTV[96] no espaço urbano leva-nos, de certa forma, à realidade distópica descrita por George Orwell em 1984, onde tudo podia ser visto pelos olhos do *Big Brother*. Parece ser, numa escala socialmente ampliada, o Panótico das instituições disciplinares

[93] Cabral, M. M. (2012). A colisão entre os direitos de personalidade e o direito de informação. In: *Fruet, G.; Miranda,* J.; Rodrigues Junior, O. (Org.). Direitos da personalidade. São Paulo: Atlas, p. 108-152.

[94] "For Foucault the Panopticon represented a key spatial figure in the modern project and also a key dispositive in the creation of modern subjectivity, in other words in the remaking of people (and society) in the image of modernity. Panopticism, the social trajectory represented by the figure of the Panopticon, the drive to self-monitoring through the belief that one is under constant scrutiny, thus becomes both a driving force and a key symbol of the modernist project." Wood, D. (2003). *Foucault and Panopticism revisited*. Surveillance & Society, 1(3), p. 234-239.

[95] Foucault, M. (1997). Resumo dos cursos do Collège de France: 1970-1982. Tradução de Andrea Daher. Rio de Janeiro: J. Zahar, p. 134.

[96] Closed Circuit Television Camera.

modernas, que mantém um olhar constante sobre toda a população e, neste caso, regula as suas ações"[97], que de acordo com Michel Foucault "*He is seen, but he does not see. Hence the major effect of the Panopticon: to induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of power*"[98].

No momento atual o que se verifica é uma quantidade enorme de mecanismos desenvolvidos não só pelos Estados, como também por empresas, capazes de vigiar os cidadãos de uma maneira discreta ou cujas razões verdadeiras não sejam transpostas para a sociedade. São inúmeras as situações em que, após aprofundado o conhecimento na área, se constata que nem tudo é o que parece e que nem tudo são teorias da conspiração. As pequenas câmaras colocadas em quase todos os aparelhos tecnológicos atualmente serão realmente necessárias? Ou será uma maneira de existirem mais "olhos" para nos poderem monitorar e traçar comportamentos desde que somos pequenos até sermos idosos? Precisamos mesmo de fornecer informações pessoais constantemente em ocorrências do dia-a-dia? Ou será novamente uma ferramenta para estarmos debaixo de olho de quem tem mais poder? São perguntas que, felizmente, cada vez mais vão tendo as respostas reais, mas ao mesmo tempo não parece existir um esforço por parte dos Estados e das empresas para contrariar esta realidade.

Desde o início do presente século, a luta contra o crime tem-se tornado um ponto central nas campanhas políticas. No ano de 2008, a segurança pública e o crime foram considerados as maiores preocupações dos cidadãos, ultrapassando pela primeira vez na história o desemprego.[99] Dado o contexto, os discursos e práticas dos políticos têm-se focado primordialmente em propostas capazes de resolver este novo grande problema, a insegurança. Consequentemente, intensificaram-se os mecanismos de controlo social juntamente com um crescimento de intervenções estatais em espaços públicos, tais como parques, praças e ruas iluminadas ou a monitorização das cidades 24 horas por dia através de câmaras de videovigilância espalhadas pelas mesmas. Acontecimentos como o atentado de 11 de setembro de 2001 provocaram um aumento significativo na vigilância, tendo-se tornado uma rotina e algo tomado como garantido, tornando-se num problema social e político numa nova maneira. Este novo problema é dos mais complexos que a nossa sociedade já experienciou ao longo da história, pois abarca diferentes intervenientes, em que cada defende o seu ponto de vista fazendo com que se torne complicado convergir todas as partes para um meio termo. Por um lado temos aqueles que impulsionam o aumento de ferramentas de vigilância como meio de tentar assegurar uma sociedade mais segura, por outro lado temos aqueles que defendem que aquilo que parecem ser ferramentas que facilitam o dia-a-dia das pessoas são, nos mais comuns casos, ferramentas de recolha de dados que por sua vez são guardados, processados e analisados para o proveito das entidades que os recolhem. Recentemente ficou disponível na plataforma Netflix um

[97] Lio, V. (2016). *The Urban Panopticon*, p. 129.
[98] Tradução: Ele é visto, mas ele não vê. Daí o maior efeito do Panopticon: induzir no prisioneiro um estado de visibilidade consciente e permanente que assegure o funcionamento automático do poder.
[99] Lagos, M., & Dammert, L. (2012). La seguridad ciudadana. El problema principal de América Latina. Corporación Latinobarómetro, 9, p. 31-32.

documentário sobre o escândalo da Cambridge Analytica chamado “Nada é privado: O escândalo da Cambridge Analytica”, onde são expostas as técnicas que originaram a eleição de Donald Trump enquanto Presidente dos Estados Unidos da América, de Jair Bolsonaro enquanto Presidente do Brasil, e muito mais. Este documentário reflete, naturalmente, o posicionamento do seu autor, mas de qualquer forma, vem mostrar ao público mais desatento o cuidado que é preciso ter relativamente ao domínio dos nossos dados pessoais e à nossa privacidade online. O escândalo começou a ganhar contornos mediáticos após a eleição de Donald Trump, que apenas aconteceu (assim o afirmam no documentário) devido à empresa com quem trabalharam, Cambridge Analytica, que foi contratada para fazer, simplesmente, campanha política. Porém, o problema prendeu-se precisamente no modo como esta empresa influenciou os eleitores a votarem no atual presidente dos EUA. Através do Facebook, a empresa, a partir de 2014, deu início à recolha de dados de utilizadores da rede social através de uma aplicação desenvolvida por Aleksandr Kogan, cientista da Universidade de Cambridge, em que consistia numa pesquisa apenas para uso académico, porém, esta aplicação recolhia não só todos os dados de quem concordasse participar neste simples teste de personalidade (sendo que estes deram o seu consentimento para que tal fosse feito, muito provavelmente sem lerem as políticas de privacidade), mas também de todos os seus amigos na rede social Facebook, o que originou que conseguissem nada mais nada menos, do que os dados pessoais de cerca de 87 milhões de pessoas, conseguindo cinco mil pontos de dados sobre todos os eleitores norte-americanos, sendo que procurariam com eles influenciar através de anúncios e imagem (muitas das vezes recorrendo a ataques contra a oposição, neste caso, Hillary Clinton, com afirmações que não estavam ainda comprovadas) os que estariam mais indecisos a votar em Trump. Porém, esta situação só se tornou um problema quando David Carrol, professor na Parsons School of Design, decidiu pedir à empresa todos os dados que a mesma tinha sobre ele, algo que todos temos o direito de fazer. No entanto, a Cambridge Analytica recusou-se a respeitar o pedido de David, o que originou uma batalha entre ambos os lados, tendo com isso ganhado contornos maiores do que alguma vez a empresa tecnológica desejava que acontecesse. David Carrol lamenta dizendo “estávamos tão apaixonados pela conectividade que ninguém se deu ao trabalho de ler os termos de serviço”. No documentário, antigos funcionários da Cambridge Analytica prestaram testemunhos contra a antiga empresa, sentindo remorsos por aquilo que a sua ajuda originou. Brittany Kaiser, uma das grandes propulsoras de todo este acontecimento mostrou todo o seu arrependimento pela situação que causou, afirmando que não queria que fosse este o legado que queria deixar na História. Atualmente, Kaiser, em entrevista ao Dinheiro Vivo, considera que o direito à posse dos dados deve ser visto como um direito básico, dizendo mesmo que “se as pessoas estão a criar valor para uma empresa, então merecem ser compensadas por isso. Não lhes é oferecido, elas têm esse direito”[100].

Existe, geralmente, da parte dos utilizadores a noção de uma espécie de contrato entre o serviço prestado e os detalhes privados oferecidos por estes. Geralmente, talvez sem se debruçarem

[100] Sanlez, A. (2018). *Brittany Kaiser: "Multa à Google foi uma enorme conquista".* [online] Dinheiro Vivo. Disponível em: https://www.dinheirovivo.pt/economia/a-multa-aplicada-a-google-foi-uma-enorme-conquista/ [Acedido a 8 de abril de 2019].

sobre o assunto, os utilizadores, ao aceitarem essa circunstância, assumem que a sua privacidade está a ser respeitada e que os seus dados não serão utilizados para mais do que o necessário, e por isto entende-se a venda de informação para outras empresas de tratamento de dados por exemplo. Para além disso, parece existir nos dias de hoje, um aumento significativo de sistemas colocados com o objetivo de controlar a população, sem que exista um consentimento da mesma, ou apenas mesmo o conhecimento. Como já foi referido anteriormente, o artigo 12.º da Declaração Universal dos Direitos do Homem diz que "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.", no entanto, tal não se está a verificar, sendo preocupante que não exista por parte das autoridades responsáveis uma verificação dos detalhes. É importante perceber então como é que os direitos dos indivíduos são respeitados legalmente.

Esta constante vigilância começa a ser um dado adquirido não só por aqueles que são visados mas também por aqueles que realizam esta prática, algo que se pode perceber através das palavras de Hans-Jörg Albrecht: "A vigilância das telecomunicações, a busca de arrastão[101], a vigilância domiciliária, os agentes encobertos e infiltrados, a vigilância acústica e visual de espaços públicos são cada vez mais objeto de acordo europeu e internacional, como demonstram a Convenção das Nações Unidas sobre Criminalidade Transnacional (a Convenção de Palermo de 2000) ou a Diretiva 2006/24/CE[102] da União Europeia relativa ao armazenamento e utilização de dados de tráfego das telecomunicações."[103] No mesmo texto, Albrecht refere algo bastante preocupante no que toca à invasão da privacidade, neste caso concreto referindo-se a situações de investigações criminais: "A vigilância de telecomunicações tem as características paradigmáticas dos métodos de investigação encobertos ou secretos: os métodos de investigação secretos são ocultados ao arguido e tornam os convencionais direitos do arguido obsoletos; são abrangentes e incidem sobre um elevado número de terceiros; geram um elevado número de informações relativas, não apenas ao passado mas em especial ao futuro ou ao tempo prévio e posterior aos factos; incluem informações independentemente do direito de não prestar declarações das testemunhas; incluem informações independentemente da intimidade e fiabilidade da comunicação." Na Alemanha foi inclusive formado um movimento de defensores dos direitos fundamentais e da proteção de dados pessoais aquando de um muito controverso processo legislativo relativo à transposição para o Direito alemão, da Diretiva do

[101] Busca de suspeitos com determinadas características através de cruzamento de dados efetuada por meio de computador.

[102] de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE.

[103] Albrecht, H. J. (2009). *Vigilância das Telecomunicações: Análise teórica e empírica da sua implementação e efeitos. In Que futuro para o direito processual penal?* Simpósio em homenagem a Jorge de Figueiredo Días, por ocasião dos 20 anos do código de processo penal português. Coimbra Editora, p. 725.

Parlamento Europeu e do Conselho de 15 de março de 2006, relativa à conservação de dados no domínio das telecomunicações, a mesma referida anteriormente[104].

"O desenvolvimento de tecnologias que facilitam a vigilância estatal das comunicações tem evidenciado como os próprios Estados vêm falhando no dever de assegurar que leis e regulamentos relacionados a essa atividade observem os padrões de direitos humanos, protegendo os direitos à privacidade e à liberdade de expressão"[105], no entanto, segundo Klaus Rogall, "os pressupostos para a autorização da vigilância de telecomunicações são os seguintes: tem de existir suspeita de um crime grave, comprovada por factos[106]; o crime em causa deve ser grave no caso concreto (gravidade concreta do facto[107]; e a medida tem de ser necessária para o esclarecimento dos factos ou para investigação do paradeiro do arguido[108]."

Ao contrário do ocorrido no *Panótico*, atualmente os cidadãos, na maioria das situações, não sabem nem quando, nem por quem estão a ser vigiados, na internet por exemplo (que é invisível), não existe uma torre de vigia, mas há muitos olhos a controlarem o comportamento dos utilizadores na rede. "A ideia do Panótico é que é um problema para o sujeito quando está inserido nele, mas pelo menos há um lado de fora. Pode deixar o local de trabalho e deixa de estar no Panótico. Pode deixar a prisão e não está mais no Panótico. Hoje, o capitalismo de vigilância está a criar um ambiente de "não escapatória". Os dados são usados para criar uma previsão sobre, não só para onde alguém se desloca, mas também como se está a sentir, o que provavelmente fará quando chegar a um determinado sítio e quando poderá ser o momento ideal para enviar uma mensagem no telefone sugerindo uma compra de um vestido novo, de um capacete de bicicleta ou de uma prescrição de medicamentos"[109]. No nosso espaço privado online não nos sentimos expostos, portanto, não sentimos que o nosso corpo de informação está a ser vigiado também porque não sabemos onde acaba e começa esse mesmo corpo. Cada vez mais a maioria das pessoas vive grande parte da sua vida online partilhando enormes quantidades de informação, no entanto não sentimos uma relação ou uma importância tão grande como com o nosso corpo. Porém, como já se tem vindo a constatar ao longo do trabalho, os nossos dados, a nossa informação pessoal, a nossa atividade (sobretudo online), encontram-se sob vigilância, não apenas por parte dos governos, mas igualmente por parte das empresas que fazem enormes quantidades de dinheiro capitalizando os dados pessoais. Uma maneira mais simples de compreender esta constante vigilância é tentando perceber como funcionam as

[104] Presente em Rogall, K. *A nova regulamentação da vigilância das telecomunicações na Alemanha,* em: *2º Congresso de Investigação Criminal*, ASFIC-PJ e IDPCC-FDUL, p. 119.
[105] Consultado em: International Principles on the Application of Human Rights to Communications Surveillance
[106] Crimes enunciados num catálogo constante do §100a Abs. 2 StPO. "Crime grave" é mais do que um "crime de significado relevante", mas menos do que um "crime especialmente grave".
[107] Com isto, o legislador pretende que o Tribunal se confronte com a situação, fundamentando a sua decisão, não se limitando a conceder formalmente o requerimento do Ministério Público, sem uma confirmação atenta.
[108] A medida torna-se necessária quando o esclarecimento dos factos ou a descoberta do paradeiro do arguido se revelem muito difíceis ou impossíveis de realizar com o recurso a outros meios.
[109] Zuboff, S. (2017). Shoshana Zuboff: No escape from the Panopticon. Disponível em: https://sciencenode.org/feature/shoshana-zuboff,-part-one-no-escape-from-the-panopticon.php [Acedido a de 2 março de 2019]

tecnologias presentes na nossa vida bem como as que ainda estão por surgir. Visto que a inteligência artificial[110] é cada vez mais uma realidade na nossa sociedade, e com o avançar da tecnologia e o aumento da comunicação entre dispositivos inteligentes faz com que seja e que continue a ser, necessário albergar imensas informações pessoais que permitem a comunicação entre os aparelhos, colocando a privacidade (ou a falta dela) num risco cada vez maior. O problema maior nesta questão é que esta informação pessoal não vai ser transmitida somente entre estes dispositivos inteligentes, mas também entre empresas e governos. Tudo desde aparelhos de monitorização do ritmo cardíaco até GPS no calçado, temos mais uma vez um holofote na nossa direção. O recém-falecido Stephen Hawking[111] e o criador e CEO da Tesla, Elon Musk[112], avisaram precisamente para o perigo desta questão. Por exemplo, como menciona Joe Shute no seu artigo "Can anyone escape Brittain's surveillance state?", publicado no jornal Telegraph[113], as pessoas que têm iPhones podem não estar despertas para a situação, mas existe um programa chamado "Frequent Locations" inserido nas definições de privacidade que faz um rastreio de todos os nossos movimentos, bem como a data e hora desses mesmos movimentos. Nas televisões inteligentes, como é o caso das da Samsung[114], foi descoberto que estas realizam uma gravação de conversas com o intuito de partilhar essas conversas com a empresa e terceiros. Richard Tynan, da Privacy International, ONG britânica que monitoriza a vigilância exercida por ordem governamental, chama a estes fenómenos "o caminho da vida", pois "está-se a tornar cada vez mais impossível de deixar de criar algum tipo de registo sobre o que alguém está a fazer e deixar algum tipo de rasto que uma empresa ou governo possa aperfeiçoar para tentar o rastrear,"[115].

Muitas das fundamentações dadas para justificar a inclusão destes dispositivos na sociedade são os benefícios que proporcionam à saúde e bem-estar das pessoas, o que não é mentira, até certo ponto, têm é de ser pesados os prós e os contras em vez de se procurar apenas evoluir as tecnologias sem pensar nas repercussões. Neste caso pode não existir uma torre central, mas existem sensores nos nossos objetos pessoais capazes de comunicarem entre si e para o exterior. O objetivo de Bentham aquando da criação do *Panótico* não era que este fosse tornado numa ferramenta de opressão, sendo que mais tarde, dado o falhanço do mesmo, levou-o a desenvolver uma espécie de

[110] Termo que surgiu em 1956 por John McCarthy, cientista de computação Americano, e que atualmente é definido pelo English Oxford Living Dictionary como "a teoria e o desenvolvimento de sistemas computacionais capazes de realizar tarefas que normalmente requeriam a inteligência de um ser humano para tal, tal como perceção visual, reconhecimento de voz, tomada de decisões e tradução de idiomas".

[111] "The development of full artificial intelligence could spell the end of the human race.", disse o cientista em entrevista à BBC, tal como "Humans, who are limited by slow biological evolution, couldn't compete, and would be superseded."

[101] Musk diz que se trata da "maior ameaça à humanidade existente"

[113] Shute, J. (2019). *Can anyone escape Britain's surveillance state?* Disponível em: https://www.telegraph.co.uk/technology/news/11831533/Can-anyone-escape-Britains-surveillance-state.html [Acedido a 23 de junho de 2019].

[114] Matyszczyk, C. (2015). *Samsung's warning: Our Smart TVs record your living room chatter*. [online] CNET. Disponível em: https://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/ [Acedido a 12 de agosto de 2019].

[115] Shute, J. (2019). *Can anyone escape Britain's surveillance state?* Disponível em: https://www.telegraph.co.uk/technology/news/11831533/Can-anyone-escape-Britains-surveillance-state.html [Acedido a 23 de junho de 2019].

anti panótico, situação em que um ministro se senta no centro de uma sala aberta, rodeado por membro do público que o escutam e colocam perguntas.

3.4. Pode haver equilíbrio entre a vigilância constante e a privacidade?

O sistema legal dos Estados Unidos da América impede que as forças policiais e os serviços de informação consigam aceder às comunicações privadas de cidadãos americanos sem a posse de um mandato[116], algo que tem vindo a evoluir com o passar dos anos, pois após o trágico acontecimento terrorista de 11 de setembro de 2001, em Nova Iorque, teve lugar um aumento de legislação antiterrorista, mais concretamente o chamado "USA Patriot Act", que proporcionava um novo e vasto leque de poderes ao governo americano para realizar vigilância eletrónica na Internet. A legislação providenciava ao governo a possibilidade de poderem colocar escutas telefónicas, a eliminação de barreiras entre as agências policiais e as agências de inteligência e concedia uma maior autoridade à procuradoria geral para deter e deportar estrangeiros suspeitos de terem ligações terroristas.[117] Anos mais tarde, em 2015, surgiu o "USA Freedom Act", que teve como objetivo substituir a lei mencionada anteriormente, pois esta não foi exatamente eficaz como era esperado[118], e acrescendo a isso, após as revelações de Edward Snowden em 2013 acusando o governo de abusar da lei, revelando documentos secretos comprovando isso mesmo, o governo viu-se obrigado a realizar alterações à legislação. Esta lei, assegurava o governo de Barack Obama, foi imposta com o intuito de assegurar ao povo americano que o governo já não estava atrás das informações dos cidadãos, embora mais tarde se tenha vindo a comprovar que tal não era verdade. Considerado de maior importância, o "Freedom Act" obrigou a que a National Security Agency (NSA) terminasse com a recolha de informação telefónica em massa e permitiu que as empresas pudessem reportar publicamente aos seus clientes em situações em que o governo solicite informações dos mesmos.[119]

Os tribunais, porém, têm tido alguma dificuldade em estabelecer concretamente o que constitui exatamente a privacidade online e os limites da mesma. O juiz do Supremo Tribunal Americano, Louis Brandeis, referindo-se à privacidade, diz que esta "é o mais compreensivo dos direitos e o mais valorizado por pessoas civilizadas". Comentadores afirmam que "é essencial para governos democráticos", crítica "para manter a nossa capacidade de criar e manter diferentes tipos de relações sociais com diferentes pessoas", necessária para "permitir e proteger uma vida autónoma", e importante para alcançar uma "tranquilidade emocional e psicológica".[120] O Brasil afirma que "a

[116] U.S. Department of Justice (2019). *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*. White Paper, p. 8-9.
[117] McCarthy, M. T. (2002). *USA patriot act*, p. 1.
[118] Lind, D. (2015). *Everyone's heard of the Patriot Act. Here's what it actually does*. [online] Vox. Disponível em: https://www.vox.com/2015/6/2/8701499/patriot-act-explain [Acedido a 8 de julho de 2019].
[119] Kapocsi, C. (2018). *What is the USA FREEDOM Act? What's So Free About It?* Disponível em: https://www.cloudwards.net/freedom-act/ [Acedido a 27 de agosto de 2019]
[120] Parent, W. A. (2017). *Privacy, morality, and the law*. In Privacy, p. 105-124.

privacidade, a vida privada, a honra e a imagem das pessoas são invioláveis", a África do Sul proclama que "toda a gente tem o direito à privacidade", a Coreia do Sul diz que "a privacidade dos cidadãos não deve ser infringida". Existem países em que a privacidade não se encontra diretamente mencionada nas suas constituições, no entanto, os tribunais de muitos desses países reconheceram direitos constitucionais implícitos à privacidade, como foi o caso de países como o Canadá, França, Alemanha, Japão e Índia. É evidente que a privacidade é cada vez mais um tema discutido, resultado também da maior consciencialização por parte dos cidadãos, no entanto, ao mesmo tempo, é difícil incutir a necessidade de alterar comportamentos, rotinas que "sempre" tivemos sem pensar nos prós e contras dos mesmos.

Mesmo que a realidade em que vivemos atualmente não nos permita escapar ao *Panótico ou ao Big Brother*, tem sim de existir uma adaptação e uma utilização inteligente e esclarecida dos direitos que todos temos, em simultâneo com o desenvolvimento de instrumentos eficazes por parte dos reguladores que permitam a todos os cidadãos uma fácil e intuitiva aplicação dos mesmos.

Constitucionalmente, a expectativa daquilo que é privado, encontra-se razoavelmente delineado, mas, no entanto, os tribunais deparam-se com alguns problemas para determinar o que constitui uma expectativa razoável de privacidade on-line. O principal ponto de divergência prende-se com a questão de, se essas tais previsões são determinadas pelo que o governo pode coletar ou pelo que deveria coletar, porque a realidade é que o governo pode coletar seja o que for, portanto, se se recusar a respeitar a privacidade, qualquer expectativa de privacidade deixa de ser razoável. A alternativa passa pelos tribunais, levando a cabo uma determinação normativa, isto é: quando os cidadãos agem de modo a considerarem as suas comunicações como privadas, os tribunais devem decidir de forma a que se honre isso mesmo, ainda que o governo possa possuir a tecnologia para aceder a essas informações.

Porém, não é somente neste ponto que termina o problema da constante vigilância. A contribuir para o mesmo encontram-se as empresas, que se alimentam de uma recolha de dados privados sem limites, com o objetivo de obter lucro ou vantagem comercial sobre as outras empresas, fazendo com que, se seja levado a um excesso, de tal forma que quando se lida com quantidades enormes de informação, se perca o controlo das mesmas, ameaçando assim a privacidade de todos os cidadãos, num mundo conectado onde há cada vez mais pessoas a viverem a maior parte das suas vidas em mundos virtuais, fornecendo mais dados de onde são extraídas mais e mais informações, recorrendo normalmente a técnicas de data mining[121]. Não são apenas informações bancárias que podem ser recolhidas no mundo virtual, algo que, felizmente, muitas pessoas já estão alertadas para, e evitam ao

[121] Em português "mineração de dados", que é "parte de um processo maior conhecido como KDD (Knowledge Discovery in Databases) – em português, Descoberta de Conhecimento em Bases de Dados –, que, segundo Addrians & Zantinge (1996), permite a extração não trivial de conhecimento previamente desconhecido e potencialmente útil de um banco de dados. Esse conceito é enfatizado por Fayyad et al. (1996b), ao afirmar que é "o processo não trivial de identificação de padrões válidos, desconhecidos, potencialmente úteis e, no final das contas, compreensíveis em dados". - Conceitos e Aplicações de Data Mining, Data Mining, Heloisa Helena Sferra e Ângela M. C. Jorge Corrêa.

máximo expor-se online nesse sentido, com a crescente evolução da tecnologia cresce também o número de pessoas que procuram tirar proveito da mesma, e por isso, deveria existir um acompanhamento recíproco de conhecimento do que fazer para nos protegermos, mas muitas vezes não é isso o caso. Deste modo, deveria caber aos governos (e no caso dos países da União Europeia, um trabalho conjunto entre esta e todos os Estados-Membros) assumir um papel urgente de liderança na proteção da privacidade dos consumidores contra invasões privadas que reforçasse e melhorasse a presente lei no sentido de não só eles, mas também as empresas respeitassem um limite previamente definido da privacidade dos cidadãos.[122] Porém, visto que não é possível determinar quando é que tal pode acontecer, deve existir um esforço por parte dos cidadãos em protegerem-se a si, bem como os seus dados pessoais. Esta proteção que deve ser levada a cabo diariamente, deve ter em consideração não apenas o governo e as empresas, mas também possíveis pessoas mal-intencionadas que objetivam tirar proveito de outras, e isso pode fazer-se através de:

1. Perguntar sempre o porquê de precisarem da nossa informação – seja online, em pessoa ou por telefone, é importante certificarmo-nos que concedemos apenas a informação necessária a quem diz precisar dela. Mais recentemente em Portugal tem havido uma consciencialização por parte dos cidadãos referente ao Cartão de Cidadão, visto que ninguém é obrigado a conceder uma cópia do mesmo seja em que circunstância for. Mas em situações mais recorrentes em que nos pedem a morada ou o código postal, visto que são dados de alguma relevância, devemos evitar transmiti-los quando não é necessário.

2. É muito importante ler, efetivamente, as condições e termos de privacidade das aplicações e não instalarmos se não concordarmos com os dados que temos que ceder.

3. Reforçar as passwords em todos os aparelhos eletrónicos – não só pelo facto de poderem ser furtados, mas também pela cada vez maior facilidade em entrar indevidamente num computador, tablet, smartphone, etc., e também em contas online (email, redes sociais, finanças, etc.) é importante proteger esses mesmos aparelhos e contas da melhor maneira e o primeiro passo é mesmo o reforçar das palavras-passe. Para além da complexidade que estas devem ter, não devem ser repetidas, pois no caso de se descobrir uma descobrir-se-ia automaticamente as palavras-passe de todas as contas. Para facilitar a gestão de todas as passwords deve usar-se um gestor de palavras-passe que trata de encriptar e armazenar todas estas, protegido através de uma password mestre;

4. Assegurar que o computador não tenha a presença de vírus – caso um computador (por ex.) esteja infetado com um vírus ou *malware*, permite não só que hackers possam visualizar a informação pessoal da pessoa e até roubar-lhe a identidade, mas podem também bloquear o acesso aos documentos, por parte do dono legítimo deles, e exigir um

[122] Fairfield, J. A. (2009). *Escape into the Panopticon: Virtual worlds and the surveillance society*. *Yale Law Journal Pocket Partigo* p. 132-133.

resgate para devolver acesso, chamado ataque de *ransomware*[123]. Portanto, deve existir um cuidado e bom senso por parte das pessoas e escolher um antivírus eficaz, capaz de fazer frente a possíveis ataques.

5. Garantir a segurança do Navegador (Browser) – sendo que é através destes que interagimos com o mundo digital é importante que se encontrem seguros e que não deixemos pegadas digitais à medida que "surfemos na net". Muitas vezes são websites e *marketeers* a seguirem os nossos movimentos, mas noutras ocasiões pode mesmo ser um hacker a espiar o nosso comportamento. Uma das primeiras coisas a fazer é desligar uma opção que existe nos browsers chamada de "third-party *cookies*[124]". Se é verdade que as *cookies* facilitam em muitas questões, são igualmente muito evasivas da nossa privacidade, e para garantir logo na raiz do problema não sermos sujeitos a estas, basta navegar online usando a opção de navegação anónima.

6. Ter cuidado naquilo que partilhamos online – a verdade é que, quando estamos nas redes sociais, muitas vezes pode parecer que estamos a ter uma conversa pessoal, mas tal não podia estar mais errado. Se existir uma grande exposição online e dado o funcionamento da internet, passamos rapidamente a mostrar-nos demasiado ao mundo, podendo haver quem consiga, com essa informação, fazer um perfil dessa pessoa podendo inclusive começar a segui-la na vida real, o que é muito perigoso. É, portanto, muito importante que não adicionemos pessoas desconhecidas à nossa rede social privada e que tenhamos o conteúdo partilhado restrito a essas pessoas de confiança.

7. Não nos deixarmos apanhar em esquemas – cada vez mais há que ter atenção a determinados sites, emails e chamadas telefónicas que solicitam os nossos dados pessoais, isto porque, como tudo, quem pratica este tipo de atividades está a evoluir tornando-se mais perigoso. Há que ter, necessariamente, cada vez mais cuidado com estes esquemas, exigindo a nossa atenção e desconfiança em situações desta natureza.

[123] "Ransomware is a category of malicious software which, when run, disables the functionality of a computer in some way. The ransomware program displays a message that demands payment to restore functionality. The malware, in effect, holds the computer ransom. In other words, ransomware is an extortion racket.", O'Gorman, G. and McDonald, G. (n.d.). *Ransomware: A Growing Menace*. [online] Symantec.com. Disponível em: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf [Acedido a 14 de julho de 2019], p. 2.

[124] "A third-party cookie is one that is placed on a user's hard disk by a Web site from a domain other than the one a user is visiting. As with standard *cookies*, third-party *cookies* are placed so that a site can remember something about you at a later time. Both are typically used to store surfing and personalization preferences and tracking information. Third-party *cookies*, however, are often set by advertising networks that a site may subscribe to in the hopes of driving up sales or page hits." - Rouse, M. (2014). *What is third-party cookie?* - Definition from WhatIs.com. [online] WhatIs.com. Disponível em: https://whatis.techtarget.com/definition/third-party-cookie [Acedido a 8 de julho 2019].

8. Usar apenas softwares confiáveis – seja no telefone ou no computador, existem softwares capazes de coletar informação pessoal dos utilizadores indevidamente. Caso não tenhamos a certeza do que estamos a instalar, o melhor é mesmo não o fazer.

9. Usar apenas redes Wi-Fi de segurança – redes públicas podem muitas vezes ser um palco para pessoas mal-intencionadas espiarem a atividade dos utilizadores. Se a usarmos para acedermos a contas pessoais deve ter-se o cuidado de usar um serviço VPN de modo a encriptar toda a informação enviada.[125]

Ao contrário do que ainda muitas (demasiadas) pessoas pensam, há muito mais que pode ser intercetado no mundo digital para além de informação como os números dos cartões de crédito. A chamada "falsa anonimidade" no ciberespaço, fez com que muitos utilizadores ao terem movido importantes dimensões das suas vidas pessoais para o online, passaram a poder ser monitorizadas, possibilitando que, mais do que hackers, as próprias empresas possam seguir e processar todo e qualquer atividade a ocorrer neste meio. O governo deveria assumir um papel importante neste aspeto e procurar proteger a privacidade do consumidor contra invasões da mesma, reforçando (com recurso a ferramentas como o Regulamento Geral de Proteção de Dados) as leis relacionadas com o acesso indevido a informação privada, com ênfase no consentimento dado pelos portadores dos dados.

Importa então perceber se existe espaço para que a vigilância em massa continue a ser colocada em prática sem ser demasiado evasiva para com a privacidade dos cidadãos, ou se é necessário uma mudança de paradigma. É por demais evidente que se tem vindo a fazer um caminho no sentido de dar cada vez mais valor à privacidade de cada um de nós, cidadãos, já existindo legislações que visam de facto colocar um fim às violações a que somos muitas vezes sujeitos. No entanto, a maioria dos sistemas pecam, ainda, por não terem mecanismos de controlo eficazes, permitindo que exista um incumprimento por parte das organizações sem que as devidas consequências sejam impostas. Enquanto não existir um funcionamento correto nesta matéria irão continuar a existir indesejáveis casos (por muito excecionais que venham a ser no futuro) de invasão da privacidade. Concluindo, tão importante como o mencionado acima é assegurarmo-nos que o povo se encontra bem educado e consciente para os riscos que o seu comportamento diário pode acarretar à sua privacidade e, enquanto isso, se o excesso de mecanismos de vigilância tanto por parte dos Estados como das organizações não reduzir e se continuar a encarar a informação pessoal como um bem/recurso, o equilíbrio muito dificilmente será alcançável.

[125] Harper, E. (2018). *9 Simple Ways to Protect Your Privacy*. [online] Techlicious.com. Disponível em: https://www.techlicious.com/tip/simple-ways-to-protect-your-privacy/ [Acedido a 26 de junho de 2019].

4. Estudo de caso

4.1. Método de pesquisa

Perante a problemática abordada ao longo deste trabalho ficou patente que o ciberespaço é uma zona de risco para a segurança dos nossos dados pessoais e que o controlo desses dados é sobretudo responsabilidade do cidadão, que deve estar empoderado das competências que lhe permitam fazer valer os direitos salvaguardados pelas regulamentações existentes.

Que conhecimento têm os cidadãos dos instrumentos à sua disposição para fazer valer os seus direitos? Será que os cidadãos estão mesmo interessados nessa tarefa?

Estas questões foram, no essencial, o estímulo para a realização deste trabalho, que na primeira parte procurou contextualizar as dimensões teórico normativas dos direitos associados à salvaguarda da privacidade. No entanto pareceu-nos relevante tentar criar um retrato atual da forma como os cidadãos se posicionam perante estas problemáticas e foi nesse sentido que se criou o instrumento que deu origem a este estudo de caso, recorrendo a uma amostra que pode ser definida como "um subconjunto de uma população ou de um grupo de sujeitos que fazem parte da mesma população (…) É, de qualquer forma, uma réplica em miniatura da população alvo."[126]. A pesquisa tem uma natureza exploratória descritiva tem como objetivo identificar opiniões expressas na generalidade da população, assim como relatar a distribuição do fenómeno na população ou entre subgrupos da mesma ou ainda, realizar uma comparação entre as distribuições.[127] Foi então efetuada uma pesquisa de corte transversal, com o propósito de descrever e analisar o estado de uma ou mais variáveis. Após a problematização desenvolvida na parte inicial da dissertação realizou-se uma pesquisa no terreno com o objetivo de percebermos o é que o indivíduo sente relativamente à sua privacidade.

4.2. Interpretação dos resultados

Para este caso, a população-alvo utilizada para o estudo foi a população residente em Portugal com idades compreendidas entre os 18 e 85 anos, que segundo dados da PORDATA[128] de 2018 totalizava cerca 8 200 000 milhões de utilizadores, sendo que foram inquiridas um total de 364 pessoas, onde 175 das mesmas eram do sexo masculino e as restantes 189 do sexo feminino. Na primeira parte do instrumento foram aplicadas algumas questões sócio demográficas, procurando com

[126] Fortin, M. F. (1999). *O Processo de Investigação: Da Conceção à Realização.* Loures, Lusociência – Edições Técnicas e Científicas, Lda, p. 202.

[127] Pinsonneault, A., & Kraemer, K. (1993). Survey research methodology in management information systems: an assessment. Journal of management information systems, 10(2), 75-105, p.4.

[128] Pordata.pt. (2019). *População residente média anual total e por grupo etário*. [online] Disponível em: https://www.pordata.pt/Portugal/Popula%c3%a7%c3%a3o+residente++m%c3%a9dia+anual+total+e+por+grupo+et%c3%a1rio-10 [Acedido a 23 de agosto de 2019].

isto realizar a caracterização da amostra. Numa segunda instância foram inseridas questões que procuram avaliar o tipo de interação que os inquiridos possuem com serviços digitais na rede. Na terceira secção, “Perceções sobre a privacidade e segurança da informação”, foi utilizada o item Likert, com uma variação de cinco pontos, entre 1 (menor concordância com as afirmações) e 5 (discordância total com as mesmas), para obter maior exatidão relativamente à intensidade com a qual a pessoa concorda ou discorda da afirmação. Por último, na quarta parte do questionário foram aplicadas questões sobre o conhecimento do inquirido sobre os direitos e deveres perante a privacidade da informação, com o objetivo de avaliar o conhecimento dos inquiridos relacionado com a privacidade e segurança de informação. Quase metade dos inquiridos tinham a sua idade compreendida entre os 18 e os 24 anos de idade, sendo que a segunda fatia mais significativa dizia respeitos ao intervalo de idade entre os 50-59 anos. 72,1% das pessoas indagadas encontram-se empregadas, 21,5% são estudantes, 5,7% encontram-se em situação de desemprego e apenas 0,8% são domésticos(as). Nesta primeira fase do questionário a última questão dizia respeito às habilitações escolares, onde se verificou que a maioria dos inquiridos (55,8%) são licenciados, praticamente ao mesmo nível encontram-se as pessoas com mestrado e com o ensino secundário concluído, com 20,2% e 19,3% respetivamente. Por último, 3,3% pessoas são doutoradas e apenas 1,4% têm somente o 9º ano de escolaridade. Num segundo momento procuramos traçar o perfil de cibernauta das pessoas onde verificámos que quase todas elas possuem conta na rede social Facebook (96,7%), 91,2% são utilizadoras do Whatsapp e 79,3% são membros do Instagram. Como seria expectável, o número de pessoas sem qualquer conta numa rede social é bastante reduzido, foram somente 4 pessoas que assinalaram essa opção, perfazendo 1,1%. Para a questão acerca dos serviços pagos subscritos, numa amostra de 184 pessoas, neste seguinte caso, 72,8% são subscritoras da Netflix e 34,2% do Spotify. Na pergunta que se segue é que se começa a aprofundar mais o questionário para onde o queremos encaminhar, procurando, neste caso, saber quantas pessoas leram as políticas de privacidade ou termos de aceitação dos serviços e redes sociais em que possuem conta, o que mostrou, sem surpresa, que a maioria (51,7%) não leu nenhum termo ou política em qualquer das redes ou serviços. De seguida segue-se com 36,5% aqueles que fizeram uma leitura resumida dos mesmos, e com percentagens ínfimas encontram-se aqueles que leram alguns e todos detalhadamente. Estes números mostram bem aquilo que se verifica para a generalidade das pessoas, a ausência de preocupação e sobretudo a confiança que depositamos nas aplicações que instalamos, nos sites que visitamos e nos serviços que subscrevemos, sem realizarmos na maioria das vezes qualquer leitura das políticas de privacidade ou termos de aceitação das mesmas, fazendo com que fiquemos sujeitos a correr riscos contra a nossa privacidade e segurança desnecessariamente. No entanto, na pergunta seguinte, que pertence já à terceira parte do questionário, há quase que como um contrassenso com a anterior, pois quando questionamos se os inquiridos se se importam quando um site divulga os seus padrões de compra a terceiros 39% responderam dizendo que se importam muito, 27,1% que se importam moderadamente, sendo que apenas 4,1% é que afirmam não se importarem com isso. Ora, na maioria das políticas de privacidade de sites e aplicações, é referido precisamente que grande parte das informações disponibilizadas irão ser partilhadas com outras empresas, e o consumidor, quase sempre, concorda com essas políticas. Na pergunta seguinte

questiona-se se os inquiridos sentem que os seus dados pessoais se encontram seguros na organização onde desenvolvem a sua atividade, sendo que o maior número de respostas incidiu sobre a terceira opção, opção essa que significa algum desconhecimento relativamente a esse tema dentro da sua organização. Novamente com maior incidência na opção número 3 foi a pergunta seguinte, onde se questiona se o controlo das informações pessoais enquanto consumidor/cliente ajuda a reforçar a privacidade ou se independentemente desse esforço, as empresas, se quiserem, farão o que bem entenderem com os dados pessoais dos clientes. Com estas respostas pode-se concluir que existe uma incerteza presente nos inquiridos relativamente ao que acontece nessa situação, algo que pode ocorrer também por existir pouco conhecimento geral acerca do que as empresas fazem ou não com os nossos dados pessoais.

Quando se questiona as pessoas se se sentem incomodadas quando as empresas lhe pedem informações pessoais, é notório que a grande maioria (mais de 60%) se sente de facto importunada ou muito importunada com essa situação. No seguimento desta pergunta, e em conformidade com as respostas anteriores, questionou-se desta vez se quando sucede a situação anteriormente descrita, se o inquirido prefere ou não usufruir das possíveis vantagens que o fornecimento dos dados pessoais lhe iria trazer, ao que a grande maioria das pessoas (72,7%) respondeu que prefere não usufruir dessas possíveis vantagens. Como foi referido anteriormente, ainda estamos numa fase de algum desconhecimento acerca do que as empresas fazem com os nossos dados pessoais, no entanto, com as respostas nesta questão, é seguro concluir que, apesar desse possível desconhecimento, as pessoas preferem não arriscar e assegurar que a sua privacidade se encontra, por pouco que seja, mais intacta do que beneficiar dessas tais vantagens que a empresa providencia. Prova disso mesmo, mais uma vez, são as respostas dadas na pergunta seguinte, em que praticamente a mesma percentagem (72,9%) respondeu que é motivo de preocupação pensar que as organizações possam conter nas suas bases de dados diferentes versões das informações pessoais dos clientes, muitas das vezes incorretas. Neste caso, apenas 8% dos inquiridos é que acreditam que o questionado não se verifica. Prova de que a privacidade possa ser de uma importância maior para os cidadãos do que aquela que inicialmente se pensa, são as respostas da pergunta “Em qual ou quais destas circunstâncias é que aceitaria que, não só as empresas como também o Estado, tenham acesso aos seus dados privados presentes nos nossos aparelhos tecnológicos?”, ao que quase 50% dos inquiridos responderam que só com ordem judicial é que providenciavam os seus dados, 45,3% em situações de ameaça terrorista e 18,2% afirmam que em nenhuma circunstância o fariam. Estas respostas mostram que só os cenários mais extremos é que levariam as pessoas a fornecer os seus dados pessoais. Indo agora de encontro ao foco do trabalho, a pergunta seguinte diz respeito aos direitos de personalidade, mais concretamente, procurar saber se sentem que os mesmos estão a ser colocados em risco face à constante vigilância a que estamos sujeitos, ao que a grande maioria (68,2%) afirmou que sim, 19,1% dizem que não e 12,7% declaram não ter conhecimento na matéria. Caminhando para a fase terminal desta terceira parte do questionário, foi questionado se os inquiridos têm a noção de que a sua informação pessoal tem valor monetário para as empresas, ao que 50,8% dos mesmos dizem ter noção disso, mas ao mesmo tempo afirmam não saber o que podem fazer para alterar essa prática. 19,9% dizem igualmente saber, referindo que irão tomar medidas para limitar o uso das suas informações

pessoais, 16% declaram não saber que tal sucedia, 12,7% dizem, mais uma vez, saber, mas não se importam pois também fazem uso dos serviços dessas empresas gratuitamente e, por último, apenas 2 pessoas afirmam não acreditar que o questionado se verifica. Após estas perguntas, achámos interessante questionar se os indagados estariam interessados em frequentar um curso gratuito online sobre a proteção de dados e a segurança de informação (disponibilizados pela *nau*, plataforma da Direção Geral de Educação) ao que 41,2% responderam talvez, 37,3% mostraram-se interessados e 21,5% não expuseram essa vontade. As conclusões, embora interessantes, são confusas, pois existe por parte dos inquiridos a intenção de alterar o modo como se relacionam com as empresas e o estado no sentido de garantirem um maior controlo dos seus dados pessoais, no entanto, quando são questionados se frequentariam um curso gratuito online relativamente a este tema, as respostas afirmativas têm uma percentagem abaixo do esperado, algo que ainda é mais surpreendente pelo facto de muitos terem respondido que queriam alterar o modo como se relacionam com as entidades anteriormente referidas, mas não saberem como o podem fazer.

Na última parte do questionário, como já foi referido, decidimos fazer 5 perguntas que testassem o conhecimento dos cidadãos na matéria. A primeira, questionava se independentemente da forma como as organizações obtiveram as informações pessoais de alguém, se pode ser pedido que as mesmas sejam eliminadas, ao que 49,8% responderam acertadamente na resposta “Sim, desde que não exista nenhum vínculo contratual”. Na segunda questão procurámos verificar o conhecimento dos inquiridos sobre um dos temas abordados inserido na diretiva que mais se tem falado ultimamente no meio empresarial, o Regulamento Geral de Proteção de Dados, mais concretamente o que se considera ser a nossa informação pessoal. 50% responderam erradamente na resposta “tudo o que pode ser definido como pessoal para si”, algo que não seria possível de regulamentar, pois daria azo a que existissem diferentes noções daquilo que cada pessoa consideraria pessoal. 24,6% acertaram na resposta certa que é “o mencionado acima (o seu nome, email, data de nascimento, número de identificação, dados bancários, publicações nas redes sociais, informação médica, o IP do seu computador e, em determinadas circunstâncias, imagens suas e informação dos seus familiares, entre outras informações”. Na terceira pergunta colocou-se o seguinte cenário aos inquiridos: “surgiu uma nova rede social onde se registou, tendo fornecendo vários dados pessoais necessários à definição do seu perfil. Qual das seguintes opções considera ser a mais correta no que toca ao tratamento transparente dos seus dados?” e verificou-se uma grande proximidade entre as respostas dadas, sendo que aquela que mais incidência teve (29,3%) foi a que diz “o tratamento de dados pessoais só pode ser feito com base no consentimento do titular do dados”, a que mais respostas obteve de seguida foi a que refere “o tratamento só pode ser feito se o titular dos dados pessoais compreender todas as consequências decorrentes do tratamento dos seus dados pessoais”, e só em 3º lugar é que surge a resposta certa, com 25,1%, onde consta “o tratamento tem de ser feito tendo na sua base uma lei, no consentimento, em negociações ou na celebração de um contrato e, em todos os casos, indicando ao titular dos dados, com linguagem concisa e clara, as finalidades do tratamento e um conjunto de outras informações que lhe permitam compreender o que é feito com os seus dados pessoais”. Mais uma vez, na questão seguinte, resolvemos colocar uma situação hipotética aos cidadãos, perguntando “em qual das seguintes situações não foi feito o uso dos seus dados pessoais?”, ao que 68,5% das pessoas

acertaram na resposta, que diz "respondi anonimamente a um inquérito sobre o consumo de frutas e vegetais". Por último, e acabando todo o questionário com muitas respostas certas, procurámos saber se era do conhecimento geral a função da Comissão Nacional de Proteção de Dados, ao que 79,8% responderam acertadamente "fiscalizar o tratamento de dados pessoais realizados pelas entidades privadas e pelas entidades públicas".

Com recurso ao software estatístico SPSS, foi feita uma análise mais detalhada com o objetivo de perceber se as características individuais têm relação direta com o tipo de resposta dada. Realizou-se os testes com mulheres e homens, mulheres com e sem ensino superior, homens com e sem ensino superior, homens e mulheres com idades compreendidas entre os 18 e os 29 anos e também entre os 30 e os 59 anos. O que foi possível retirar da extração e consequente análise dos dados no software foi que, na maioria dos casos, se verifica a existência de um padrão nos resultados obtidos para a generalidade das respostas dadas pelos inquiridos, apenas com a existência de ligeiras variações. Porém, em determinadas situações, verifica-se que os cidadãos com ensino superior tendem a ter outro tipo de respostas do que os não possuem ensino superior e, aqueles com idades compreendidas entre os 18 e os 29 anos têm ocasionalmente respostas distintas dos com idades entre os 30 e os 59 anos, como é possível constatar no anexo 1. Neste caso em que se questiona se estariam dispostos a frequentar um curso gratuito online, o que se constata é que os inquiridos mais jovens e também os que não possuem acreditação superior têm mais tendência em responder negativamente à questão colocada, enquanto que os restantes respondem mais frequentemente que estariam interessados em frequentar o curso. Esta situação pode ser explicada pelo facto de aqueles que possuem licenciatura, mestrado ou doutoramento estarem mais habilitados para responder a este tipo de problemáticas por estarem mais cientes dos riscos a que hoje a nossa privacidade se encontra sujeita. Relativamente aos cidadãos mais novos, o facto de muitos deles se estarem a iniciar no mercado de trabalho e na vida adulta, pode fazer com que ainda não se encontrem completamente despertos para certas situações que ocorrem na sociedade, como a questão da privacidade. No anexo 2, quando se compara os mesmos grupos de pessoas, desta vez questionando se se importam quando um *site* divulgam os seus padrões de compras a terceiros, o que se pode verificar é que os mais jovens, novamente, têm menos tendência a sentirem-se importunados que os mais velhos. Já no caso dos sujeitos com ou sem nível de ensino superior, apesar de existirem variações, estas não são de todo significativas. No mesmo sentido, no anexo 3 não existem variações representativas quando se procede à comparação entre as diferentes segmentações da amostra, quando se questiona em quais das situações é que estariam dispostos a conceder acesso aos seus dados privados nos aparelhos tecnológicos, sendo que os casos de ameaça à segurança nacional[129] é o que maior ocorrência tem. Por último, e novamente com alguma semelhança às anteriores questões, quando se pergunta se é motivo de preocupação para os inquiridos pensar que os seus direitos de personalidade estão a ser colocados em risco fruto da constante vigilância a que somos sujeitos diariamente, é percetível, no anexo 4, que

[129] Decidiu-se, por questões práticas englobar as respostas "ameaça terrorista", "ameaça ambiental", investigação criminal cível" e "investigação criminal financeira" numa só categoria intitulada de "ameaça à segurança nacional".

há uma maior incidência na resposta sim em todas as diferentes segmentações. A análise segmentada nas diferentes questões mostra que não existem variações substanciais de caso para caso. No entanto, podem ser retiradas conclusões interessantes nas poucas alterações verificadas que, embora já referidas anteriormente, importa reforçar. No anexo 5 constata-se que, independentemente da idade ou do grau académico, há uma tendência a não ler a políticas de privacidade dos serviços e redes sociais em que possuem conta, sendo que, no máximo, há um número não tão reduzido de pessoas que realizou uma leitura reduzida, com o público mais jovem a apresentar uma maior discrepância entre as opções respondidas. Os mais jovens são, sem dúvida, aqueles que menos cuidado têm quando navegam na internet, talvez por terem crescido numa época com uma cultura digital muito grande, fazendo com que questionem pouco aquilo que se encontra à sua disposição. Neste ponto a falha é também da sociedade no geral, sobretudo daqueles cujo papel é manterem o povo informado e educado.

No início deste capítulo procurámos encontrar resposta para três perguntas: existe um sentimento de alarme na generalidade das pessoas na matéria da privacidade? Essas mesmas pessoas encontram-se conscientes da falta de privacidade que, muito provavelmente, são vítimas? E por último, essa falta de privacidade é motivo de incómodo para elas? Analisando as respostas dadas pelos inquiridos quando são questionados se sentem que os seus dados se encontram seguros na organização onde se encontram profissionalmente empregados, se é motivo de preocupação para os mesmos a possibilidade das organizações possuírem diferentes versões das informações nas suas bases de dados e em que circunstâncias dariam acesso aos seus dados pessoais presentes nos seus aparelhos eletrónicos, conseguimos ter uma boa perceção se para os cidadãos é motivo de alarme a situação atual do modo como se lida com a privacidade. Na primeira questão o que se verifica é que apenas 29% sentem que os seus dados pessoais não se encontram seguros na organização onde desenvolvem atividade, sendo que praticamente 40% creem que os seus dados estão seguros. No entanto, quando analisamos as respostas obtidas para a segunda pergunta, o cenário é bastante distinto, pois muitos dos inquiridos dizem sentir-se preocupados com a possibilidade de as organizações terem versões diferentes, e consequentemente erradas, nas suas bases de dados, mais concretamente 72,9% dos mesmos. No âmbito da privacidade, as respostas nesta questão levam a crer uma realidade diferente sentida por parte das pessoas, em comparação às dadas na questão analisada anteriormente, sendo que, neste caso, há uma expressão consideravelmente superior. Por último, a terceira pergunta utilizada para tentar perceber se há um sentimento de alarme sentido pelas pessoas volta novamente a ter respostas bastante interessantes. Neste caso, e recorrendo novamente ao anexo 2, constatamos que a maioria respondeu que só facultaria acesso aos seus dados pessoais de livre vontade em situações muito extremas, provando que, no geral, existe uma elevada preocupação com a proteção das suas informações privadas. Concluindo, neste caso, as respostas providenciadas pelos inquiridos nestas três questões levam a crer que existe um sentimento de alarme sentido por estes, sobretudo causado por empresas que não aquelas onde praticam a sua atividade profissional e também pelo Estado, levando a crer que existe uma desconfiança sentida pelos cidadãos em relação a esses órgãos.

De modo a obter resposta à segunda conclusão que procuramos retirar deste estudo de caso, analisaremos as questões “Dos serviços e redes sociais em que possui conta, em quantos leu as políticas de privacidade ou termos de aceitação?” e “Sabe que a sua informação pessoal tem valor monetário para as empresas, e que estas geram milhões de euros ao vender as informações dos seus utilizadores?”. Na primeira, apenas 9 pessoas entre as 362 (2,5%) que responderam ao questionário é que dizem ter efetuado uma leitura detalhada de todas as políticas de privacidade, enquanto que mais de metade nunca leram nem uma dessas. A não leitura dos termos e das políticas de privacidade leva a que, naturalmente, não exista um conhecimento das práticas executadas pelas organizações relativamente ao modo como realizam o tratamento dos dados pessoais dos seus clientes. Por exemplo, a google tem nas suas políticas a opção automaticamente ativa de “permitir que a Google e os seus parceiros tecnológicos recolham dados e utilizem *cookies* para personalização e medição de anúncios”, dando consentimento nesta opção abrimos os nossos dados a centenas de serviços parceiros do Google. Na segunda questão, as respostas são indicativas de uma situação semelhante à constatada anteriormente, cerca de 85% das pessoas afirmam saber que as empresas utilizam a informação pessoal dos seus clientes como um recurso monetário, sendo que a grande maioria dessas admite que não sabem o que podem fazer para que a situação seja alterada, mostrando novamente que não se encontram suficientemente informadas relativamente ao modo como se processa o tratamento de dados pessoais a nível empresarial. Nesta situação, cerca de 16% afirmam não saber que a sua informação era valiosa para as empresas. Como podemos ver, com recurso ao anexo 6, as respostas foram relativamente semelhantes entre as diferentes segmentações utilizadas, no entanto, consegue-se constatar que os inquiridos mais jovens têm uma percentagem consideravelmente superior na opção “não sabia” do que os restantes e uma percentagem relativamente menor na opção “sei e importo-me e vou tomar medidas para limitar esse uso da minha informação pessoal”, comprovando novamente que os mais jovens são, por norma, aqueles que menos conhecimento têm de como funciona o mundo digital e, porém, são os que mais tempo passam no ciberespaço. Dadas as respostas a estas questões, é percetível que uma grande parte dos inquiridos (e provavelmente grande parte da população) se encontra mal informada relativamente à falta de privacidade de que diariamente são vítimas. A responsabilidade, para além delas, é também das empresas que por vezes não são transparentes o suficiente com os seus clientes. A Sapo, por exemplo, tem nas suas políticas de privacidade o seguinte

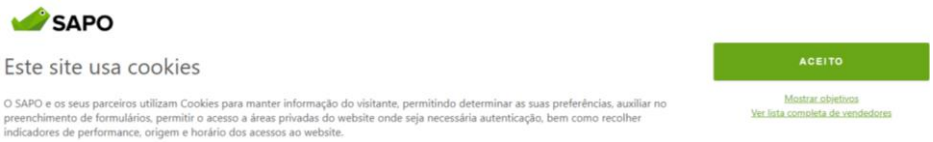


Figura 1 – Política de *cookies* da Sapo

e quando se aceita essas *cookies* não estamos apenas a influenciar o modo como interagimos com o *site* em questão, estamos igualmente a

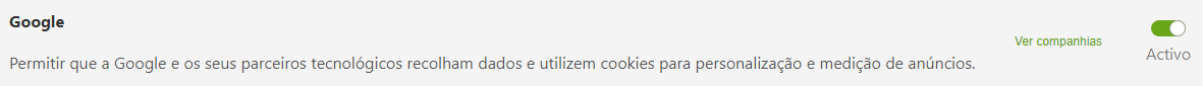


Figura 2 – Permissão de recolha de dados e *cookies* (Google)

que, por sua vez, quando carregamos na opção “ver companhias”, temos novos parceiros tecnológicos (desta vez da Google) que utilizam os dados e *cookies* para determinados fins, como se pode ver na seguinte imagem:

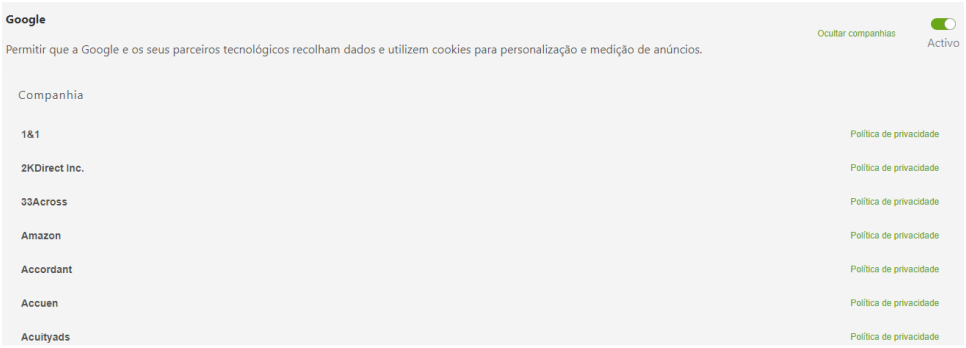


Figura 3 – Permissões para a Google e os seus parceiros tecnológicos

Como se pode constatar, quando se aceita as *cookies* de um determinado *site* não estamos apenas a concordar com as políticas desse, mas sim de uma lista enorme de parceiros que por sua vez têm as suas próprias políticas.

A falta de privacidade é de facto motivo de incómodo para as pessoas? Com vista a esclarecermos a última questão a que nos propusemos com a realização deste estudo de caso, importa analisar as respostas obtidas para as perguntas “Importa-se quando um site divulga os seus padrões de compra a terceiros?”, “Fica incomodado quando as empresas ou instituições lhe pedem informações pessoais?”, “Quando a situação em cima referida acontece, prefere não usufruir das possíveis vantagens adjacentes do que fornecer essas mesmas informações pessoais?”, “Sente, na sua vida pessoal, que os seus direitos de personalidade (direito à vida, nome, honra, privacidade, etc.) estão a ser colocados em risco hoje em dia, dada a constante vigilância em que estamos a ser sujeitos?” e “Estaria interessado(a) em frequentar um curso gratuito online sobre a proteção de dados e a segurança de informação?”. É por demais evidente que, e recorrendo novamente ao anexo 3, há um sentimento de incómodo pela grande maioria das pessoas, por os seus padrões de compra serem divulgados por *sites* a terceiros. Respondendo à segunda questão, no mesmo sentido, e talvez por força de acontecer essa partilha de informações, mais uma vez a grande maioria dos inquiridos não gostam quando as suas informações pessoais são requisitadas por empresas ou instituições. Confirmando que a maior parte das pessoas se mostra incomodada com essas práticas efetuadas pelas empresas, são as respostas obtidas na pergunta seguinte, em que apenas 27% responderam que preferem usufruir das possíveis vantagens que estas lhes podem proporcionar, apesar de terem de fornecer as suas informações pessoais. Por conseguinte, não é surpresa quando constatamos que a maior parte dos inquiridos sentem que os seus direitos de personalidade estão a ser violados, sendo a privacidade o principal afetado. Dadas estas respostas, seria expectável que, na questão seguinte,

se verificasse uma predisposição maior para frequentar um curso gratuito online sobre a proteção de dados e a segurança de informação, mas isso não foi o que se verificou. Apenas 37,3% é que se mostraram interessados em realizar o respetivo curso. Com isto, pode-se concluir que, no geral, a maior parte das pessoas se sente de facto incomodada com a falta de privacidade a que somos sujeitos atualmente, porém, com as respostas fornecidas na última questão, percebe-se que isso não é motivação suficiente para muitas dessas pessoas atenderem um curso onde, possivelmente, iriam esclarecer grande parte das dúvidas que teriam e o modo como poderiam alterar determinadas situações desconfortáveis a nível da privacidade.

Os resultados apresentados neste estudo de caso sugerem que os utilizadores da Internet em Portugal devem realizar uma introspeção relativamente à importância da preservação da privacidade das suas informações pessoais e a reavaliação do seu comportamento (principalmente online) e o modo como expõem as suas informações pessoais no dia-a-dia online. Convém reforçar que devem ser levadas a cabo ações de capacitação e sensibilização, especialmente o público jovem. Não só isso como tem de surgir um investimento forte ao nível do sistema educativo formal, introduzindo o tópico da segurança e privacidade no currículo de pelo menos uma área disciplinar, o que iria significar, obrigatoriamente, formar devidamente os docentes.

Conclusão

Vivemos numa altura de mudança constante, a uma velocidade vertiginosa, o que provoca muitas incertezas, e uma multiplicidade de opiniões sobre os mais variadíssimos temas, provocando pontos de vista suscetíveis de chocar uns com os outros. No caso concreto que originou este trabalho, é o cidadão comum que tende a discordar dos comportamentos tomados tanto por empresas como pelos governos, que têm influência direta no seu dia-a-dia e na sua interação com a sociedade. Foi por isso que neste trabalho procurámos perceber se de facto existe uma invasão da privacidade dos indivíduos por parte das empresas, das instituições a quem confiamos os nossos dados, e uma consequente violação dos direitos de personalidade dos mesmos, ou se todas estas suspeitas não são mais que as chamadas *fake news*[130] que tanto estão na voga nos dias de hoje.

Consideramos que começam a existir indícios de uma sociedade dividida e fragmentada, onde há cada vez menos confiança por parte dos cidadãos nas organizações e sobretudo no governo. Será que à medida que a generalidade das pessoas começar a ganhar consciência dos métodos de vigilância praticados atualmente essa fragmentação tenderá a aumentar ainda mais? A opinião de muitos é que não pode continuar, muito menos continuar a aumentar no registo que se tem verificado, sendo necessário existir, necessariamente, uma reeducação da sociedade neste aspeto. O uso excessivo e desinformado das redes sociais é uma das principais práticas que ninguém se apercebe (ou fazem de conta que não se apercebem) que tem um elevado peso na privacidade que temos ou deixamos de ter. Juntamente com este uso, ou será que já podemos considerar abuso, a outra prática que leva a maioria das pessoas a serem vítimas de invasão de privacidade é a aceitação "cega" das políticas de privacidade dos serviços que usam, onde constam quais os dados que irão ser coletados bem como o que será feito com esses dados. Esse é, talvez, o maior perigo, pois já é do senso comum que é comportamento usual dos cidadãos não lerem essas políticas, originando que algumas empresas solicitem uma extensão de dados que habitualmente não concordaríamos em ceder, aceitando-as por omissão.

Num trabalho onde procurámos averiguar se os direitos da personalidade estão a ser colocados em risco, quer pela pressão que estamos sujeitos para ceder esses dados, quer pela constante vigilância a que somos sujeitos, fez sentido iniciarmos a exploração do tema, precisamente sobre os direitos da personalidade, sendo que o enfoque principal incidiu na legislação existente que "garante" ao cidadão essa proteção. No primeiro capítulo evidenciámos a importância que os direitos de personalidade têm nos normativos essenciais e como se impactam no nosso quotidiano e que merecem ser respeitados por todos, sejam pessoas individuais ou coletivas. No entanto, foi a partir do final da 2ª Guerra Mundial que a defesa dos direitos em questão se começaram a manifestar com maior vigor na sociedade até que, atualmente, inicia-se um novo capítulo na luta pelo respeito dos

[130] As chamadas "notícias falsas", termo que começou a ser mais usado após as eleições Americanas de 2016 que elegeram o atual presidente Americano Donald Trump.

desse direitos como direitos essenciais, neste caso, a luta contra as ameaças à privacidade a que todos somos sujeitos.

Como é por demais evidente e nessa medida não deixámos de o referir ao longo deste trabalho, assistimos hoje a um desenvolvimento tecnológico que nos permite entre muitas outras coisas mantermo-nos conectados constantemente, a chamada sociedade de informação, que origina muitos debates sobre o que realmente significa. "Para Webster (1995, apud. Coutinho, 2003) é possível dividir o debate sobre a "sociedade da informação" em duas grandes correntes: a primeira, constituída pelos teóricos defensores do pós-industrialismo (Daniel Bell), pós-modernismo (Jean Baudrillard, Mark Poster), especialização flexível (Michel Piore) e do modo informacional de desenvolvimento (Manuel Castells), que acreditam que este novo modelo marca o surgimento de uma nova ordem social que tem como característica básica a circulação e modificação das informações de uma forma nunca antes imaginada, significando uma total rutura com o passado; e a segunda, que compreende os neomarxistas (Herbert Schiller), os defensores da teoria da regulação e da acumulação flexível (Aglietta, David Harvey), do estado nacional e a violência (Anthony Giddens) e da esfera pública (Habermas) que têm em comum o facto de, embora reconhecendo que, de facto, a conceção, manipulação e utilização da informação nas diversas atividades e esferas humanas atingiram patamares incomparáveis, acreditam que a nova ordem social representa um processo contínuo e evolutivo da sociedade."[131] Seja qual for o conceito com que nos identificamos mais, não restam dúvidas que a informação é a base desta nova era e por informação, neste caso, entenda-se o conjunto dos nossos dados, os que voluntariamente partilhamos e os de cariz mais pessoal.

A pressão da sociedade de informação, de onde é quase impossível fugirmos, impede-nos muitas vezes de sermos capazes de definir limites àquilo que queremos manter privado e, como sucede à medida que avançamos enquanto civilização, surgem novas regulamentações precisamente com o intuito de proteger os cidadãos. Como vimos, temos atualmente, para além da Constituição e do Código Civil, outras diretivas e regulamentos onde este direito se encontra protegido com especial relevância para o Regulamento Geral de Proteção de Dados que procura, justamente, impor um controlo relativamente ao tratamento de dados pessoais por parte das empresas, proporcionando deste modo aos clientes das mesmas a garantia de que as suas informações pessoais estão seguras. Porém, e agora referindo em particular o cenário português, existe ainda uma necessidade enorme de reeducação não só dos portadores de informações pessoais (que somos todos nós), mas também de quem lida com as mesmas em todos os setores, pois apesar dos avanços verificados, estamos ainda atrasados relativamente a alguns países.

Sendo o principal direito de personalidade abordado nesta dissertação a privacidade, era necessário discutir esse direito com uma abordagem mais profunda. Vimos, pois, que para além dos documentos mencionados no parágrafo anterior, existem a montante, outros dois instrumentos que garantem a proteção da privacidade enquanto direito de personalidade, são eles a Declaração

[131] Coutinho, C. P., & Lisbôa, E. S. (2011). *Sociedade da informação, do conhecimento e da aprendizagem: desafios para educação no século XXI*. Revista de Educação, 18(1), 5-22, p.6.

Universal dos Direitos Humanos (DUDH) e o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP) onde estão consignadas as principais questões relacionadas com o tema, bem como as garantias oferecidas por estes documentos. Estes direitos são muitas vezes obliterados no dia-a-dia por decisões das empresas que essencialmente se prendem com as vantagens que podem advir de possuírem o maior acervo de dados possível.

Cada vez existem mais regulamentos que "obrigam" as empresas a realizar corretamente o tratamento de dados pessoais dos seus clientes, onde está incluída a obrigatoriedade de informar aquilo que será feito com as suas informações. Porém, ao mesmo tempo que não existem ainda as condições para a fiscalização desejada por parte dos reguladores, que têm a tarefa de verificar se as empresas estão de facto a realizar as boas práticas que são obrigadas a ter, existe no mesmo sentido uma inexperiência profissional por parte daqueles que diariamente se dedicam ao tratamento de dados pessoais (resultado de uma falta de preparação pela generalidade das empresas em Portugal e da falta de Encarregados de Proteção de Dados[132] profissionalmente preparados para assumirem esse mesmo cargo dentro de uma organização).

Com vista a um enquadramento mais abrangente desta análise fez sentido observar a realidade verificada noutros países Europeus, para percebermos também em que ponto de situação nos encontramos comparativamente a esses países. Podemos concluir que as nações analisadas (Alemanha, Reino Unido e França) encontram-se relativamente mais avançadas do que Portugal, sendo a prova principal disso a preparação que existiu nestes países aquando da entrada em vigor do Regulamento Geral de Proteção de Dados em que já possuíam leis nacionais de proteção de dados adequadamente organizadas e prontas para serem implementadas na mesma data em que o RGPD se tornou ativo, e a falta dessa mesma preparação em Portugal em que a lei de proteção de dados pessoais (58/2019), a lei de execução do RGPD só foi aplicada dia 14 de junho de 2019 (mais de um ano depois do regulamento). Os casos de países como a Inglaterra ou Alemanha são exemplos para os outros países, no entanto, mesmo nesses existe um longo caminho a percorrer até se alcançar uma relação ideal com os dados que, naturalmente, é sempre subjetiva, pois cada pessoa tem a sua interpretação daquilo que é privado ou não e o que já pode ser considerado invasão da mesma. Ao nível de um tópico preocupante hoje em dia vimos que as leis nacionais de aplicação do Regulamento Geral de Proteção de Dados em Portugal e na Alemanha já contêm restrições à videovigilância, o que é um presságio muito bom para o que pode vir a acontecer no campo da defesa dos direitos de personalidade. Ainda assim, a mudança tem de acontecer e para países como Portugal essa mudança não pode apenas ser feita exclusivamente a pensar neste tema, pois será mais difícil de se alcançar um resultado desejável, é sim recomendável que se leve a cabo uma mudança de mentalidade no modo como se lidam com os compromissos assumidos e os interesses instituídos. Só após estas

[132] Um DPO (Data Protection Officer) "tem o poder de garantir que a organização esteja em conformidade com todos os aspetos do novo regime de proteção de dados. As organizações devem agora nomear e designar um DPO para a organização. (...) o novo DPO será muito ativo em transmitir a mensagem e a exigência do novo regime de proteção de dados a toda a organização - incluindo os benefícios." Lambert, P. (2016). *The Data Protection Officer: Profession, Rules, and Role*. CRC Press, p.3.

mudanças é que os cidadãos também conseguem começar a ter mais confiança nas questões relacionadas com os dados pessoais e a privacidade. A título de exemplo, refira-se a recente necessidade de intervenção da Comissão Nacional de Proteção de Dados, desaplicando "algumas normas da Lei n.º 58/2019, de 8 de agosto, por estas contradizerem manifestamente o estatuído no regulamento europeu de proteção de dados, o que viola o princípio do primado da União, bem como prejudica seriamente o funcionamento do mecanismo de coerência que tem como objetivo uma aplicação uniforme das regras de proteção de dados em todo o espaço da União Europeia."[133] Se por um lado esta ação pode ser percecionada como uma saudável manifestação da independência de poderes, por outro lado é espelho da falta de compromisso dos poderes públicos para enfrentar um problema para o qual o próprio Estado não se preparou convenientemente.

Transversal à maioria dos países é o impacto da internet e o modo como nos relacionamos com a mesma. Nos chamados países desenvolvidos já se encontra socialmente assumida uma cultura tecnológica em que quem não se encontra digitalmente "conectado" é um *outsider*, originando cada vez mais frequentemente situações em que os gadgets tecnológicos são brinquedos para crianças ou até mesmo bebés, fazendo com que desde cedo comecem a olhar para estes como recompensas, afetando deste modo a interação futura que vão tendo com esses dispositivos cujos ecrãs exercem um fascínio incontornável. Se pode parecer previsível um adulto não ler as políticas de privacidade de um *site* ou *app* quando navega online, uma criança certamente que não o vai fazer, podendo originar consequências reais relacionadas com a (falta de) privacidade sem se ter consequência do ocorrido. No entanto não queremos, nem podemos afirmar que a internet de hoje em dia seja um território selvagem e sem lei. Na verdade, existem algumas leis que regulam a utilização da internet e que estabelecem princípios e garantias, visando tornar a internet um lugar mais seguro para quem nele se encontra inserido. Neste esforço de regulação, a situação brasileira foi interessante de se analisar com especial destaque para o Marco Civil da Internet[134] que procura precisamente disciplinar o comportamento dos indivíduos no mundo virtual, regulando o uso da Internet no Brasil por meio de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado. No mesmo sentido, a Diretiva relativa à Privacidade e às Comunicações Eletrónicas, da União Europeia[135], assegura a proteção dos direitos e liberdades fundamentais, estabelecendo regras para ser assegurada a segurança respeitante ao tratamento de dados pessoais, à notificação da violação de dados pessoais e à confidencialidade das comunicações, não deixando de garantir a livre circulação de dados, equipamentos e serviços de comunicações eletrónicas na União. Todas estas questões são atualmente de extrema relevância, e normas como estas procuram

[133] CNPD, (23.9.2019), Comunicado de Imprensa, Deliberação sobre a desaplicação de normas da Lei n.º 58/2019, de 8 de agosto, Lei nacional de execução do RGPD.
[134] Planalto.gov.br. (2018). LEI Nº 12.965, DE 23 DE ABRIL DE 2014. [online] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm [Acedido a 5 de setembro de 2019].
[135] Eur-lex.europa.eu. (2002). DIRECTIVA 2002/58/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 12 de julho de 2002 relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas). [online] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT [Acedido a 7 de outubro de 2019].

precisamente tornar a tarefa de assegurar a proteção dos dados mais facilitada para todos os intervenientes. Como é percetível já são muitas as tentativas de alterar o paradigma em que hoje nos encontramos através da atualização de leis, de regulamentos, entre outros, mas a passividade dos cidadãos relativamente a este tema é de salientar, podendo de certa forma ser comparável ao caso das alterações climáticas, isto é, é do conhecimento geral que acontece e quem tem noção disso sente-se incomodado com a situação, no entanto, não existe um real esforço individual para alterar a situação. Com isto, entendemos que seria importante a realização de mais estudos e análises profundas aos contextos de abuso em relação à privacidade por entidades de topo, divulgando-os, de forma a que tenham um efeito didático sobre a sociedade, evidenciando a importância da alteração do comportamento dos indivíduos.

Focámos neste trabalho as consequências da utilização abusiva dos nossos dados devido aos nossos comportamentos mais complacentes em relação às autorizações que damos à sua utilização, mas não podemos esquecer a outra dimensão, certamente com mais graves consequências, a utilização dos nossos dados duma forma ilegal. São cada vez mais comuns os casos de ataques cibernéticos por diversas razões, pelo grau de facilidade de execução dos mesmos comparativamente com ataques presenciais, sendo que a segunda razão prende-se exatamente com isso, o facto de não termos de nos deslocar de uma secretária para executarmos o ataque e por último, por ser mais complicado a nossa identidade ser descoberta quando estamos a praticar a ação ilegal face a, supostamente, e na maioria dos casos, por cidadãos incapazes de fazer face ao ocorrido. Do mesmo modo que deve existir uma tentativa de informar e educar as pessoas para os riscos que a falta de privacidade proporciona, deve no mesmo sentido existir um esforço semelhante para que os cidadãos estejam cientes dos perigos que a internet acarreta e como fazer para nos tentarmos salvaguardar de possíveis ataques cibernéticos. Nesta linha, na ótica dos prestadores de serviços na internet, existem outras ferramentas que são utilizadas diariamente que podem à primeira vista ser inofensivas mas que, aprofundada a questão, se podem tornar em mais instrumentos capazes de nos ferirem a privacidade, como é o caso dos *clickstreams*, dos *cookies* e até mesmo os metadados. Estes mecanismos de coleta de dados servem muitas vezes para vender essas mesmas informações a terceiros, podendo neste processo originar que pessoas mal-intencionadas consigam intercetar a partilha dos dados.

A videovigilância é um tema que tem um grande impacto quando se fala de privacidade e que começa atualmente a gerar algum debate e controvérsia, e com uma disseminação cada vez maior. Através da videovigilância conseguiu-se alcançar uma sociedade mais segura, sendo que esta tendência ganhou novos contornos a partir do momento em que começaram a surgir atentados a nível global. Naturalmente, o facto de sabermos que podemos estar constantemente sob vigilância faz com que não tenhamos determinados comportamentos incorretos, porém, essa segurança tem um custo: a privacidade. Estamos agora sob o efeito do *Panótico* moderno. O direito à imagem e à reserva da intimidade da vida privada das pessoas é salvaguardada por diversos documentos incluindo a Constituição, o Código Civil e o Código Penal, algo que causa conflito com a vigilância em massa pois é realmente complicado a existência desta sem que os direitos anteriormente referidos não sejam feridos. Neste caso, quem está encarregue de assegurar a segurança na sociedade (sejam entidades

públicas ou privadas) deve procurar garantir que os direitos mencionados são salvaguardados o máximo de vezes possível sem que isso implique efetivamente uma menor segurança. Devem, portanto, ser levados a cabo estudos que procurem o que pode ser feito para salvaguardar o destino dos dados recolhidos por esses sistemas, sem que se comprometa a segurança do modelo. No entanto, estes mecanismos de vigilância não se encontram apenas dispostos fisicamente aos olhos de todos nós, nos nossos aparelhos eletrónicos somos constantemente vítimas da necessidade sentida pelas empresas e pelos governos em controlarem todos os nossos movimentos, cada um pelas suas razões. Aqui, há mesmo um aproveitamento puro e duro do desconhecimento geral da população relativamente a estas práticas e à quantidade de dados pessoais que são armazenados diariamente resultado da constante conexão digital em que quase todos se encontram. Deve, então, existir um trabalho feito pelas entidades reguladoras de modo a controlarem ao máximo aquilo que é passível de ser considerado como invasão de privacidade e, simultaneamente, realizarem esforços com o objetivo de garantir o cumprimento das normas impostas pelas mesmas. Nesse sentido, aproveitamos para levantar uma questão que nos parece pertinente, porque é que os *sites* em vez de terem as políticas de privacidade do modo que têm atualmente, não invertem a situação? Isto é, em vez de as pessoas terem de desativar as preferências que os *sites* em questão permitem desativar, deveria ser ao contrário, cada pessoa deveria ter essas preferências desativas e, caso quisesse, ativava-as. Desta forma, mais uma vez, as entidades competentes devem, e neste caso têm, de garantir que a sociedade está realmente informada do peso das suas ações online e quais as consequências que as suas não ações têm relativamente à sua privacidade. Por último, os tribunais devem melhorar a sua interpretação da legislação em vigor de modo a conseguirem de uma forma mais objetiva, definir o que constitui realmente a privacidade online e quais os limites da mesma, de modo a que nos julgamentos relativos à invasão da privacidade ou dos dados pessoais, não haja margem de manobra para quem de facto cometa essas infrações aproveitando-se de lacunas ainda existentes nos livros de direito. Extremamente importante também é a necessidade de a capacidade de produção legislativa ser capaz de acompanhar o ritmo dos avanços tecnológicos.

Finalmente, com recurso a um estudo de caso, procurámos averiguar se os cidadãos sentem que os seus direitos de personalidade estão a ser violados, se tinham conhecimento nas matérias em questão e por último se é algo que os incomoda ao ponto de alterarem o seu estilo de vida com vista a alcançarem uma convivência com a sociedade ideal aos seus olhos. Como vimos nos resultados da amostra inquirida os cidadãos manifestam alguma preocupação, mas não demasiada intenção em agir proactivamente. De igual forma os dados do estudo de caso evidenciam pouco conhecimento dos direitos e dos meios disponíveis para fazer valer esses direitos.

Tal como já afirmamos anteriormente, entendemos que estes são sinais de uma crise de crescimento da consciência em relação à importância do tema da privacidade dos dados, que o caminho no sentido de um maior conhecimento que posteriormente permita a ação, está a ser percorrido, só que não a uma velocidade suficiente para acompanhar os riscos, os desafios. É um tema importante que pode ter consequências diretas no nosso modo de vida e que, no nosso entender, só através da educação poderá evoluir. Só com cidadãos educados, teremos cidadãos conscientes e

ativos na defesa dos seus direitos, que se materializam nos direitos de toda a sociedade, pelo que, como já foi mencionado, a nossa proposta é que a intervenção a este nível se faça através de ações de capacitação e sensibilização, sobretudo ao nível do público mais jovem no sistema educativo formal, com a introdução do tema da segurança e privacidade no currículo de algumas áreas disciplinares. Não só isso, como também se devem promover ações de sensibilização recorrendo a quem está mais próximo do público alvo e seja relevante, como *youtubers* ou artistas. Estas ações devem ser promovidas pelo Estado, mas alavancadas nas empresas que mais estão nesta área, ou seja, que estas financiem as ações, sob condição de poderem ser limitadas nas suas atividades, para que, no futuro, não corramos o risco de chegar um ponto praticamente irreversível em que já todos estamos habituados a fazer uso da tecnologia sem nos questionarmos dos riscos inerentes à utilização dos mesmos. Temos consciência que é necessária coragem política para estas medidas, mas o desígnio assim o exige.

Como consideramos de extrema importância a alteração do paradigma atual no tratamento de dados pessoais, para além das sugestões deixadas resolvemos procurar uma alternativa oferecida por nós, pois achamos que mais do que apontar as falhas e esperar que alguém as corrija, é importante tomar uma ação. Então, resolvemos criar uma página na rede social Instagram onde esclarecemos questões que achamos relevantes clarificar de modo a manter o público mais e melhor informado dos seus direitos e deveres enquanto consumidores de serviços online. Esperamos que, com o (desejado) crescimento e notoriedade da página possamos elevar este tipo de ação mais além, com o objetivo de, num futuro breve, organizar ações de sensibilização sobretudo em escolas. Acreditamos que esta ferramenta possa alterar o modo como os jovens olham para a tecnologia, estimulando assim a importância de, não só ser um consumidor atento, mas também de não ser um dependente da tecnologia.

Referências Bibliográficas

Abrantes, José João (2014). *Direitos Fundamentais da Pessoa Humana no Trabalho, em especial a reserva da intimidade da vida privada*, Almedina.

Agostini, Leonardo Cesar de. *A intimidade e a vida privada como expressões da liberdade humana*. Porto Alegre: Núria Fabris, 2011.

Albrecht, H. J. (2009). *Vigilância das Telecomunicações: Análise teórica e empírica da sua implementação e efeitos. In Que futuro para o direito processual penal?* Simpósio em homenagem a Jorge de Figueiredo Días, por ocasião dos 20 anos do código de processo penal português. Coimbra Editora.

Beltrão, S. R. (2005). *Direitos da Personalidade – De Acordo com o Novo Código Civil*. São Paulo (SP): Atlas.

CABRAL, M. M. (2012). A colisão entre os direitos de personalidade e o direito de informação. In: Fruet, G.; Miranda, J.; Rodrigues Junior, O. (Org.). Direitos da personalidade. São Paulo: Atlas.

Cne.pt. (1966). *Pacto Internacional sobre os Direitos Civis e Políticos*. [online] Disponível em: http://www.cne.pt/sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf [Acedido a 21 de janeiro de 2019].

Código civil Português. (1970). Coimbra: Almedina.

Coutinho, C. P., & Lisbôa, E. S. (2011). *Sociedade da informação, do conhecimento e da aprendizagem: desafios para educação no século XXI*. Revista de Educação, 18(1), 5-22.

Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G., & Weippl, E. (2019). Measuring *Cookies* and Web Privacy in a Post-GDPR World. In International Conference on Passive and Active Network Measurement.

de Oliveira Ascensão, J. (2002). *A Reserva da Intimidade da Vida Privada e Familiar,* Vol. XLIII – n.º 1. Coimbra Editora.

de Souza, T. B., Catarino, M. E., & dos Santos, P. C. (2012). *Metadados: catalogando dados na Internet. Transinformação*, 9(2).

DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO - relativa aos direitos de autor no mercado único digital. (2016). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52016PC0593 [Acedido a 11 de março de 2019].

Doneda, D. (2012). *Reflexões sobre proteção de dados pessoais em redes sociais*. Revista da rede académica internacional de proteção de dados pessoais, 1.

Eltantawy, N. and Wiest, J. (2011). *Social Media in the Egyptian Revolution: Reconsidering Resource Mobilization Theory*. [online] Research Gate. Disponível em: https://www.researchgate.net/publication/285908894_Social_Media_in_the_Egyptian_Revolution_Reconsidering_Resource_Mobilization_Theory [Acedido a 11 de junho de 2019].

Eur-lex.europa.eu. (2016). *REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. [online] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679 [Acedido a 13 de novembro de 2018].

Fairfield, J. A. (2009). *Escape into the Panopticon: Virtual worlds and the surveillance society*. *Yale Law Journal Pocket Partigo*

Flumignan, W. (2018). *Responsabilidade civil dos provedores no Marco Civil da Internet* (Lei n. 12.965/14). Universidade de São Paulo.

Foucault, M. (1997). Resumo dos cursos do Collège de France: 1970-1982. Tradução de Andrea Daher. Rio de Janeiro: J. Zahar.

Fortin, M. F. (1999). *O Processo de Investigação: Da Conceção à Realização.* Loures, Lusociência – Edições Técnicas e Científicas, Lda.

Greenwald, G. (2014). Edward Snowden Sem esconderijo.

Gomes, C. M. & Moreira, V. (2014). *Compreender os Direitos Humanos, Manuel de Educação para os Direitos Humanos.* Coimbra Editora.

Gonçalves, M. (2007). *Código Penal Português*. Lisboa: Almedina.

Gouveia, Luís Manuel Borges (2004), *"Notas de contribuição para uma definição operacional".* Disponível em: http://www2.ufp.pt/~lmbg/reserva/lbg_socinformacao04.pdf [Acedido a 22 de maio de 2019].

Gouveia, J. B. (2013). *Direito Internacional da Segurança*. Leya.

Government Europa. (2018). *Information security and privacy protection aspects of CCTV systems*. Disponível em: https://www.governmenteuropa.eu/information-security-cctv-systems/85930/ [Acedido a 15 de maio de 2019].

Harkin, D., Molnar, A., & Vowles, E. (2019). The commodification of mobile phone surveillance: An analysis of the consumer spyware industry. Crime, Media, Culture.

Harper, E. (2018). *9 Simple Ways to Protect Your Privacy*. [online] Techlicious.com. Disponível em: https://www.techlicious.com/tip/simple-ways-to-protect-your-privacy/ [Acedido a 26 de junho de 2019].

Horst Dreier, in Grundgesetz-Kommentar (org. por Horst Dreier), Tübingen, 1996, anot. 5 ao artigo 2.º.

HUMANOS, D. U. D. D. (2015). Declaração Universal dos Direitos Humanos.

Joseph, S., & Castan, M. (2013). *The international covenant on civil and political rights: cases, materials, and commentary*. Oxford University Press.

Lagos, M., & Dammert, L. (2012). La seguridad ciudadana. El problema principal de América Latina. *Corporación Latinobarómetro*, *9*.

Lambert, P. (2016). *The Data Protection Officer: Profession, Rules, and Role*. CRC Press.

Law in France - DLA Piper Global Data Protection Laws of the World. (2018). Disponível em: https://www.dlapiperdataprotection.com/index.html?t=law&c=FR&c2= [Acedido a 29 de março de 2019].

Law in Germany - DLA Piper Global Data Protection Laws of the World. (2018). Disponível em: https://www.dlapiperdataprotection.com/index.html?t=law&c=DE&c2= [Acedido a 29 de março de 2019].

Law in United Kingdom - DLA Piper Global Data Protection Laws of the World. (2018). Disponível em: https://www.dlapiperdataprotection.com/index.html?t=law&c=GB&c2= [Acedido a 29 de março de 2019].

Lei nº 67/98. (1998). *DIÁRIO DA REPÚBLICA*, *I SÉRIE-A*.

Lind, D. (2015). *Everyone's heard of the Patriot Act. Here's what it actually does*. [online] Vox. Disponível em: https://www.vox.com/2015/6/2/8701499/patriot-act-explain [Acedido a 8 de julho 2019].

Lio, Vanesa. *The Urban Panopticon.*

Lurdes Dias Alves, *A videovigilância e a compreensão da privacidade.*

Machado, M. (2019). *Portugal aprova lei de proteção de dados um ano depois do RGPD – Observador*. Disponível em: https://observador.pt/2019/06/14/portugal-aprova-lei-de-protecao-de-dados-um-ano-depois-do-rgpd/ [Acedido a 27 de maio de 2019].

Machado, M. (2019). RGPD. *Um ano depois, os nossos dados já são privados?* – Observador. Disponível em: https://observador.pt/2019/05/25/rgpd-um-ano-depois-os-nossos-dados-ja-sao-privados/ [Acedido a 14 de junho de 2019].

MacMillan, D. (2018). *Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail.* Disponível em: https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442 [Acedido a 10 de julho de 2019].

Manfred Nowak. 2005. CCPR Commentary, artigo 17.º CCPR.

Martins, A. M. G. (2015). *A Carta dos Direitos Fundamentais da União Europeia e os direitos sociais*. Revista Direito Mackenzie, 3(2).

Matyszczyk, C. (2015). *Samsung's warning: Our Smart TVs record your living room chatter*. [online] CNET. Disponível em: https://www.cnet.com/news/samsungs-warning-our-smart-tvs-record-your-living-room-chatter/ [Acedido a 12 de agosto de 2019].

Mazouchi, A., Chokhawala, A., & Kusam, A. (2019). U.S. Patent Application Nº. 15/788,466.

Mazur, M. (2012). *Direitos da Personalidade – A dicotomia entre os direitos de personalidade e os direitos* fundamentais. São Paulo: Atlas.

McCahill, M. (2013). *The surveillance web*. Willan.

McMullan, T. (2015). *What does the panopticon mean in the age of digital surveillance?* [online] the Guardian. Disponível em: https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham [Acedido a 15 abril de 2019].

Milt, K. (2019). *PROTEÇÃO DOS DADOS PESSOAIS*. [online] Europarl.europa.eu. Disponível em: http://www.europarl.europa.eu/ftu/pdf/pt/FTU_4.2.8.pdf [Acedido a 12 de julho de 2019].

Miranda, J., Medeiros, R., & Ferreira, E. P. (2005). *Constituição portuguesa anotada*. Coimbra: Coimbra Editora.

Miranda, J., Rodrigues Junior, O., Fruet, G. (2012). *Direitos da Personalidade – Principais problemas dos direitos da personalidade e estado-da-arte da matéria no direito comparado*. São Paulo: Atlas.

Miranda, J. (2004). *Manual de direito constitucional.*

Moreira, A., & Moreira, T. (2004). *Código do trabalho*. Coimbra: Almedina.

Nunes, F. (2019). *Já houve quatro multas em Portugal por causa do RGPD*. Disponível em: https://eco.sapo.pt/2019/05/17/ja-houve-quatro-multas-em-portugal-por-causa-do-rgpd-uma-foi-ao-hospital-do-barreiro-e-tres-a-empresas-privadas/ [Acedido a 2 de junho de 2019].

O'Gorman, G. and McDonald, G. (n.d.). *Ransomware: A Growing Menace*. [online] Symantec.com. Disponível em: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf [Acedido a 14 de julho de 2019].

Orwell, G., (2012). 1984. Lisboa: Antígona.

Parent, W. A. (2017). *Privacy, morality, and the law*. In Privacy.

Parreira, R., & Caçador, F. (2019). *Direito de Autor: Artigos 11 e 13 (agora artigos 15 e 17) foram aprovados.* Disponível em: https://tek.sapo.pt/noticias/internet/artigos/artigos-11-e-13-agora-artigos-15-e-17-foram-aprovados [Acedido a 12 de abril de 2019].

Parreira, R., & Caçador, F. (2019). RGPD: *Um ano depois só há 4 multas. Videovigilância concentra principais queixas*. Disponível em: https://tek.sapo.pt/noticias/internet/artigos/rgpd-um-ano-depois-so-ha-4-multas-videovigilancia-concentra-principais-queixas [Acedido a 14 de maio de 2019].

Pinsonneault, A., & Kraemer, K. (1993). *Survey research methodology in management information systems: an assessment. Journal of management information systems*, 10(2), 75-105.Pinto, P. M. (2018). *Direitos de Personalidade e Direitos Fundamentais*. GESTLEGAL.

Pgdlisboa.pt. (1996). *Lei nº 24/96, de 31 de julho - LEI DE DEFESA DO CONSUMIDOR*. [online] Disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=726&tabela=leis [Acedido a 17 de abril de 2019].

Pontieri, A. (2019). *Marco civil da internet, neutralidade de rede e liberdade de expressão*. [online] Jus.com.br. Disponível em: https://jus.com.br/artigos/70495/marco-civil-da-internet-neutralidade-de-rede-e-liberdade-de-expressao [Acedido a 10 de maio de 2019].

Pordata.pt. (2019). *População residente média anual total e por grupo etário*. [online] Disponível em: https://www.pordata.pt/Portugal/Popula%c3%a7%c3%a3o+residente++m%c3%a9dia+anual+total+e+por+grupo+et%c3%a1rio-10 [Acedido a 23 de agosto de 2019].

Rogall, K. *A nova regulamentação da vigilância das telecomunicações na Alemanha,* em: *2º Congresso de Investigação Criminal*, ASFIC-PJ e IDPCC-FDUL.

Rouse, M. (2014). *What is third-party cookie? - Definition from WhatIs.com*. [online] WhatIs.com. Disponível em: https://whatis.techtarget.com/definition/third-party-cookie [Acedido a 8 de julho de 2019].

Rutkowska, J. (2006). Introducing stealth malware taxonomy. *COSEINC Advanced Malware Labs*, 1-9.

Sanlez, A. (2018). *Brittany Kaiser: "Multa à Google foi uma enorme conquista"*. [online] Dinheiro Vivo. Disponível em: https://www.dinheirovivo.pt/economia/a-multa-aplicada-a-google-foi-uma-enorme-conquista/ [Acedido a 8 de abril de 2019].

Schreiber, A. *Direitos da Personalidade*. São Paulo: Atlas, 2011; Reis, Clayton (Coord.). Responsabilidade civil em face da violação aos direitos da personalidade: uma pesquisa multidisciplinar. Curitiba, Juruá, 2011.

Schreiber A. (2013). *Direitos da Personalidade*. 2ª Edição Revista e Atualizada. São Paulo: Editora Atlas S.A.

Shute, J. (2015). *Can anyone escape Britain's surveillance state?* Disponível em: https://www.telegraph.co.uk/technology/news/11831533/Can-anyone-escape-Britains-surveillance-state.html [Acedido a 10 de março de 2019].

SILVA, V. R. B., LUCIANO, E. M., & WIEDENHÖFT, G. C. (2016). AMEAÇAS POTENCIAIS À PRIVACIDADE DAS ORGANIZAÇÕES CAUSADAS PELO COMPORTAMENTO INSEGURO DE USUÁRIOS: UMA ANÁLISE SEGUNDO O FAIR INFORMATION PRINCIPLES.

Sousa, R. V. A. C. D. (1995). *O direito geral de personalidade (Doctoral dissertation)*.

Supremecourt.gov. (2017). *SUPREME COURT OF THE UNITED STATES - CARPENTER v. UNITED STATES*. [online] Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf [Acedido a 12 de julho de 2019].

Taniguchi, D. (2009). U.S. Patent No. 7,587,486. Washington, DC: U.S. Patent and Trademark Office.

UN. (1948). *The United Nations and human rights*. New York.

U.S. Department of Justice (2019). *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*. White Paper.

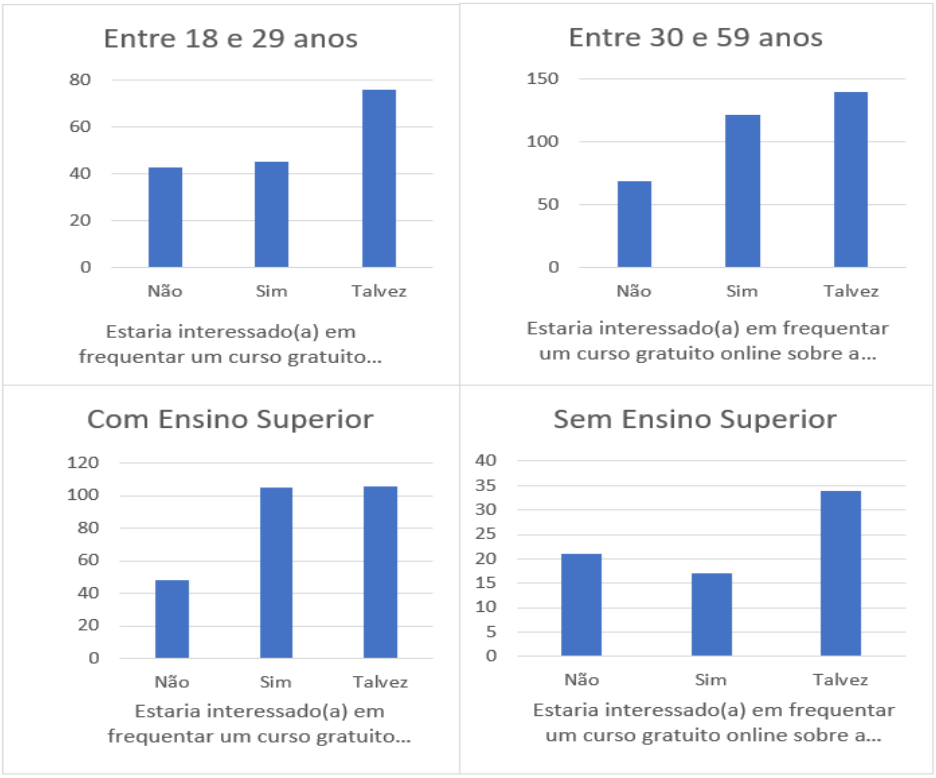
Wood, D. (2003). *Foucault and Panopticism revisited*. Surveillance & Society, 1(3).

Zerlang, J. (2017). *GDPR: a milestone in convergence for cyber-security and compliance*. Network Security, 2017(6).

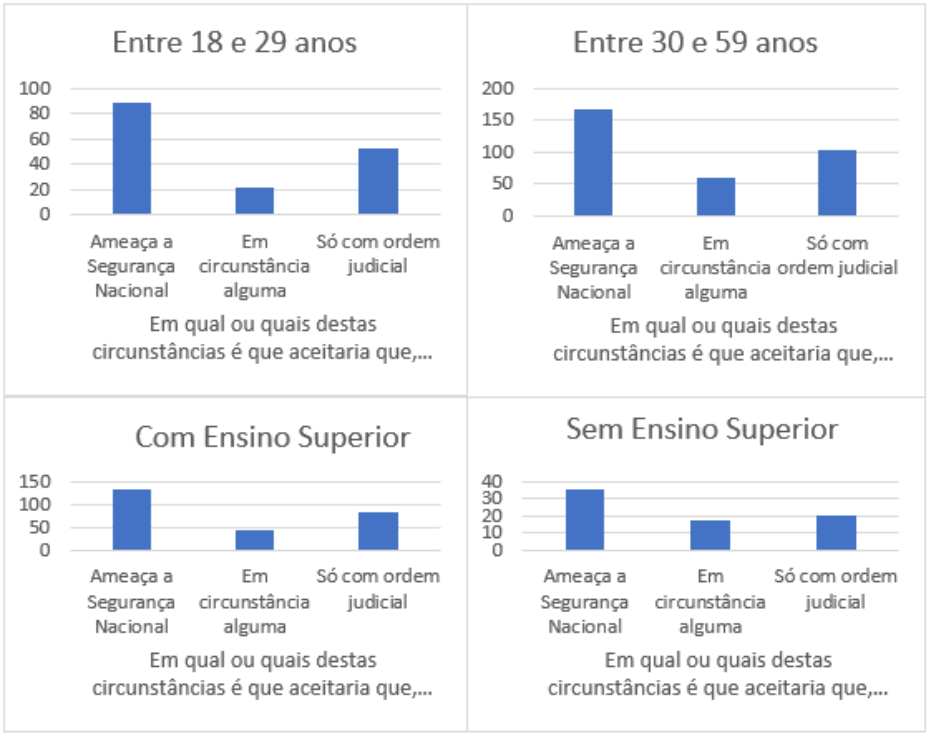
Zrinski, T. (2019). *EU GDPR vs. German Bundesdatenschutzgesetz (BDSG).* Disponível em: https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-vs-german-bundesdatenschutzgesetz-similarities-and-differences/ [Acedido a 14 de março de 2019].

Zuboff, S. (2017). Shoshana Zuboff: *No escape from the Panopticon.* Disponível em: https://sciencenode.org/feature/shoshana-zuboff,-part-one-no-escape-from-the-panopticon.php [Acedido a 2 de março de 2019].

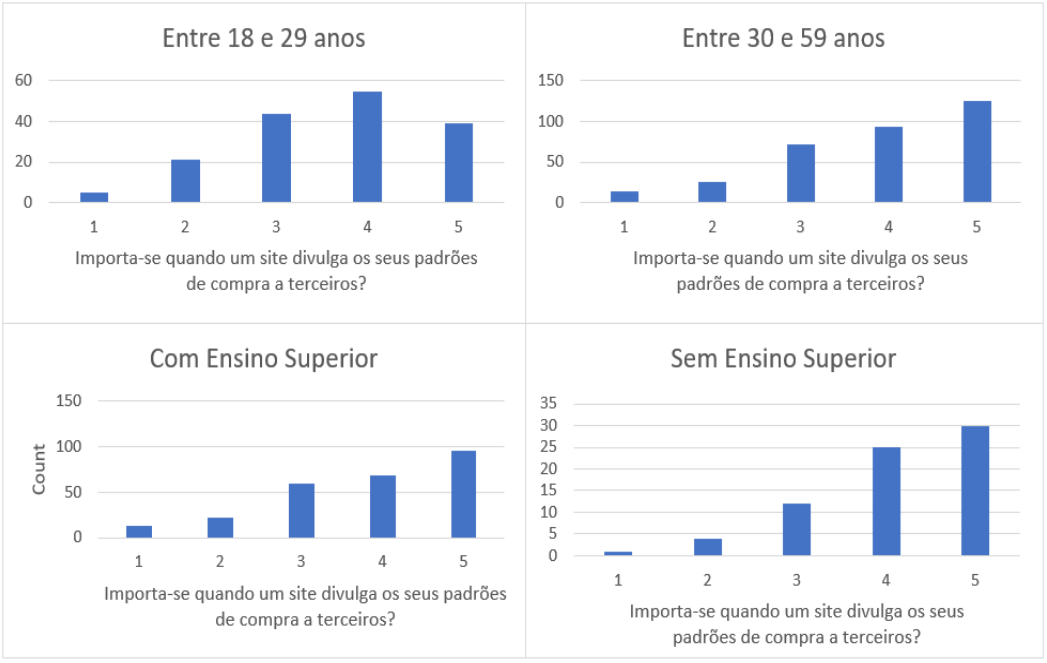
Anexos



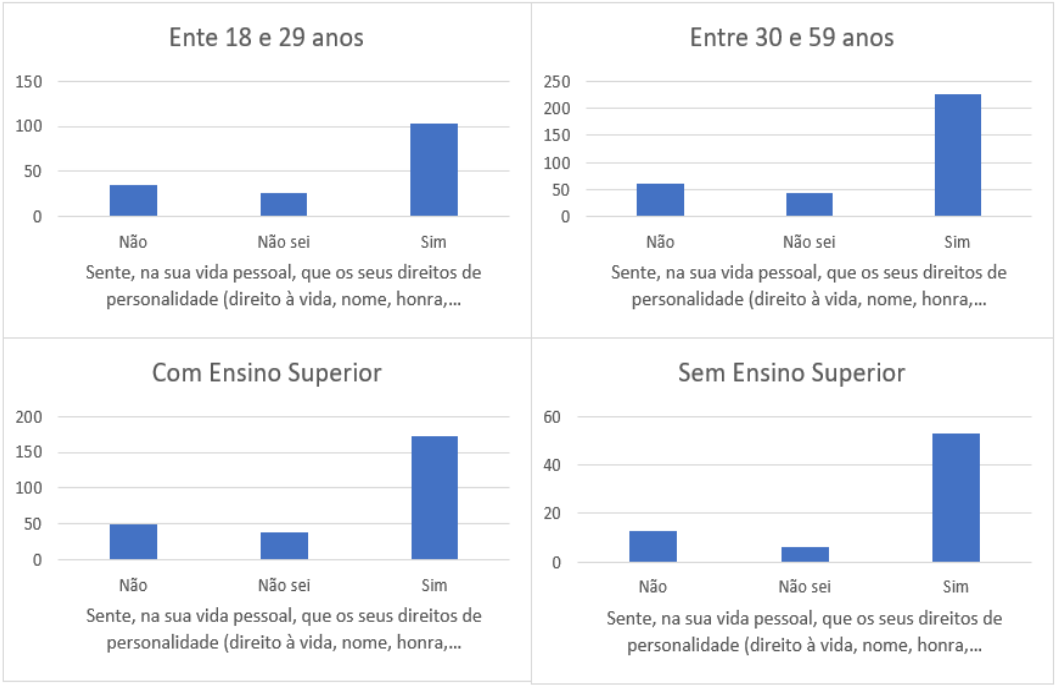
Anexo 1 – “Estaria interessado(a) em frequentar um curso gratuito online sobre a proteção de dados e a segurança de informação?”



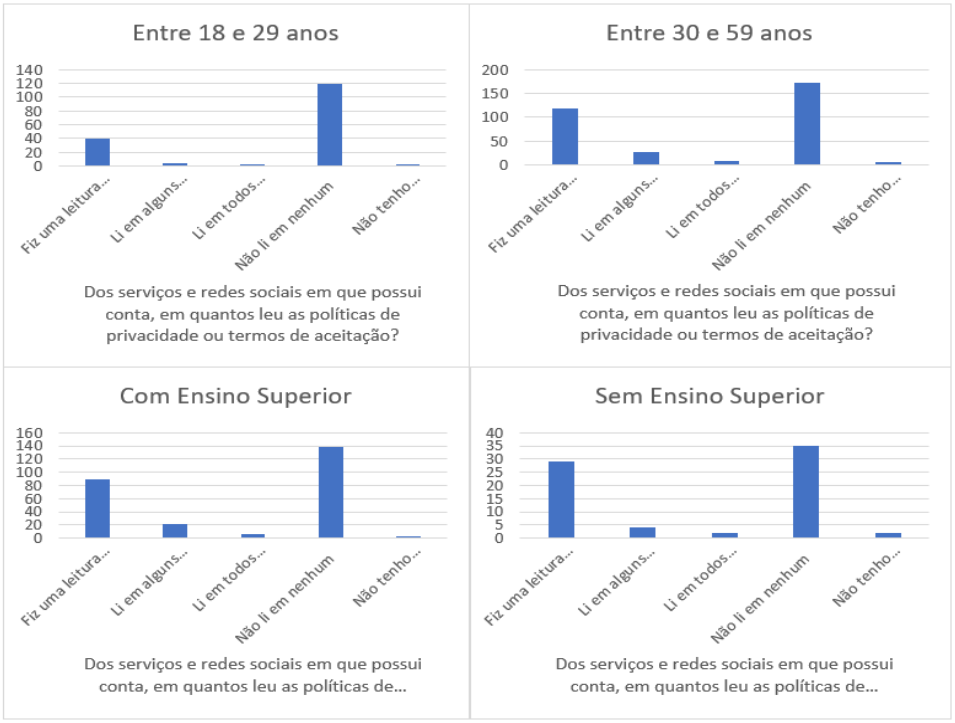
Anexo 2 – “Em qual ou quais destas circunstâncias é que aceitaria que, não só as empresas como também o Estado, tenham acesso aos seus dados privados presentes nos nossos aparelhos tecnológicos?”



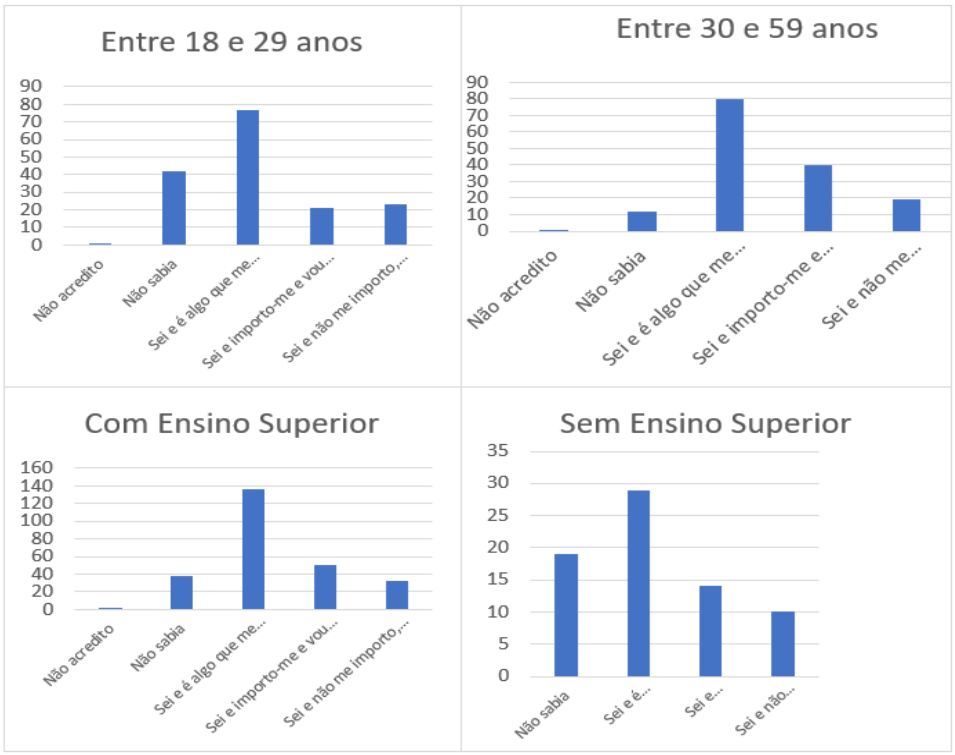
Anexo 3 – “Importa-se quando um site divulga os seus padrões de compra a terceiros?”



Anexo 4 – “Sente, na sua vida pessoal, que os seus direitos de personalidade (direito à vida, nome, honra, privacidade, etc.) estão a ser colocados em risco hoje em dia, dada a constante vigilância em que estamos a ser sujeitos?”



Anexo 5 – “Dos serviços e redes sociais em que possui conta, em quantos leu as políticas de privacidade ou termos de aceitação?”



Anexo 6 – “Sabe que a sua informação pessoal tem valor monetário para as empresas, e que estas geram milhões de euros ao vender as informações dos seus utilizadores?”