# DADOS PESSOAIS: PROTEÇÃO DOS DADOS PESSOAIS NAS COMUNICAÇÕES ELETRÓNICAS.[1]

**Katy Sony Monteiro Fernandes**[2]

*"O Progresso técnico é ao mesmo tempo*
*fonte de liberdade e de servidão".*
**J.A. Sacadura Garcia Marques**

**Sumário**

Portugal assumiu-se muito cedo como pioneiro em matéria de proteção jurídico (de base constitucional) de dados pessoais. O legislador constituinte tomou consciência da importância que a temática dos dados pessoais teria na sociedade ao prever a sua tutela, reservando-lhe um espaço na lei Magna, o artigo 35.º, sob a epígrafe, utilização da Informática. Volvidos uma década e meia foi possível densificar os preceitos ali consagrados, permitindo os ter aplicabilidade prática. A primeira lei de proteção de dados pessoais (Lei de Proteção de Dados Pessoais - LPDP), foi publicada em 29 de abril de 1991 (Lei n.º 10/91), formalmente, pois o mesmo só veio a ser publicado no Diário da República n.º 191/94, I-A Série, em 19 de agosto de 1994, através da Resolução da Assembleia da República n.º 53/94. A LPDP esteve em vigor cerca de sete anos e veio a ser revogada pela Lei n.º 67/98, de 26 de outubro, por força da transposição da Diretiva comunitária ( 95/46/CE de 24 de outubro de 1995).

Seguindo as pegadas do constituinte Português a *norma normarum* de Cabo Verde, previu expressamente a proteção dos dados pessoas no artigo 44. ° n.º 3 e 45 da Constituição da República (CRCV). Num plano material, a matéria de proteção de dados encontra especial acolhimento na Lei N.º 132/V/2001 de 22 de janeiro que estabelece o regime jurídico de tratamento de dados pessoais no sector das telecomunicações e na Lei N.º 41/VIII/2013 – que estabelece o regime jurídico geral de Proteção de Dados Pessoais das Pessoas Singulares (RJPD).

**Palavra Chaves:** Dados Pessoais, Comunicações eletrónicas, transferência de dados, dados de base, dados de conteúdo, dados de tráfego, Direito Comparado, Cabo-Verde.

[1] Trabalho realizado no âmbito da disciplina Transferência Eletrónicas de Dados e Serviços de Telecomunicações – Universidade de Minho no Mestrado em Direito e Informática, em Novembro de 2017.

[2] Jurista licenciada pela Faculdade de Direito da Universidade Jean-Piaget de Cabo-Verde, Jurista no Gabinete Jurídico e de Resolução de Conflitos, da Autoridade Reguladora para a Comunicação Social de Cabo verde. Mestre (Especialidade Ciência Jurídico Empresariais) pela Universidade Portucalense de Portugal, em Direito e Mestranda em Direito e Informática na Universidade de Minho, Braga - Portugal.

**Introdução**

"Durante uma entrevista nos anos 50, Albert Einstein declarou que três grandes bombas haviam explodido durante o século XX: a bomba demográfica, a bomba atômica e a bomba das telecomunicações. Aquilo que Einstein chamou de bomba das telecomunicações foi chamado, por meu amigo Roy Ascott (um dos pioneiros e principais teóricos da arte em rede), de "segundo dilúvio", o das informações. As telecomunicações geram esse novo dilúvio por conta da natureza exponencial, explosiva e caótica de seu crescimento. A quantidade bruta de dados disponíveis se multiplica e se acelera. A densidade dos *links* entre as informações aumenta vertiginosamente nos bancos de dados, nos hipertextos e nas redes. Os contatos transversais entre os indivíduos proliferam de forma anárquica. É o transbordamento caótico das informações, a inundação de dados, as águas tumultuosas e os turbilhões da comunicação, a cacofonia e o psitacismo ensurdecedor dos Mídias, a guerra das imagens, a propagandas e as contrapropagandas, a confusão dos espíritos"[3]. O intento da aposição à cabeça, desse pequeno excerto, diremos assertivo, de Pierre Levy é que tal profecia diariamente se concretiza.

Presentemente vivemos numa Sociedade de Informação (SI), a qual corresponde à uma sociedade cujo o funcionamento corresponde a uma rede digital de informação. Volvidos os anos dourados da sociedade industrial e a sua massiva transformação do estrato social, atualmente adentramos numa fase pós-industrial onde a energia não é o principal propulsor, a força motora, o centro nefrálgico de toda a mudança, mas sim algo intangível, um ativo imaterial e poderosa, a **Informação**.

Nesse passo é interessante notar a que nível estamos, como foi reconhecido no parágrafo quinto do Livro Verde para a Sociedade de Informação em Portugal, o qual transcrevemos na íntegra, "as tecnologias da informação e das comunicações são já parte integrante do nosso quotidiano. Invadiram as nossas casas, locais de trabalho e de lazer. Oferecem instrumentos úteis para as comunicações pessoais e de trabalho, para o processamento de textos e de informação sistematizada, para acesso a bases de dados e à informação distribuída nas redes eletrónicas digitais, para além de se encontrarem integradas em numerosos equipamentos do dia a dia, em casa, no escritório, na fábrica, nos transportes, na educação e na saúde. A sociedade da informação não pertence a um

[3] Pierre Levy, Cibercultura, tradução Carlos Irineu da Costa, Editora 34, São Paulo 1999, pág. 12.

futuro distante. Assume uma importância crescente na vida coletiva atual e introduz uma nova dimensão no modelo das sociedades modernas"[4].

Assim, nos propusemos a analisar as diversas tipologias de Dados, nomeadamente os Dados de Base, de Conteúdo e de Tráfego, devido à sua importância prática relativamente à regulação das comunicações eletrónicas, tendo em consideração os direitos de personalidade a eles subjacentes e a sua circulação na *Internet*.

O trabalho está estruturado por tópicos e divide-se em duas partes. Na primeira parte daremos uma breve pincelada sobre a tutela dos Dados Pessoais, sua segurança e proteção na nossa atual SI e na segunda parte, faremos um apanhando geral sobre esses mesmos dados desmaterializados na Rede e por último faremos uma breve alusão sobre os diferentes tipos de dados existentes nas comunicações eletrónicas. O objetivo não é exaurir o estudo dos tipos de dados especificados, apenas traçar os marcos importantes da proteção e da tutela jurídica dos dados de tráfico e de conteúdo na nossa atual sociedade de informação, quer no que tange ao nível de faturação[5] quer no que tange ao combate à violação ou ao uso indevido e abusivo dos dados pessoais.

Este estudo tem como fonte principal leis, decreto - leis, jurisprudências e como fonte acessória e complementária manuais e artigos que versam sobre o tema.

Devido à falta de argumentos doutrinárias relativo às tipologias de dados, a nossa atenção versará essencialmente sobre diplomas legais e jurisprudências como forma de podermos driblar essa deficiência.

## 1. Os Dados Pessoais na Era Digital

Hodiernamente o estudo da temática de dados pessoais está intimamente relacionada com o da "vida privada"[6], enfatiza Garcia Marques. No entanto, reconhece o

[4] Livro Verde para a Sociedade de Informação em Portugal, iniciativa nacional para a sociedade de informação, pág. 7, disponível em http://homepage.ufp.pt/lmbg/formacao/lvfinal.pdf e acedida a 2 de 01 de 2017.

[5] "A chamada facturação detalhada é um meio colocado ao dispor do assinante para verificar a exactidão dos montantes cobrados pelo prestador do serviço mas, sendo um registo de conversações telefónicas, e, consequentemente, de dados de tráfego, põe em causa a privacidade dos utilizadores das comunicações electrónicas. Certamente por essa razão o artigo 8.º da Lei n.º 41/2004 admite a regulação da matéria com intervenção da Comissão Nacional de Protecção de Dados", Parecer da Procuradoria Geral da República N.º P000792008, *in* http://www.dgsi.pt/pgrp.nsf/0/b90edf9f8e8a47e480257515003eb4e8.

[6] **Telecomunicações e Proteção de Dados** *in* As Telecomunicações e o Direito na Sociedade de Informação, Faculdade de Direito de Coimbra, pág. 98.

autor que estes dois temas não se misturam, pois, apar de serem distintos um do outro tendem a ter abordagens igualmente distintas, factualidade essa que, não exclui as certas associações que os identificam.

Antes de prosseguirmos convém deixar assente que o tratamento da temática dos dados pessoais não se limita à sua correlação com a informática e o seu tratamento através de meios tecnológicos e telemáticos, a sua extensão vai mais além (os registos em papel de dados pessoais e a sua conservação e tratamento por meios manuais podem e devem merecer tutela jurídica, *rectius* documentos administrativos)[7].

Hoje em dia com a fluidez do conceito da vida privada, mais do que nunca convém ter em atenção o panorama dos dados que circulam todos os dias na rede.

Apregoa Garcia Marques, que entre os dados pessoais há graus ou níveis diferenciados de proteção, que vai desde o nível mínimo, ao qual pertencem os dados considerados público, até atingir o "núcleo duro" dos dados "pessoalíssimos" o qual mereceu especial atenção pelo legislador Constitucional no n° 3 do art.º 35. ° da Constituição da Republica Portuguesa e, no n.º 3 do artigo 45.° da Constituição de Cabo Verde.

Como é sabido, "a utilização da informática e o desenvolvimento das telecomunicações e das redes – nomeadamente a *Internet* - permitem uma crescente explosão de tráfico internacional de dados"[8]. Disso pode-se extrair a noção de que a *internet* ("Rede das redes") constitui uma ferramenta eficiente e eficaz de armazenamento de dados para sua posterior interconexão, difusão e utilização tanto ao nível interno como num cenário global.

Daí que, como salienta e bem Garcia Marques, "a informática é utilizada no tratamento de dados pessoais, como um armazenamento de informação mais ou menos detalhada sobre o individuo, há que compatibilizar os interesses relativos ao processo

[7] *Vide* a alínea b) do art.º 3.° da lei de proteção de dados pessoais que diz que " 'Tratamento de dados pessoais' ('tratamento'): qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição". No mesmo sentido ver o art.º 4. ° n.º 1 do mesmo diploma.

[8] **Telecomunicações e Proteção de Dados** *in* As Telecomunicações e o Direito na Sociedade de Informação, Faculdade de Direito de Coimbra, pág. 107.

económico social e ao desenvolvimento do comércio com a defesa e respeito pelos direitos fundamentais das pessoas singulares"[9].

Define-se dados pessoais no artigo 3. ° da lei n.º 67/98, de 26 de outubro na sua versão atualizada, doravante lei de proteção de Dados Pessoais, como "qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social". Similarmente o legislador de Cabo Verde define dados nos termos dos artigo (5.° n.º 1, alínea a) da Lei N.º 41/VIII/2013 – que prevê o Regime Jurídico Geral de Proteção de Dados Pessoais das Pessoas Singulares – doravante RJPD.

Devido ao caráter difuso da presença do individuo na rede, face à informática e às inovações tecnológicas convém acentuar que há tipos de dados que não são passíveis de tratamento, *verbi gratia* aqueles que abarcam os dados ditos "absolutamente" proibidos de tratamento informático, *verbi gratia* as convicções filosóficas, filiação partidária com exceções dos dados destinados ao tratamento estatístico desde que com a salvaguarda da "anominação"; conferir o art.º 35.° da Constituição cuja a *ratio* é o de impor limites à utilização dos dados informáticos e ao seu livre acesso pelos legítimos titulares.

Face ao desenvolvimento acelerado e sem freios da tecnologia de informação, o problema de segurança de informação se correlaciona essencialmente com a proteção conferida às informações armazenadas, processadas ou transmitidas, sob forma eletrónica contra ameaças deliberadas ou acidentais, a que está sujeita.

Sabendo que um sistema de informação é segura considerando os seguintes termos: que haja confidencialidade de informações, no sentido de permitir o acesso aos utilizadores autorizados, integridade, o que significa a garantia de que a informação é correta e a disponibilidade da mesma, ou seja, a possibilidade de utilizar a informação quando ela é necessária[10].

---

[9] **Telecomunicações e Proteção de Dados** *in* As Telecomunicações e o Direito na Sociedade de Informação, Faculdade de Direito de Coimbra, pág. 107.

[10] Ana Vaz – Segurança de Informação, Proteção da Privacidade e dos Dados Pessoais, revista Nação e Defesa, n.°7, 3° série, pág. 35 -63.

Enfatiza Oliveira Ascensão que "a *internet* assenta em estruturas de transmissão de dados em tempo real que revolucionaram os meios de comunicação. Não vale a pena insistir no que é de todos conhecidos"[11].

Quanto ao panorama dos dados em rede, a lei n° 41/2004 de 18 de agosto transpôs a diretiva n° 2002/EU relativa ao tratamento de dados pessoais e à proteção de privacidade no sector das telecomunicações eletrónicas, assegurando a proteção dos dados pessoais e os interesses dos assinantes[12]. Na ordem jurídica Cabo-verdiano vigora a Lei N.º 132/V/2001 de 22 de janeiro que estabelece o regime jurídico de tratamento de dados pessoais no sector das telecomunicações.

## 2. Proteção de Dados, Internet e os Direitos da Personalidade

A proteção de dados ao ser considerada como digna de tutela jurídica teve como alicerce e bem jurídico primacial - os direitos da personalidade. Desde antanho que os direitos da personalidade sempre estiveram ligados ao direito natural pondo enfase na tutela de direitos individuais e na noção da dignidade da pessoa humana.

Certos direitos da personalidade devido à sua natural sensibilidade, por exemplo, o direito à vida privada, direito à honra, direito à própria imagem, à intimidade etc.,

[11] Propriedade Intelectual e Internet**,** *in* Direito da Sociedade de Informação, volume VI, Coimbra editora, pág. 145. Importante frisar que a privacidade aqui designada é a "privacidade do conteúdo informativo somente com exclusão de aquelas que dizem respeito ao aborto, ao uso de métodos contracetivos, à homossexualidade, ou seja tópico relacionados com a liberdade da vida privada, não obstante tampouco a nossa intenção será o de excluir do âmbito da proteção de dados a liberdade à vida privada, mas sim concretiza-lo e se possível dimensiona-lo com respeito estrito à proteção dos dados pessoais nas comunicações eletrónicas.

[12] A origem do chamado "right of privacy" despoletou nos anos 1890 nos Estados Unidos da América num artigo publicado pela Harvard Law Review intitulada "Right of Privacy" dos autores Samuel Waren e Louis Brandes o qual foi pioneiro no estabelecimento das bases doutrinarias do "direito a ser deixado só" (*right to be alone*, na sua nomenclatura original), *in* http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.htmlno. No entanto esse direito só foi oficialmente reconhecido em 1966 pelo Supremo Tribunal Federal no caso Grisword *vs* Connectict, *vide* https://www.law.cornell.edu/supremecourt/text/381/479. No entanto hoje em dia vozes há que declaram a tutela da proteção dos dados pessoais fora do âmbito do direito à privacidade enquadrando-o num novo direito fundamental - o direito à autodeterminação informática, so o estudo dessa nova faceta de dados pessoais recomendamos a leitura do artigo "A releitura da privacidade: do "direito de ser deixado só" ao direito à autodeterminação informativa" de Kalline Carvalho G. Eler, publicado na revista Internacional de tecnologia, ciência e sociedade, vol. 5, num. 2, *in* http://journals.epistemopolis.org/index.php/tecnoysoc/article/view/1351, acedida a 11 de 01 de 2017. *Vide* igualmente o artigo intitulado "O direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança nos pós 11 de Setembro" de Catarina Sarmento e Castro, *in* http://www.buscalegis.ufsc.br/revistas/files/anexos/5544-5536-1-PB.pdf.

estando diretamente interligadas com a *internet* (por extensão da vida cotidiana à rede, através de manifestações diárias, partilha de opiniões, pensamentos, ideias, atos, imagens, transações, etc), através de relacionamentos gerados e na vivência *versus* convivência dos *Netcitzens City* (Cidadãos da Rede) na atual *City Bits* (Capital do Séc. XIX) na rede. Essa relação ou interceção homem-máquina num ambiente invisível / virtual, tem vindo a ser alvo de atenção por causa da exposição que certos níveis do social tem sobre o digital ou virtual.

Nessa ordem de ideia, e da disposição de situações fáticas, problemas vários surgem pondo em causa não só o direito à autodeterminação informacional, à privacidade à intimidade da vida dos indivíduos como a violação de seus dados pessoais, direito este como tantos outros considerados, invioláveis. Por exemplo, com um simples envio de publicidade via *e-mail* quando não solicitada (um *spam*) em que o usuário se vê invadido na sua esfera de intimidade com notícias de serviços e informações de produtos que não solicitado, ou ainda, através das técnicas *cookies* e *profiling*[13].

Também no âmbito do comércio eletrónico temos problemas que se corelacionam aos contratos eletrónicos, no qual as partes necessitam de navegarem num ambiente seguro e de confiança, mas que, por vezes são surpreendidos ou defraudados em suas espectativas necessárias do sigilo de certos dados confidenciais, por haver o perigo de dados virem a ser transferidos para terceiros (relações multipartidárias) ou virem a ser enganados ludibriados, através do uso ilegal e abusivo dos mesmos dados, questões estas que também ferem os direitos dos consumidores[14].

O grande dilema com qual se lida na atual era digital sugere que existe um lado que não nos importamos de revelar (de tornar público) e do outro lado, dados que queremos preservar da observação alheia (de manter em privado). Vítor Magalhães opina que a "distinção não é tão clara e muito menos banal", alega o mesmo que, não é por acaso que descriminamos dados familiares, privados, íntimos, relacionados aos nossos sonhos e atividades sexuais e vida amorosa, dados relacionados com a nossa saúde, etc. Para o mesmo autor, existe um longo *continuum* entre esses dois mundos, "público e

[13] O tratamento de dados de tráfego com a finalidade de recolher informação pelo administrador de um servidor para efeitos estatísticos ou comerciais, ou para efeitos de estabelecer o perfil dos usuários ("*profiling*"), vem expresso na Diretiva 2002/58/CE, nos considerandos 24 e 25.

[14] Cláudia Lima Nery *at., all., in* A Proteção de Dados Pessoais e a Internet, *in* http://www.tex.pro.br/home/artigos/258-artigos-dez-2013/6364-a-protecao-de-dados-pessoais-e-a-internet-the-personal-data-protection-and-the-internet.

privado pleno de matizes e ramificações de cinzentos infinitamente mais escuros ou mais claros"[15].

Relativamente à exclusão de certos dados em rede e ao seu tratamento cuidada, postula o autor supracitado que "a verdade é que somos seres sociais, mas também somos **entes** (sublinhado nosso) privados, indivíduos com uma mente secreta só nossa e esse espaço virtual de absoluta liberdade é essencial para sermos quem somos. Precisamos desse recato, da certeza de que não estamos a ser observados para levar a cabo aquele diálogo connosco mesmo que define o nosso eu, os nossos pensamentos, que estrutura os nossos atos que nos dá coerência com a mesma historia e as nossas ideias". Conclui o mesmo que a "vida privada se tornou apenas um jardim mais difícil de cuidar"[16].

## 2.1. Dados Pessoais e a Comunicação Eletrónica

Legislador constitucional consagra expressamente no artigo 34, n.º 4, "é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal». Apenas se vislumbra como legitima a ingerência nesse tipo de comunicação eletrónica para efeitos de investigação criminal, com a ressalva de que "mesmo em matéria de processo-crime, a ingerência nas telecomunicações só é permitida nos casos de o tipo legal d crime corresponder ao catálogo de crimes cuja gravidade social e o relevante interesse da paz social permitem essa ingerência"[17].

Por seu turno, o legislador Cabo-Verdiano assevera no n.º 2 do artigo 45.° da Constituição que "é proibida a utilização dos meios informáticos para registo e tratamento de dados individualmente identificáveis relativos às convicções politicas, filosóficas ou ideológicas, à fé religiosa, à filiação partidária ou sindical ou à vida privada", salvo nos casos em que haja consentimento do próprio titular, quando estiver previsto na lei ou para fins estatísticos.

---

[15] Fórum de Proteção de Dados, n° 1, julho de 2015, Comissão Nacional de Proteção de Dados (CNDP) Opinião – "Um Mundo de Coisas a Esconder", pág. 16.
[16] Fórum de Proteção de Dados, n° 1, julho de 2015, Comissão Nacional de Proteção de Dados (CNDP) Opinião – "Um Mundo de Coisas a Esconder", pág. 16.
[17] A Monitorização de dados pessoais de tráfego nas comunicações eletrónicas, Armando da Veiga *at. All.* Revista Raízes Jurídicas, Curitiba, vol. 3, n. 2, julho/dezembro2007, pág. 71, in http://ojs.up.com.br/index.php/raizesjuridicas/article/viewFile/168/140.

A liberdade e confidencialidade da correspondência e de todas as outras formas de comunicação constituem um dos pilares das sociedades democráticas modernas. A sua inviolabilidade encontra-se plasmado no artigo 8.º, n.º 1 da Convenção Europeia do Direito do Homem, quando diz "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". Na ordem jurídica interna, essa tal inviolabilidade do sigilo da correspondência e de outros meios de comunicação privada tem acolhimento expressa no artigo 34.º da CRP, consagrando-se o direito **à autodeterminação comunicativa ou da informação** (*vide* art.º 35 do mesmo diploma). A Declaração Africana sobre Direitos e Liberdades na Internet, garante aquela liberdade no seu ponto 8. Paralelamente o artigo 8.° (Capítulo II) da Convenção da União Africana sobre a Cibersegurança e a Proteção de Dados Pessoais. Esse mesmo direito fundamental encontra guarida na ordem jurídica de Cabo Verde no artigo 44. ° da Magna Carta.

O legislador constitucional português no seu artigo 34.° sem fazer nenhuma distinção ao nível da proteção dos diferentes tipos de meios de comunicação, proclamou que "o domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis», reiterando-se, no n.º 4 que "é proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo penal", podendo acrescer à comunicação ai retratada o a especificidade de ela ser "*eletrónica"*.

Reina na ordem jurídica interna português os princípios gerais no qual se fudam a proteção de dados pessoais, que são segundo a *ratio* da lei 67/98 os princípios da transparência e do respeito pelos direitos, liberdades e garantias individuais, mais especificamente o da reserva da vida privada[18]. Paralelamente em Cabo verde *vide* o artigo 44. ° da Constituição, que encontra aplicabilidade prática com no RJPD.

A Lei n.º 41/2004 de 18 de agosto, sobre a proteção da privacidade nas comunicações eletrónicas transpõe para a ordem jurídica interna a diretiva a diretiva da União Europeia (EU) 2002/59/CE, que veio complementar o disposto na lei 67/98 e

[18] Constitui um direito fundamental e ao mesmo tempo um direito fundamental próxima, de forma direta e incondicional à pessoa, art.º 70.° e seguintes da CRP. António Filipe, Acordos entre Portugal e Estados Unidos para a Cedência de Dados Pessoais, *in* Revista Seara Nova, n.º 1715, Primavera 2011, acedida em 24 de 12 de 2016, http://www.searanova.publ.pt/pt/1715/.

aplica-se a qualquer informação trocada ou enviada entre um número finito de comunicação eletrónica acessível ao público.

Reza o artigo 4. ° da lei 41/2004 no seu n.º 1 que**, "**as empresas que oferecem redes e ou serviços de comunicações eletrónicas devem garantir a inviolabilidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas acessíveis ao público".

A mesma prerrogativa foi salvaguardada no artigo 6. ° da Lei N.°132/V/2001 de 22 de janeiro quando dispõe que os prestadores de serviços e os operadores de rede devem garantir a confidencialidade e o sigilo das comunicações através dos serviços de telecomunicações acessíveis ao público e das redes pública de telecomunicações.

São três as tipologias ou se se quiser espécies de dados informáticos de nas comunicações eletrónicas[19], a saber dados de base, de tráfico e dados de conteúdo[20].

No que ao primeiro concerne, são dados de base os relativos à conexão à rede, com uma especial ressalva, para aqueles que são "cobertos pelo sistema de confidencialidade, a solicitação do assinante; nestes há que ter em consideração que o sigilo profissional em causa se releva de um simples interesse pessoal do utilizador que não contende com a respetiva esfera privada"[21];

---

[19] Dados informático no âmbito da Lei do Cibercrime (Lei n.°109/2009 de 15 de setembro) são quaisquer representações de factos, informações «ou conceitos sob uma forma suscetível de processamento num sistema informático incluindo os programas aptos a fazerem um sistema informático executar uma função", art.º 2. ° alínea b), e artigo 2.° n.º ali., d) da lei de proteção de dados nas comunicações eletrónica.

[20] Não obstante tem-se entendido que com a evolução das Diretivas comunitárias em matéria de comunicações eletrónicas verificou-se uma metamorfose no paradigma da proteção jurídica dos dados pessoais em que, ao lado da mencionada trilogia de dados de tráfego, de base e de conteúdo, surge agora a definição de dados de localização, Acórdão do Tribunal da relação de Guimarães (TRG) de 12 de abril de 2010 in www.dgsi.pt. **Dados de localização** são "quaisquer dados tratados numa rede de comunicação eletrónicas que indiquem a posição geográfica de equipamentos terminal de um assinante ou de qualquer utilizador de um serviço de comunicação eletrónica acessível ao publico", Lei n.º 32/2008 de 17 de julho que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, 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, *in* http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?artigo_id=selected&nid=1264&tabela=leis&pagina=1&ficha=1&nversao=.

[21] Contudo, e nesse mesmo acórdão, citando **Paulo Pinto de Albuquerque** *in* Comentário do Código de Processo Penal, pode-se discernir do comentário do mesmo relativo ao art.º 190°do CPP, o seguinte: "A obtenção dos dados de base, isto é, dos dados de conexão à rede, tais como a identidade do titular do telefone, a sua morada e o número do telefone, ainda que cobertos pelo sistema de confidencialidade a solicitação do assinante, obedece ao regime do artigo 135 do CPP. Estes elementos estão a coberto do sigilo profissional das operadoras telefónicas, mas não contendem com a privacidade dos titulares, pelo que podem ser comunicados a pedido de qualquer autoridade judiciária, aplicando-se correspondentemente, quando tenha sido deduzida escusa, o regime processual do incidente previsto no artigo 135 do CPP." Acórdão do Tribunal da Relação de Lisboa (doravante TRL) de 18 de 01 de 2011, in www.dgsi.pt .

Um exemplo prático de dados de base seria o caso de um senhor X que celebrasse um contrato com uma ISP[22] (*Internet Service Provider*) ou IAP (*Internet access provider*), empresas provedoras de *interne*, para o fornecimento de acesso à *internet*. Contudo, essas empresas oferecem principalmente serviço de acesso, mas como acessório, às vezes, agrega à prestação principal outros serviços relacionados, tais como: "conteúdo/notícias", serviços de "e-mail", de "hospedagem de sites" ou de "blogs", entre outros.

Os dados de tráfico[23] dizem respeito aos dados funcionais necessárias ao estabelecimento de uma ligação ou comunicação. São exemplos de dados de tráfego, a

[22] Parecer da Procuradoria Geral da República n.° 21/2000, in http://www.dgsi.pt/pgrp.nsf/0/b90edf9f8e8a47e480257515003eb4e8.

[23] Art.° 2.° alínea c) da Lei do Cibercrime são "dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático gerado poe este sistema como elemento de uma cadeia de comunicação, indicando a origem de comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo de serviço subjacente", como se pode constatar essa definição é bem mais ampla que o disposto na lei 41/2004, que considera dados de tráfico quaisquer dados tratados para efeito de envio de uma comunicação através de uma comunicação eletrónica ou para efeitos de faturação do mesmo. Relativamente a esse dado importante referir a **Diretiva 2002/58/CE**, que apenas se faz referência no rol das suas definições, os dados de tráfego, o qual "são quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações eletrónicas ou para efeitos da faturação da mesma", artigo 6.° n.º 2. No considerando 15 explica-se: "os dados de tráfego podem ser, nomeadamente, relativos ao encaminhamento, à duração, ao tempo ou ao volume de uma comunicação, ao protocolo utilizado, à localização do equipamento terminal do expedidor ou do destinatário, à rede de onde provém ou onde termina a comunicação, ao início, fim ou duração de uma ligação", *in* http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32002L0058&from=PT. De acordo com a opinião versada no parecer 10/2003 da CNPD, "também aqui se incluirão os dados identificativos", na medida opina-se no mesmo parecer "só a possibilidade de identificar o titular dos dados transformará esta informação em informação de carácter pessoal, objeto, por isso, da especial proteção das Diretivas comunitárias respeitantes à proteção de dados pessoais", *in* https://www.cnpd.pt/bin/decisoes/2003/htm/par/par010-03.htm. Sobre a proteção desses dados em específicos ver a Lei de comunicação eletrónica (LCE) e a lei da privacidade no setor das comunicações eletrónicas (LPSCE), que não infelizmente não conseguiremos aqui explanar, pelo que aconselhamos a leitura do artigo - A Monitorização de dados pessoais de tráfego nas comunicações eletrónicas, Armando da Veiga *at. All.* Revista Raízes Jurídicas, Curitiba, vol. 3, n. 2, julho/dezembro2007, pág. 14, in http://ojs.up.com.br/index.php/raizesjuridicas/article/viewFile/168/140. No entanto podemos deixar aqui um pequeno excerto no que tange aos dados de tráfego e o seu tratamento na LCE e na LSPCE, ali considerou-se o seguinte: "No seio da União Europeia, e em complemento da Directiva 95/46/CE, foi adotada a Directiva 2002/58/CE, em matéria de privacidade no sector das comunicações eletrónicas, que viria a ser transposta para o nosso ordenamento jurídico através da Lei n.º 41/2004, de 18 de Agosto, na qual se concretiza para que efeitos e em que termos é permitido o armazenamento de dados de tráfego. A concretização jurídico-legal da tutela dos dados de tráfego, atualmente, assenta na Lei das Comunicações Eletrónicas (LCE)72, e na Lei da Privacidade no sector das Comunicações Eletrónicas (LPSCE). Assim, na LCE encontra-se estabelecido como princípio geral de regulação das comunicações eletrónicas, a ser assegurado pela Autoridade de Regulação Nacional, «defender os interesses dos cidadãos (...)» (artigo 5.º, n.º 1, al. c). A defesa é assegurada, na temática que nos ocupa, pela garantia de «um elevado nível de proteção dos dados pessoais e da privacidade» (artigo 5.º, n.º 4, al. c). A defesa dos cidadãos em matéria de inviolabilidade do sigilo das comunicações privadas deve ser assegurada pelas empresas que oferecem redes e serviços de comunicações que deverão garantir a segurança das redes públicas contra o acesso não autorizado [artigo 27.º, n.º 1 al. e)] e a «proteção dos dados pessoais e da privacidade no domínio específico das comunicações eletrónicas, em conformidade com a legislação aplicável à proteção dos dados pessoais e da privacidade» [artigo 27.º, n.º 1, al g)]. O regime de inviolabilidade do sigilo das comunicações

localização do utilizador, ou a localização do destinatário[24], a duração da utilização dos serviços, a data e hora, frequência do seu uso. Um exemplo específico de dados de tráfico seria o caso desse mesmo Senhor X, ligado devidamente ao serviço de *internet*, resolver enviar uma mensagem de correio eletrónico a um amigo (do tipo 'amanhã vamos jantar às 21 horas, abraças, assinado António').

Nesse caso, a hora do envio da mensagem, o volume dos dados transmitidos o IP (*internet protocol*) de origem etc., farão parte integrante da estrutura dos dados de tráfego[25].

Tendo em conta que são vários os serviços de telecomunicações utilizados para a transmissão de comunicações verbais ou de outro tipo, *verbi gratia*, mensagens escritas, dados por pacotes, os elementos inerentes à comunicação podem estruturar-se

---

eletrónicas implícito na LCE apenas encontra a limitação, configurada na obrigatoriedade de «instalação, a expensas próprias, e disponibilização de sistemas de interceção legal às autoridades nacionais competentes bem como fornecimento dos meios de desencriptação ou decifração sempre que ofereçam essas facilidades (...)». O quadro legal das comunicações eletrónicas acabado de enunciar de definição geral remete para a legislação aplicável à proteção dos dados pessoais e em matéria de privacidade. Torna-se, por isso, necessário fazer um breve incurso pela LPSCE, em busca da concretização das disposições enunciadas. A LPSCE, estabelece como princípio geral a inviolabilidade do sigilo das comunicações eletrónicas referindo *expressis verbis* que «as empresas que fornecem redes ou serviços de comunicações electrónicas devem garantir a inviolabilidade das comunicações e respetivos dados de tráfego (...)» (artigo 4.º, n.º 1), ficando, por outro lado, proibida «a escuta, instalação de dispositivos de escuta, o armazenamento ou outros meios de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, com exceção dos casos previstos na lei» (artigo 4.º, n.º 2). A observância deste regime não impede o armazenamento digital, intermédio e transitório ou o acesso a dados de tráfego para determinadas finalidades expressamente contempladas legalmente".

[24] Importa deixar claro que nos termos do considerando 35 da Diretiva 2002/58 da EU "en las redes móviles digitales se tratan los datos sobre localización que proporcionan la posición geográfica del equipo terminal del usuario móvil para hacer posible la transmisión de las comunicaciones. Tales datos constituyen datos sobre tráfico a los que es aplicable el artículo 6 de la presente Directiva. Sin embargo, además, las redes móviles digitales pueden tener la capacidad de tratar datos sobre localización más precisos de lo necesario para la transmisión de comunicaciones y que se utilizan para la prestación de servicios de valor añadido tales como los servicios que facilitan información sobre tráfico y orientaciones individualizadas a los conductores. El tratamiento de tales datos para la prestación de servicios de valor añadido sólo debe permitirse cuando los abonados hayan dado su consentimiento. Incluso en los casos en que los abonados hayan dado su consentimiento, éstos deben contar con un procedimiento sencillo y gratuito de impedir temporalmente el tratamiento de los datos sobre localización". Frisa-se igualmente "que só é possível verificar-se a transmutação dos dados de localização em dados de tráfego ao nível dos sistemas de localização GPS, sempre que os mesmos são usados ao nível dos serviços de valor acrescentado. Entende-se por "dados de localização" aqueles que são tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma. Por seu turno, estamos perante "serviços de valor acrescentado" sempre que um serviço requeira o tratamento de dados de tráfego ou dados de localização que não sejam dados de tráfego, para além do necessário à transmissão de uma comunicação ou à faturação da mesma", *vide* A Monitorização de dados pessoais de tráfego nas comunicações eletrónicas, Armando da Veiga *at. All.* Revista Raízes Jurídicas, Curitiba, vol. 3, n. 2, julho/dezembro2007, pág. 14, in http://ojs.up.com.br/index.php/raizesjuridicas/article/viewFile/168/140, pág. 76.

[25] Parecer n.º 21/2000 da Procuradoria Geral da República, in http://www.dgsi.pt/pgrp.nsf/0/b90edf9f8e8a47e480257515003eb4e8.

sequencialmente em quatro tempos: a **fase prévia** à comunicação, **o estabelecimento da comunicação**, **a fase da comunicação propriamente dita** e a **fase posterior à comunicação**.

No primeiro tempo domina os dados de base, já nos restantes, considera-se a materialização dos dados de tráfego e de conteúdo.

Tecnicamente falando, como expõem os relatores do acórdão do Tribunal da Relação de Guimarães "os dados de base constituem, na perspetiva dos utilizadores, os elementos necessários ao acesso à rede, designadamente através da ligação individual e para utilização própria do respetivo serviço: interessa aqui essencialmente o número e os dados através dos quais o utilizador tem acesso ao serviço. (...) Diversamente dos elementos de base (elementos necessários ao estabelecimento de uma base para comunicação), que estão aquém, antes, são prévios e instrumentos de qualquer comunicação, os chamados elementos de tráfego (elementos funcionais da comunicação), como os elementos ditos de conteúdo, têm já a ver diretamente com a comunicação, quer sobre a respetiva identificabilidade, quer relativamente ao conteúdo propriamente dito da mensagem ou da comunicação"[26].

Do referido acórdão se pode concluir igualmente que os elementos ou dados funcionais (de tráfego), necessários ou produzidos pelo estabelecimento da ligação da qual uma comunicação concreta, com determinado conteúdo, operada ou transmitida, **são a direção, o destino (*adressage*) e a via, o trajeto (*routage*)**. (... ). Como ficou assente, estes elementos **funcionalmente necessários** ao estabelecimento e à direção da comunicação identificam, ou permitem identificar a comunicação: "quando conservados, possibilitam a identificação das comunicações entre o eminente e o destinatário, a data, o tempo, e a frequência das ligações efetuadas".

Estes elementos dizem respeito diretamente à comunicação, uma vez que possibilitam a identificação, "em tempo real ou a *posteriori"*, dos utilizadores, do relacionamento direto entre os mesmos através da rede, a localização, a frequência, a data, hora e a duração da comunicação, estes mesmos elementos "devem participar das garantias a que está submetida a utilização do serviço, especialmente tudo quanto respeite ao sigilo das comunicações"[27].

[26] Acórdão do Tribunal da Relação de Guimarães (TRG) de 12 de abril de 2010, in www.dgsi.pt.
[27] Acórdão do Tribunal da Relação de Guimarães (TRG) de 12 de abril de 2010, in www.dgsi.pt.

Importante ter presente a Recomendação do Conselho da Europa sobre a proteção dos dados pessoais no sector das telecomunicações[28]:

No seu ponto n.º 3 considera, que a conservação generalizada dos dados de tráfego relativos a todas as comunicações e operações eletrónicas dos cidadãos, com o único objetivo de proporcionar material de investigação às autoridades responsáveis pela aplicação da lei, poria seriamente em risco a democracia que pretensamente visa proteger. No seu ponto n.º 5 quando apela aos Estados-Membros a velarem para que as medidas para a conservação dos dados de tráfego por parte dos prestadores de serviços de comunicações eletrónicas:

a) Sejam claramente regulamentadas por lei;
b) não revelem, direta ou indiretamente, o conteúdo das comunicações recolhidas;
c) se revistam de salvaguardas suficientes contra o acesso ilegal e a interceção, a divulgação ou qualquer outro abuso.

O acesso das autoridades responsáveis pela aplicação da lei aos dados conservados deve:

a) Exigir a autorização das autoridades judiciais baseada numa necessidade demonstrada e no respeito de condições estritas;
b) Limitar-se exclusivamente aos objetivos pelos quais a legislação da União Europeia e a Convenção Europeia dos Direitos do Homem permitem exceções ao princípio da confidencialidade das comunicações;
c) referir-se especificamente a uma operação, a um assinante ou a um utilizador.

E a final, faz uma importante ressalva que achamos por bem deixar aqui assente. A de que "os dados aos quais as autoridades responsáveis pela aplicação da lei tenham acesso não devem ser transmitidos a países não membros da União que não respeitem as garantias relativas à confidencialidade das comunicações e o direito à privacidade e à proteção dos dados consignados na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia dos Direitos do Homem".

[28] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B5-2003-0013+0+DOC+XML+V0//PT.

Note-se que os dados, registos e informações inscritos em suporte de papel não deverão ser conservados pelas empresas operadoras para além do período necessário para a sua transmissão às entidades referidas. Às empresas operadoras de telecomunicações não é exigido qualquer juízo sobre a relevância das vicissitudes do processo penal em curso quanto à pertinência ou necessidade de conservação dos referidos elementos.

No entanto, nos termos da alínea e) do artigo 5.º da Lei n.º 67/98, de 26 de outubro os dados pessoais devem ser "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". No mesmo sentido vai a redação da lei n.º 41/2004 no seu art.º 6. °, n.º 3, "o tratamento referido no número anterior apenas é lícito até final do período durante o qual a fatura pode ser legalmente contestada ou o pagamento reclamado. Mais claro foi o legislador da Lei do Cibercrime (lei 109/2009 de 15 de setembro), referindo-se quanto à ordem de preservação discriminada, cujo o prazo não podia exceder três meses sob pena de nulidade da coleta, tratamento ou processamento do mesmo. Questionamos a aplicabilidade desse prazo em corelação com o previsto na Lei 41/2004, se haverá a cumulação dos mesmos, se não qual deles terá preferência.

Em Cabo Verde, numa das raras decisões, senão a única encontrada que retrata em sede judicial estas questões foi em 2017 ( acórdão 07/16-17) no âmbito de um recurso ordinário para o Supremo Tribunal de Justiça, numa ação penal, os doutos juízes pugnaram em conclusão que, tendo em conta que: *"a diligência iria, seguramente, abranger pessoas alheias aos factos em investigação, recolhendo informações de inocentes na expectativa de, entre eles, se encontrar algum suspeito, o que implica, necessariamente, uma compressão ilícita de direito à privacidade e à inviolabilidade das telecomunicações, como, nesta última, bem ajuizou o Mm°. Juiz* a quo, *no despacho recorrido. (...)*

*(....) Sendo assim, o despacho recorrido, apesar de ser lacónico, no dizer do Mmº Juiz* a quo, *termo que mereceu avocação por parte da Digníssima Procuradora de Círculo no seu parecer, não falecia, contudo, de razão; e deverá manter-se; porquanto, não havendo suspeito tal como previsto no Cód. Proc. Penal, e estando em causa direitos fundamentais (direito à privacidade e inviolabilidade das telecomunicações), as respetivas restrições, nos termos requeridos pelo Ministério Público, junto do Tribunal* a quo, *têm de se conformar com o quadro indicado pelo artigo 44º da CRCV e 255º, nº1,*

*a) e 2 do Código Processo Penal vigente, devendo, ainda, reger-se pelos critérios da proporcionalidade, adequação e necessidade, o que, pelo que ficou dito, não era o caso.*

Rege em ambos os ordenamentos o princípio da inviolabilidade das comunicações eletrónicas (artigo 4. ° da Lei N.º 41/2004 de 18/18, e em Cabo Verde nos termos do artigo 6.° da Lei N.°41/2001 de 22 de janeiro).Ou seja, as empresas que oferecem redes e/ou serviços de comunicações eletrónicas devem garantir a inviolabilidade das comunicações e os respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas acessíveis ao público sendo por isso terminantemente proibida a escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, sem prejuízo das exceções legais.

Constitui exceção à obrigatoriedade acima exposta, as gravações legalmente autorizadas de comunicações e dos respetivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas, para o efeito de prova de uma transação comercial nem de qualquer outra comunicação feita no âmbito de uma relação contratual, desde que o titular dos dados tenha sido disso informado e prestado o seu consentimento. A Lei de Cabo Verde é omissa neste aspeto, contudo, Cabo Verde sendo signatário da convenção da união africana sobre a cibersegurança e proteção de dados pessoais, observará exceções nela garantidas - artigo 10.° n.º 1.

Contudo o armazenamento referido, em Portugal, apenas é permitido se o seu titular tiver dado o seu consentimento prévio, com base em informações claras e completas nos termos da Lei de Proteção de Dados Pessoais, nomeadamente quanto aos objetivos do processamento. Ou ainda o armazenamento técnico, desde que:

a) Que tenha como única finalidade transmitir uma comunicação através de uma rede de comunicações eletrónicas;
b) Estritamente necessário ao fornecedor para fornecer um serviço da sociedade de informação solicitado expressamente pelo assinante ou utilizador.

As empresas que oferecem redes e/ou serviços de comunicações eletrónicas acessíveis ao público devem, quando tal for compatível com os princípios da necessidade, da adequação e da proporcionalidade, anular por um período de tempo não superior a 30 dias a eliminação da apresentação da linha chamadora, a pedido, feito por escrito e

devidamente fundamentado, de um assinante que pretenda determinar a origem de chamadas não identificadas perturbadoras da paz familiar ou da intimidade da vida privada, caso em que o número de telefone dos assinantes chamadores que tenham eliminado a identificação da linha é registado e comunicado ao assinante chamado.

Relativamente às Comunicações não solicitadas (Artigo 13.º-A, da Lei em Portugal) Exige o consentimento prévio e expresso do assinante que seja pessoa singular, ou do utilizador, o envio de comunicações não solicitadas para fins de marketing direto, designadamente através da utilização de sistemas automatizados de chamada e comunicação que não dependam da intervenção humana (aparelhos de chamada automática), de aparelhos de telecópia ou de correio eletrónico, incluindo SMS (serviços de mensagens curtas), EMS (serviços de mensagens melhoradas) MMS (serviços de mensagem multimédia) e outros tipos de aplicações similares.

Quanto ao regime sancionatório, tanto a lei Portuguesa quanto a Cabo-Verdiana face aos incumprimentos dos regimes elencados nas legislações em pauta, sujeita as ações dos perpetradores ao regime sancionatório aplicáveis, caso se verificar infrações aos regimes em pauta, sujeitando-os à contraordenação, punível com coima tanto a pessoas singulares quanto a pessoas coletivas, e sanções acessórias (exclusivo na lei Portuguesa) de perda a favor do Estado de objetos, equipamentos e dispositivos ilícitos, incluindo o produto do benefício obtido pelo infrator através da prática da contraordenação. Em Cabo verde permite a punição da tentativa e da negligência.

**Conclusão**

O tema em si é muito vasto, daí que se pretendeu apenas um breve apanhado sem descurar certos pontos concretos como o que seja a SI de hoje em dia, os dados pessoais e dados de comunicações assim como as tipologias de dados passiveis de serem tratadas no âmbito da própria comunicação eletrónica.

O tratamento e a tutela dos mesmos mereceram atenção cuidada tanto na própria Constituição da República como nas diversas leis ao qual se fez referência e no atual Direito da União Europeia em diversas diretivas que moldaram o tema e em sintonia com a teologia pretendido tem se vindo a resguardar e a se proteger os dados pessoais dos cidadãos, nessa sociedade cada vez mais democrática relativo às informações. Território cujo o tratamento da matéria em pauta já se pode considerar condensado e da qual Cabo

Verde tem vindo a beber, sem descurar a sua própria realidade, no sentido de fortalecer a sua ceara legislativa, colmatando zonas opacas e situações de omissão legal.

Contudo, somos de opinião que Cabo Verde tem trilhado um bom caminho nesse sentido, porque tem vido a adotar tanto medidas legislativas como ações políticas no sentido de fortificar o país de uma ordem jurídica segura e robusta.

Volvidos quase 20 que entrou em vigor a Lei cabo-verdiana de proteção de dados nas comunicações eletrónicas mister se faz uma atualização da mesma, adequando-a ao avançar da técnica. Como explicita *Zigmund Bauman* (Sociólogo Polonês, obra Vigilância Liquida) "a lei deve olhar para o futuro e construir o sistema de valor ético que seja aplicável em qualquer circunstancias tecnológicas. Nesse sentido, é aconselhável que a lei seja flexível e, para tanto, baseada de forma importante em princípios. Mas não nos esqueçamos que a proteção à privacidade está associada à evolução da técnica, num mundo imprevisível que requer flexibilidade e pensamento rápido. A Lei prescritiva será sempre restritiva não porque seja severa, mas porque é rígida (inflexível).

A liberdade hoje é desafiada pelas técnicas que se destinam à construção de uma sociedade de tecnológica. As instituições devem recorrer a meios necessários, estratégicos e adequados que possam assegurar a privacidade dos indivíduos na sociedade. A privacidade, contudo, não pode continuar sendo encarada apenas pelo prisma proposto Warren e Brandeis no "*right to be alone*" (1890) - "direito de ser deixado só", antes, em consonância com a atual sociedade da informação, precisa ser vista também como um direito à autodeterminação informativa. A proteção de dados constitui, atualmente um dos aspetos mais significativos da liberdade individual, daí que com essa pequena dissertação visou-se fornecer instrumentos valorativos para que o tratamento de dados pessoais considere o novo conceito integral de pessoa, que se manifesta pela sua identidade social e individual; pelo seu corpo físico e eletrônico. E lançamos um desafio para um melhor estudo, analise e enquadramento desse novo direito, o "direito à autodeterminação informativa" sejam feitos, pois também reconhecemos nesse direito, a possibilidade do individuo ter o direito de manter o controle sobre as próprias informações; o direito de escolher aquilo que será revelado; direito ao esquecimento, em resumo, o direito de determinar a maneira de construir a própria esfera particular.

Actualizado em Setembro de 2020, Cabo-Verde

*Katy Fernandes*

## Bibliografia

**Manuais:**

Pierre Levy**, Cibercultura**, tradução Carlos Irineu da Costa, Editora 34, São Paulo 1999

Garcia Marques**, Telecomunições e Proteção de Dados** *in* As Telecomunicações e o Direito na Sociedade de Informação, Faculdade de Direito de Coimbra.

Ana Vaz – **Segurança de Informação**, **Proteção da Privacidade e dos Dados Pessoais**, revista Nação e Defesa, n.°7, 3° série.

José Oliveira Ascensão - **Propriedade Intelectual e Internet, *in* Direito da Sociedade de Informação**, volume VI, Coimbra editora.

Vítor Magalhães - "**Um Mundo de Coisas a Esconder**", Fórum de Proteção de Dados, n° 1, julho de 2015, Comissão Nacional de Proteção de Dados (CNDP).

**Artigos:**

Livro Verde para a Sociedade de Informação em Portugal, iniciativa nacional para a sociedade de informação, disponível em: http://homepage.ufp.pt/lmbg/formacao/lvfinal.pdf

Parece da Procuradoria Geral da República N.º P000792008, em: http://www.dgsi.pt/pgrp.nsf/0/b90edf9f8e8a47e480257515003eb4e8.

Right Of Privacy em: http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.htmlno.

Kalline Carvalho G. Eler - **A releitura da privacidade: do "direito de ser deixado só" ao direito à autodeterminação informativa**", Revista Internacional de tecnologia, ciência e sociedade, vol. 5, num. 2, em: http://journals.epistemopolis.org/index.php/tecnoysoc/article/view/1351.

Catarina Sarmento e Castro - **O Direito à Autodeterminação Informativa e os novos desafios gerados pelo direito à liberdade e à segurança nos pós 11 de Setembro**, em: http://www.buscalegis.ufsc.br/revistas/files/anexos/5544-5536-1-PB.pdf.

Cláudia Lima Nery *at., all.*, - **A Proteção de Dados Pessoais e a Internet**, em: http://www.tex.pro.br/home/artigos/258-artigos-dez-2013/6364-a-protecao-de-dados-pessoais-e-a-internet-the-personal-data-protection-and-the-internet.

Armando da Veiga *at. All* - **A Monitorização de dados pessoais de tráfego nas comunicações eletrónicas,** Revista Raízes Jurídicas, Curitiba, vol. 3, n. 2, julho/dezembro2007, pág. 71, em: http://ojs.up.com.br/index.php/raizesjuridicas/article/viewFile/168/140.

António Filipe**, Acordos entre Portugal e Estados Unidos para a Cedência de Dados Pessoais**, *in* Revista Seara Nova, n.º 1715, Primavera 2011, acedida em 24 de 12 de 2016, http://www.searanova.publ.pt/pt/1715/.

Parecer da Procuradoria Geral da República n.° 21/2000, in http://www.dgsi.pt/pgrp.nsf/0/b90edf9f8e8a47e480257515003eb4e8.

**Legislações:**

Constituição da República Portuguesa

Directiva 2002/58/CE de 12 de Julho de 2002;

Lei do Cibercrime (Lei n.°109/2009 de 15 de setembro.

Lei n.º 32/2008 de 17 de julho que transpõe para a ordem jurídica interna a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março.

Lei n.º 41/2004, de 18 de Agosto.

Lei n.º 67/98 de 26 de Outubro.

**Acórdãos:**

Acórdão do Tribunal da Relação de Guimarães de 12 de 04 de 2010 in www.dgsi.pt.

Tribunal da Relação de Lisboa de 18 de 01 de 2011, in www.dgsi.pt.

http://www.jurisprudencia.cv/juris/JURIS:CV:TRB:2017:3/

**Lidos e recomendados:**

Acórdão do Supremo Tribunal de Justiça de 16 de 10 de 2014, *in* www.dgsi.pt.

Acórdão da Relação de Coimbra de 26 de 02 de 2014, in www.dgsi.pt.

Acórdão da Relação de Lisboa de 21 de 01 de 2013, in www.dgsi.pt.

Acórdão da Relação de Lisboa de 16 de 06 de 2014, in www.dgsi.pt.

Acórdão da Relação de Lisboa de 22 de 06 de 2016, in www.dgsi.pt.

Acórdão da Relação de Lisboa de 11 de 02 de 2011, in www.dgsi.pt.

http://www.jurisprudencia.cv/juris/JURIS:CV:TRB:2017:3/