
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VI – SETEMBRO/OUTUBRO DE 2018

REVISTA CIENTÍFICA SOBRE CYBERLAW DO CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO – CIJIC – DA FACULDADE DE DIREITO DA UNIVERSIDADE DE LISBOA

ISSN 2183-729

NOTAS DO EDITOR:

No prólogo de mais esta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, antecipo-me a aduzir dois actos, em breve, solenes, que não deverão passar em claro nas agendas de cada um.

O primeiro desses actos terá lugar no próximo 17 de Outubro na Universidade de Aveiro. Trata-se da Sétima edição da Iniciativa Portuguesa do Fórum da Governação da Internet.

Um sublinhado desde logo para o local do evento. É importante que a academia se sinta interligada com Portugal, no seu todo. Sair de Lisboa, do conforto centralizador da capital, é um pequeno mas mui nobre sinal de que há muito e bom trabalho a ser desenvolvido diariamente na plenitude dos mais de 98 mil quilómetros quadrados que compõem o nosso pequeno país.

No que à edição deste ano do Fórum da Governação da Internet diz respeito, trata-se de um evento organizado pela FCT (Fundação para a Ciência e a Tecnologia I.P), em parceria com a ANACOM (Autoridade Nacional de Comunicações), APDSI (Associação para a Promoção e Desenvolvimento da Sociedade da Informação), API (Associação Portuguesa de Imprensa), Associação DNS.PT, Ciência Viva (Agência Nacional para a Cultura Científica e Tecnológica), CNCS (Centro Nacional de Cibersegurança), IAPMEI (Agência para a Competitividade e Inovação), ISOC-PT

(Capítulo Português da ISOC), Polo TICE.PT, Secretaria Geral da Presidência do Conselho de Ministros, e Sociedade Civil.

Serão objecto de discussão, temas como «Governação e políticas públicas da Internet nos contextos nacional e global»; «Inteligência Artificial e *Big data*»; «Segurança no Ciberespaço: O dilema entre a privacidade do indivíduo e a segurança do Estado»; «Governação, confiança, privacidade e desafios na era do IoT»; «*Fake news, fake views* -Sociedade da (Des)Informação».

As sessões e respectivos painéis apresentam temas e oradores de reconhecida qualidade, e, seguramente, será um 17 de Outubro de 2018 muito e bem preenchido em Aveiro[1].

O outro evento, como seria natural, até pelo investimento feito pelo país na realização deste por mais dez anos em Portugal, é a *Lisboa web summit* 2018.

O programa e agenda[2] da feira, que se realizará no Altice Arena entre 5 e 8 de Novembro, já foram dados a conhecer. O destaque recai na presença de oradores como o Secretário-Geral das Nações Unidas, Sr. António Guterres; o inventor do *www*, Sir Tim Berners-Lee; o CEO do eBay, Mr. Devin Wenig; a Comissária Europeia para a Concorrência, Mrs. Margrethe Vestager; entre outros.

Os temas são vastos. A agenda *idem*. Uma semana desta feira para explorar avidamente.

Em suma, sendo eventos contrastantes na apresentação, na forma e até na finalidade, seria pouco cordial não aproveitar a proximidade destes para esta nota de agenda.

Arrolado o introito, focando-nos apenas no essencial desta nova edição, seguramente que a entrada em vigor, em pleno, do RGPD - *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*; bem como da Lei Geral de Protecção de Dados (LGPD) no Brasil, aprovada no plenário do

1 Informações sobre o programa do evento podem ser consultadas em: https://www.governacaointernet.pt/pdf/forum_programa_2018.pdf.
O evento é de entrada livre mas requer uma inscrição prévia. Mais informações em: https://www.governacaointernet.pt/2018.html
2 Mais informações em: https://websummit.com/schedule

Senado Federal pelo PLC 53/2018, a 10 de Julho; impuseram que o tema da protecção de dados pessoais fizesse, novamente, parte do cardápio da revista.

No plano nacional, a Proposta de Lei 120/XIII, que 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, continua em suave desenvolvimento[3], mais de dois anos após a publicação do Regulamento europeu, o RGPD.

Não obstante, procurando contrariar o *adagio* da Proposta de Lei 120/XIII, procuramos coligir doutrina e opinião que demonstrem um pouco do *vivace* de pessoas e organizações na adaptação às novas realidades supranacionais. Neste sentido, encontraremos *ways not to read* o RGPD; as principais dificuldades e dúvidas partilhadas por organizações e por pessoas singulares na adaptação à nova realidade jurídica europeia. *Curiosamente*, do outro lado do Atlântico, trazemos, ainda, o impacto da LGPD brasileira nos negócios e nas pessoas, neste novel quadro normativo de agregação temática. É, pela actualidade do tema, tempo, ainda, de reintegrar o conceito de desindexação, *in casu*, da desindexação de conteúdos ofensivos na net, recuperando críticas jurídicas ao relevante caso *Google Spain*.

Saltando da circunspecção dos dados pessoais e da privacidade para outro tema, serão apresentadas reflexões quanto à apreensão de correio eletrónico e registos de comunicação de natureza semelhante. O tema é fervilhante. Na actualidade, a vivência em sociedade cresce *digitalodependente*, convocando discussões doutrinárias profundas. Ainda não será desta que se pacificará, entre os intérpretes e aplicadores do direito, a distinção juridicamente relevante entre correio e correio eletrónico. Mas, as reflexões que aqui se publicam, valem a leitura e o crepitar de questões.

Colocada em perspectiva esta espécie de matrimónio, de conveniência, que o direito e a tecnologia assumiram, a problemática dos drones, inteligência artificial e robótica, também têm aqui palco no plano jurídico.

Direito e Tecnologia são meios essenciais ao desenvolvimento do homem, com implicações, dilacerantes, nas mais variadas formas em como revelamos o ser social que somos. A ética, juridicamente relevante, aliada à segurança - subjacente ao

3 Pode ser consultada a actividade relativa à Proposta de lei em: http://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=42368

conceito *Safe-by-design* (SbD) - estimulam dissecções imediatas desde o plano de concepção, no patamar R&D do desenvolvimento das mais diversas ferramentas, utensílios, *gadgets*, cada vez mais apetrechadas de inteligência artificial e robótica, que vão procurando satisfazer necessidades diversas do *mercado*, isto é, nossas.

Aproveitando a epígrafe, projecto uma questão, que gostava de ver discutida numa próxima edição da revista: será profícuo que ao invés da pirexia em torno da segurança - a qualquer custo - dos dispositivos, tentando antecipar toda a indeterminabilidade da vida humana – com todos os custos inerentes a esta tarefa de adivinhação – o foco poderia vir a incidir sobre a *responsabilidade pela segurança*? Assumindo-se a impossibilidade de segurança absoluta de toda e qualquer ferramenta, será que alvitraremos, no futuro, um modelo de responsabilidades partilhadas como solução?

A insolência típica das muitas questões não poderia terminar sem o regresso a uma ideia em processo de maturação: como conciliar diversas ordens, práticas e tradições jurídicas; actores, partes e contrapartes processuais; pessoas singulares, organizações e Estados, perante tal amálgama de situações quotidianas neste *pot-pourri* que a Internet é e do qual dependemos? Estaremos no vértice da necessidade de um Tribunal Internacional para a Internet? Mais umas penadas sobre a arquitetura de um desejável edifício de harmonização e resolução de pleitos jurídicos a nível mundial.

Resta-me, por fim, agradecer a todos pelo esforço e pelo trabalho, endereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um sentido reconhecimento a cada um dos autores: Muito Obrigado.

Cyberlaw by CIJIC, ***Direito: a pensar tecnologicamente*.**

Boas leituras.

Lisboa, FDUL, 05 de Outubro de 2018

Nuno Teixeira Castro

CYBERLAW

by CIJIC

OPINIÃO

"*WAYS NOT TO READ*" O RGPD *

RAQUEL BRÍZIDA CASTRO [1]

* 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 (Doravante RGPD).

1 Professora da Faculdade de Direito da Universidade de Lisboa; Doutora em Direito; *Of Counsel* Andersen Tax Legal Portugal. Contacto: raquelcastro@fd.ul.pt

A principal dificuldade da teoria tradicional da interpretação revela-se, precisamente, nos casos em que não existe um critério inequívoco de solução. O que, por exemplo, no plano constitucional, equivale a dizer em todas as situações que pressupõem interpretação constitucional, porque o poder constituinte optou por não o adotar.

Essa indefinição *a priori*, todavia, não legitima os erros sugeridos pela lição norte-americana através da indicação de *"ways not to read the Constitution*", a partir da identificação de dois tipos de resultados interpretativos indesejáveis, como sejam a *"desintegração"* e a *"hiperintegração"*. A *"desintegração*" constitui uma forma de interpretação que ignora o facto de as suas partes se encontrarem integradas num todo, tratando-se efetivamente de uma Constituição e não de simples conjuntos de cláusulas e preceitos separados, com histórias distintas. Pelo contrário, a *"hiperintegração"* ignora que o todo integra partes distintas, parcelas que foram introduzidas em momentos distintos da história constitucional, apoiadas e refutadas por diferentes grupos ou que refletem posições completamente diferentes e, nalguns casos, mesmo opostas. É ilegítima uma interpretação constitucional que ignore as suas contradições e incoerências, ou que se baseie na pretensão de que os valores constitucionais são imunes às contingências histórica e tecnológica.

Já todos discorremos sobre o desconcerto interpretativo gerado pelas diferentes pré-compreensões dos vários intérpretes, conducentes a leituras *hiperintegradas* da Constituição, supostas litografias fiéis da sua alegada missão unitária. O que há, então, de novo na interpretação constitucional e no alerta da doutrina constitucional norte-americana? É que esse pântano hermenêutico tende a expandir-se perante a brutal pressão mutante das novas tecnologias. A contenda constitucional é flagrante, mas perante o desconhecido para que a tecnologia nos arrasta, o intérprete socorre-se das suas mais íntimas convicções e preconceitos, privilegiando incondicionalmente este ou aquele princípio ou direito fundamental, transmutando o programa normativo-constitucional. Uma reação compreensível, mas juridicamente atacável, porquanto fundada numa ilusão de segurança hermenêutica.

Pelo exposto, urge sublinhar que é importante garantir que o que a Constituição protegia deverá continuar a proteger. Se a Constituição protege o direito à privacidade, o

facto de as novas tecnologias gerarem novas formas, mais eficazes e apetecíveis, de combate ao terrorismo ou de segurança de pessoas e bens, apenas reclama um esforço maior no sentido da procura de uma solução interpretativa apaziguante. O mesmo se diga do direito à proteção de dados perante dimensões valiosas das liberdades económicas. Cada uma dessas partes da Constituição, se as tomarmos como absolutas, conduz-nos a uma visão redutora e distorcida do ambiente jurídico-constitucional. Daí a relevância de uma interpretação constitucional tecnologicamente neutra[1], que salve a identidade constitucional, perante as adversidades tecnológicas. O que reclama flexibilidade na interpretação textual ou literal[2], uma tradução fiel dos valores constitucionais para a realidade do ciberespaço, paralela a uma incontornável interpretação atualista e evolutiva[3], sob pena de certas normas ou princípios constitucionais perderem a sua efetividade. Mas tendo sempre por limite a própria Constituição.

Tornou-se, indubitavelmente, um lugar-comum a afirmação de que a estabilidade constitucional não pode ser totalmente inflexível, porquanto uma Constituição também deve ser idónea para o futuro e modificada, caso se distancie da vontade geral[4]. Não obstante, a pressão regulatória das novas tecnologias, em que as instituições da UE mergulharam nos últimos anos, traduzida em *overdose* normativa e regulatória, não constitui causa derrogatória dos princípios constitucionais e do regime de proteção dos direitos, liberdades e garantias[5], à luz do qual são chamados à ponderação todos os bens eventualmente colidentes, desde que revistam dignidade constitucional. Nem as restrições de direitos fundamentais podem almejar sobreviver para além do estritamente necessário, conforme resultar de um escrutínio rigoroso, à luz do princípio da proporcionalidade.

Em que medida as presentes reflexões nos ajudam à interpretação e aplicação do RGPD?

---

1 BRÍZIDA CASTRO, Raquel Alexandra (2016) *Constituição, Lei e Regulação dos Media,* Almedina: Coimbra; pp. 99 e ss.

2 TRIBE, Lawrence H. (1991) "The Constitution in Cyberspace: Law and Liberty beyond The Electronic Frontier", *The Humanist*, Set-Oct; p. 15.

3 OTERO, Paulo (2010) *Direito Constitucional Português: Organização do Poder Político,* Vol. II, Almedina: Coimbra; p. 159.

4 STERN, Klaus (2008) "Desarrollo Constitucional Universal y Nuevas Constituciones", in *Dignidad de La Persona, Derechos Fundamentales, Justicia Constitucional*, Coord. Francisco Fernández Segado, Dykinson-Constitucional; p. 78.

5 Reserva de Lei (artigo 165.º, n.º 1, alínea b), da CRP); Reserva de Densificação Total; Proibição da Deslegalização (artigo 112.º, n.º 5, da CRP); Princípio da Aplicabilidade Direta (artigo 18.º, n.º 1, da CRP); Princípio da Concordância Prática (artigo 18.º, n. º2, 2.ª parte, da CRP); entre outros.

É que, por um lado, existe o próprio risco de uma leitura *hiperintegrada* do RGPD, no qual se confrontam direitos e valores fundamentais, sem legítima rendição absoluta e incondicional de qualquer um deles. Por outro lado, o RGPD não é um fim em si mesmo, nem a sua descida à terra fez brotar uma qualquer máxima hermenêutica de interpretação conforme ao RGPD.

São, efetivamente, "*ways not to read"* o Regulamento Geral de Proteção de Dados (RGPD):

i. O RGPD não criou um degrau especial e inédito na hierarquia das normas, vigente no ordenamento jurídico-constitucional português, nem fornece critérios de prevalência incondicional de quaisquer princípios, direito ou bem fundamentais, em caso de conflito;

ii. O RGPD não implica, na sua aplicação, o reconhecimento de que os direitos à proteção de dados pessoais, privacidade ou à autodeterminação informacional, inquilinos de longa data do texto constitucional, são, *a priori*, absolutos ou mais importantes do que os outros direitos ou bens fundamentais que com ele possam colidir: liberdade de expressão, direito à informação, liberdade de gestão e organização empresarial, liberdades económicas, etc.;

iii. As remissões normativas para os Estados Membros não constituem credencial habilitante da produção de normas legislativas nacionais contrárias às Constituições: o RGPD não aniquilou o princípio da constitucionalidade;

iv. O RGPD não retira competência de controlo de constitucionalidade aos tribunais comuns e, em última instância, em sede de fiscalização concreta, ao Tribunal Constitucional. Se uma norma que vigora na ordem jurídica portuguesa é inconstitucional, independentemente da forma, ela não deve ser aplicada pelos tribunais. E, em última instância, ainda que respeitadora do RGPD, se for

inconstitucional, deve ser erradicada do ordenamento jurídico, através da fiscalização sucessiva abstracta;

v. Apesar de o RGPD ser um Regulamento, os Estados membros estão a aprovar diversas legislações de execução diferentes. Sobra a fé e algum otimismo no mecanismo *One Stop Shop* e respetivo Procedimento de Coerência;

vi. O RGPD não é o único instrumento jurídico que regula o tratamento de dados pessoais com impacto nas pessoas e nas obrigações das empresas. Assistimos a uma infindável e perturbadora dispersão normativa na regulação do ciberespaço.

Os tópicos expostos são, para nós, imprescindíveis. E, para além do próprio RGPD, respetivas leis de execução e das Constituições dos Estados Membros, qualquer atividade interpretativa das regras de proteção de dados não pode deixar de ser impregnada pela Carta Europeia dos Direitos Fundamentais, jurisprudência do Tribunal de Justiça, Convenção Europeia dos Direitos do Homem, Recomendações do Conselho da Europa, o trabalho produzido pelo Grupo de Trabalho do Artigo 29.º e a produção da Comissão Nacional de Proteção de Dados, Autoridade Nacional de Controlo, e do Comité Europeu para a Proteção de Dados.

REGULAMENTO GERAL DE PROTEÇÃO DE DADOS:

PRINCIPAIS DIFICULDADES E DÚVIDAS DAS ORGANIZAÇÕES E DOS TITULARES DE DADOS PESSOAIS NA ADAPTAÇÃO AO ATUAL REGIME

LURDES DIAS ALVES [1]

1Mestre em Direito (especialidade de Ciências Jurídicas). Doutoranda em Direito na Universidade Autónoma de Lisboa, onde investiga o tema: "*A proteção de dados pessoais e o sigilo bancário – A derrogação da privacidade*". Investigadora integrada no RATIO LEGIS - UAL. Cocoordenadora de Cursos de Formação e Pós-Graduações em Proteção de Dados Pessoais, Privacidade e Cibersegurança na UE, na Autónoma. Contacto: lurdes.dias.alves@gmail.com

Com a publicação em 4 de maio de 2016, e entrada em vigor em 25 de maio de 2016, o Regulamento Geral de Proteção de Dados (RGPD) contemplou, desde logo, um período transitório de dois anos para a sua aplicação plena, no regulamento, são consagradas no quadro europeu profundas alterações ao regime jurídico da defesa da privacidade das pessoas singulares.

Os Estados, as pessoas coletivas públicas e privadas, as organizações e os agentes económicos tiveram até 25 de maio de 2018 para preparar a adaptação às novas regras de proteção de dados. Contudo, raramente, diremos, a adaptação a um novo regime decorre sem dificuldades e dúvidas.

Passados quase cinco meses de plena aplicabilidade do RGPD, considera-se pertinente efetuar uma breve reflexão sobre as principais dificuldades e dúvidas das organizações e dos titulares dos dados pessoais na adaptação ao atual regime, destacamos como principais preocupações: *COMPLIANCE* – Como aferir e provar o cumprimento do RGPD; a questão do regime de reporte e divulgação em caso de *data breach*; o estatuto e perfil do *Data Protection Officer*; a diversidade e multiplicidade dos pedidos de consentimento; o excesso de direito de acesso por parte do Estado dos dados pessoais dos cidadãos; e, mas não menos importante, a falta de literacia em matéria de proteção de dados pessoais.

Para uma maior clarificação destas dificuldades e dúvidas, efetuaremos uma reflexão de forma sucinta quanto às dificuldades das organizações, por um lado, e as principais dúvidas dos titulares dos dados pessoais, por outro.

I. AS PRINCIPAIS DIFICULDADES DAS ORGANIZAÇÕES NA ADAPTAÇÃO AO ATUAL REGIME DE PROTEÇÃO DE DADOS PESSOAIS

O RGPD alterou por completo o paradigma da regulação em matéria de proteção de dados pessoais, passando de hetero-regulação para autorregulação. Uma dessas alterações introduzidas é o fim do controlo prévio exercido pela Autoridade Nacional (no caso português, a Comissão Nacional de Proteção de Dados – CNPD). Assim, o tratamento de dados pessoais deixa de ter a obrigatoriedade de comunicação e/ou autorização prévia.

É sobre o responsável pelo tratamento dos dados pessoais de cada organização que impende a obrigatoriedade do cumprimento do regulamento, e mais ainda, o responsável pelo tratamento tem de provar o cumprimento.

A - *COMPLIANCE* – Como aferir e provar o cumprimento do RGPD

Na verdade, uma das principais dificuldades que as organizações enfrentam é como aferir e provar que cumprem o regulamento. Uma das novidades introduzida pelo RGPD é o conceito de Avaliação de Impacto sobre a Proteção de Dados – AIPD ou PIA – *Privacy Impact Assessment* (conforme texto original do regulamento).

Mas o que é uma AIPD? Trata-se de um processo concebido para descrever o tratamento, avaliar a necessidade e proporcionalidade desse tratamento e ajudar a gerir e prevenir os riscos para os direitos e liberdades dos titulares dos dados pessoas decorrentes do tratamento, avaliando-os e determinando as medidas necessárias para fazer face aos riscos. As AIPD constituem importantes instrumentos em matéria de responsabilização, ao auxiliarem os responsáveis pelo tratamento não apenas a cumprir os requisitos do RGPD, mas também a demonstrar que foram tomadas medidas adequadas para assegurar a conformidade com o regulamento (*i.e.* uma AIPD é um processo que visa aferir e provar a conformidade do tratamento de dados).

Porém, não é obrigatório realizar uma AIPD para todas as operações de tratamento. Só existe essa obrigação quando o tratamento for «*suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares*». Para aferir quais são as operações de tratamento «*suscetíveis de implicar um elevado risco*»,

devem ser considerados nove critérios: 1. Avaliação ou classificação, incluindo definição de perfis e previsão, em especial de «*aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados*»; 2. Decisões automatizadas que produzam efeitos jurídicos ou afetem significativamente de modo similar: tratamento destinado à tomada de decisões sobre os titulares dos dados e que produza «*efeitos jurídicos relativamente à pessoa singular*» ou que «*a afetem significativamente de forma similar*»; 3. Controlo sistemático: tratamento utilizado para observar, monitorizar ou controlar os titulares dos dados, incluindo dados recolhidos através de redes, ou um «*controlo sistemático de zonas acessíveis ao público*»; 4. Dados sensíveis ou dados de natureza altamente pessoal: inclui categorias especiais de dados pessoais (definido nos art.ºs 9.º e 10.º do RGPD); 5. Dados tratados em grande escala: (*v.g.* a) o número de titulares de dados envolvidos, quer através de um número específico quer através de uma percentagem da população pertinente; b) o volume de dados e/ou a diversidade de dados diferentes a tratar; c) a duração da atividade de tratamento de dados ou a sua pertinência; d) a dimensão geográfica da atividade de tratamento.) 6. Estabelecer correspondências ou combinar conjuntos de dados: (*v.g.* dados de duas ou mais operações de tratamento, com diferentes finalidades e/ou efetuadas por diferentes responsáveis pelo tratamento de dados de tal forma que excedam as expectativas razoáveis do titular dos dados aquando do consentimento); 7. Dados relativos a titulares de dados vulneráveis: o tratamento deste tipo de dados constitui um critério devido ao acentuado desequilíbrio de poder entre os titulares dos dados e o responsável pelo tratamento dos dados, significando isto que os indivíduos podem não ser capazes de consentir, ou opor-se, facilmente ao tratamento dos seus dados ou de exercer os seus direitos (*v.g.* dados de crianças; dados dos trabalhadores no contexto laboral; pessoas com doenças mentais; requerentes de asilo; idosos; doentes, etc.); 8. Utilização de soluções inovadoras ou aplicação de novas soluções tecnológicas ou organizacionais (*v.g.* a utilização da impressão digital e do reconhecimento facial para melhorar o controlo do acesso físico, etc.), aliás, o RGPD alerta que a utilização de uma nova tecnologia pode implicar a obrigatoriedade de realização de uma AIPD; 9. Quando o próprio tratamento impede os titulares dos dados de exercer um direito ou de utilizar um serviço ou um contrato (*v.g.* numa operação de tratamento destinada a autorizar, alterar ou recusar o acesso dos titulares dos dados a um serviço ou que estes celebrem um contrato.

Impõe-se que seja desmistificada a obrigatoriedade sistemática de uma AIPD, desde logo porque os responsáveis pelo tratamento de dados devem encarar a realização de uma AIPD como uma avaliação útil e positiva que ajusta o tratamento de dados efetuado com a conformidade jurídica, ao invés de a encararem como um custo adicional e uma tarefa desnecessária.

B - A questão do regime de reporte e divulgação em caso de *data breach*

Uma outra questão, não menos relevante, que tem gerado grande preocupação e dificuldade, é a que concerne a melhor interpretação do prazo máximo de 72 horas estabelecido para comunicação e reporte de falhas ou violação de dados (*data breach* no texto original do regulamento). Note-se que é consensual considerar a falta de reporte e comunicação de falhas ou violação de dados uma das questões passíveis de levar à aplicação das sanções elevadas, as quais podem facilmente ascender a 20 milhões de euros.

O problema reside essencialmente na interpretação de «quando é que um responsável pelo tratamento tem conhecimento de *data breach*, qual o momento que se deve ter em conta para a notificação?». Deverá considerar-se que um responsável pelo tratamento tem «conhecimento» quando tem um grau razoável de certeza de que ocorreu um incidente de segurança que afetou dados pessoais. Porque o RGPD exige que o responsável pelo tratamento aplique todas as medidas técnicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação e para informar rapidamente a autoridade de controlo e os titulares dos dados. Deverá ainda comprovar que a notificação foi enviada sem demora injustificada e importa ter em conta, em especial, a natureza e a gravidade da violação e as respetivas consequências e efeitos adversos para o titular dos dados.

Em caso de *data breach* o responsável pelo tratamento fica obrigado a assegurar que terá, sempre, «conhecimento» de eventuais violações em tempo útil, para que possa tomar medidas adequadas. O que não se mostra de difícil apuramento e muito menos impossível, até porque as circunstâncias de uma violação irão ditar as condições exatas em que se pode considerar que um responsável pelo tratamento tem «conhecimento» dessa violação. Casos há em que é relativamente evidente desde o início se tal ocorreu.

Todavia, a maior preocupação não deve ser centrada na prova de momento do «conhecimento» da violação de dados, mas sim na ação imediata para investigar o incidente, o que originou a falha ou violação, a fim de determinar se os dados pessoais foram de facto violados e tomar medidas de reparação e notificação.

C - O estatuto e perfil do *Data Protection Officer*

Outro conceito introduzido é a figura do Encarregado de Proteção de Dados – EPD (ou *Data Protection Officer* como é definido no texto original do regulamento). Esta nova figura tem criado sérias dúvidas nas organizações quanto à obrigatoriedade da sua designação; se um único grupo organizacional tem de nomear um único EPD ou um para cada organização; se tem de ser interno ou externo; em que local terá de estar domiciliado; quais os requisitos e qualidades profissionais; quais os recursos que o responsável pelo tratamento de dados deverá disponibilizar ao EPD; quais as salvaguardas ao dispor do EPD para desempenhar as suas funções com independência; qual a responsabilidade do EPD em caso de incumprimento dos requisitos impostos pelo RGPD; qual o papel do EPD numa AIPD – tudo isto entre outras dúvidas com que as organizações se têm deparado.

Desde logo, só é obrigatória a designação de um EPD, se: o tratamento for efetuado por autoridade ou organismo público (exceto os tribunais no exercício da sua função jurisdicional); as atividades principais do responsável pelo tratamento ou do subcontratante consistirem em operações de tratamento que exijam controlo regular e sistemático dos titulares dos dados em grande escala; e se as atividades principais do responsável pelo tratamento ou do subcontratante consistirem em operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infrações. Ainda assim, mesmo que não seja obrigatório designar um EPD, as organizações poderão considerar conveniente designar um EPD, a título voluntário.

Ressalva-se que um grupo empresarial ou organizacional pode designar um único EPD, desde que este esteja «*facilmente acessível a partir de cada estabelecimento*». O requisito essencial é exatamente a acessibilidade: o EPD tem de estar acessível e contactável em relação aos titulares dos dados, à autoridade de controlo e, naturalmente, à organização ou grupo organizacional.

O EPD pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante (EPD interno), ou exercer as suas funções com base num contrato de prestação de serviços (EPD externo). E, para que se assegure que o EPD esteja acessível, é aconselhável que esteja domiciliado na União Europeia.

Deve ser designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio das normas e práticas de proteção de dados, bem como na sua capacidade para desempenhar as respetivas funções. Salienta-se que deve ter competências no domínio das normas e práticas de proteção de dados nacionais e europeias, incluindo um conhecimento profundo do RGPD, e conhecimentos das operações de tratamento efetuadas, das tecnologias da informação e da segurança dos dados e do setor empresarial e da organização; finalmente, é importante que tenha a capacidade para promover uma cultura de proteção de dados no seio da organização.

Para que o EPD desempenhe as suas funções com total independência é necessário que os responsáveis pelo tratamento ou subcontratantes não transmitam instruções relativas ao exercício das funções do EPD. Acresce que o responsável pelo tratamento não pode destituir nem penalizar o EPD pelo exercício das suas funções. Geralmente, os cargos suscetíveis de gerar conflitos com o EPD no seio da organização podem incluir não só os cargos de gestão superiores (*v.g.* diretor executivo, diretor de operações, diretor financeiro, diretor do departamento médico, diretor de marketing, diretor dos recursos humanos ou diretor informático).

Ao EPD devem ser facultados os recursos necessários ao desempenho das suas funções face à natureza das operações de tratamento e das atividades e dimensão da organização (*i.e.*: apoio ativo às funções do EPD por parte dos quadros de gestão superiores; tempo suficiente para que os EPD desempenhem as suas tarefas; apoio adequado em termos de recursos financeiros, infraestruturas e pessoal adstrito à sua equipe de trabalho; deve ser comunicada oficialmente a nomeação do EPD a todo o pessoal; acesso a outros serviços no seio da organização, para que o EPD possa receber apoio, contributos ou informações essenciais por parte destes outros serviços; tem igual relevância a garantia de formação contínua).

Atente-se que o EPD não é pessoalmente responsável pelo incumprimento dos requisitos de proteção de dados: compete ao responsável pelo tratamento ou ao

subcontratante assegurar e poder comprovar que o tratamento respeita o Regulamento aplicável. Porém, relativamente à avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento ou o subcontratante deve solicitar o parecer do EPD, sempre que seja questionado se se deve ou não efetuar a AIPD; qual a metodologia a seguir na realização da AIPD; se deve realizar a AIPD internamente ou externalizá-la; quais as salvaguardas (incluindo medidas técnicas e organizativas) a aplicar no sentido de atenuar os eventuais riscos para os direitos e interesses dos titulares de dados; se a avaliação de impacto sobre a proteção de dados foi ou não corretamente efetuada e se as suas conclusões (se o tratamento deve ou não ser realizado e quais as salvaguardas a aplicar) estão em conformidade com os requisitos de proteção de dados.

II. AS DÚVIDAS DOS TITULARES DE DADOS PESSOAIS

O RGPD, apesar de encerrar em si muitos princípios, regras gerais, direitos e obrigações que já constavam da Diretiva 95/46/CE, veio introduzir importantes alterações: entre outras, e talvez a mais notória em termos jurídicos, temos o grau de intensificação do processo e requisitos aplicáveis à obtenção do consentimento do titular de dados pessoais nas mais diversas operações de tratamento de dados, fomentando a obrigatoriedade de demonstrar se o consentimento obtido pelo responsável pelo tratamento, e se respeita todos os novos requisitos – em caso negativo, será imprescindível obter novo consentimento do titular dos dados pessoais em conformidade com as disposições do RGPD, sob pena de o tratamento se tornar ilícito por falta de fundamento jurídico.

A - A diversidade e multiplicidade dos pedidos de consentimento

Um pedido de consentimento tem de ser apresentado ao titular dos dados pessoais de forma clara e concisa, utilizando uma linguagem de fácil compreensão, e de modo que o distinga claramente de outras informações, como os termos e condições do serviço. O pedido tem de especificar qual a utilização que será dada aos dados pessoais recolhidos e tem de incluir os contactos do responsável pelo tratamento de dados.

Atente-se, pois, que a legitimidade para o tratamento de dados pessoais advém da licitude na obtenção do consentimento do titular dos dados, e este consentimento somente é lícito - logo válido - se corresponder a uma *manifestação de vontade*, *livre*, específica, *informada* e *explícita*, pela qual o titular dos dados aceita o tratamento *mediante declaração* ou *ato positivo inequívoco*.

Conforme estabelece o n.º 1 do art.º 6.º do RGPD quanto aos requisitos conducentes à verificação da licitude para o tratamento de dados pessoais, o tratamento é lícito se o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas. E se o tratamento for necessário para: **(i)** a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; **(ii)** o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; **(iii)** a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; **(iv)** o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; **(v)** efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

Para que se considere que o consentimento é informado, o responsável pelo tratamento tem de demonstrar que o titular dos dados recebeu, pelo menos, as seguintes informações sobre o tratamento: **a)** a identidade do responsável pelo tratamento dos dados; **b)** os fins para os quais os dados irão ser tratados; **c)** o tipo de dados que serão tratados; **d)** a possibilidade de retirar o consentimento dado (v.g., enviando uma mensagem de correio eletrónico para retirar o consentimento); **e)** se aplicável, o facto de os dados irem ser utilizados para decisões exclusivamente automatizadas, incluindo a definição de perfis; **f)** informações destinadas a apurar se o consentimento está relacionado com uma transferência internacional dos dados, os possíveis riscos de transferências de dados para fora da UE se tais países não estiverem sujeitos a uma decisão de adequação da Comissão e não existirem garantias adequadas.

Os titulares dos dados pessoais têm, de facto, sido confrontados com inúmeros, diremos demasiados, pedidos de consentimento, muitos dos quais desnecessários e que refletem as dificuldades e dúvidas por parte dos responsáveis pelo tratamento; a este propósito, diga-se que, se o consentimento dado por uma pessoa antes do RGPD ser

aplicável estiver em conformidade com as condições e os requisitos do regulamento, não é necessário ser solicitado de novo o consentimento. Só é necessário um novo consentimento se a organização obteve o consentimento dos seus clientes há alguns anos utilizando um sistema de opções pré-validadas *online*. Este modelo de obtenção de consentimento deixou de ser válido em 25 de maio de 2018 - logo, o responsável pelo tratamento terá de obter um novo consentimento, caso pretenda continuar a efetuar o tratamento dos dados.

B - O excesso de direito de acesso por parte do Estado dos dados pessoais dos cidadãos

Se por um lado aplaudimos o cruzamento de informação na administração pública com vista à celeridade processual, por outro lado, este cruzamento de informação não mais é que uma transmissão de dados de uma organização para outra, sendo que o consentimento dado pelo titular dos dados tinha uma finalidade diversa daquela que se verifica após a transmissão de dados.

Na maioria das vezes estão em causa dados pessoais sensíveis (*v.g.* dados de saúde, dados genéticos, dados familiares, dados de crédito e solvabilidade, entre outros não menos importantes) que requerem uma proteção jurídica acrescida pela natureza dos direitos fundamentais em causa.

A maior dúvida neste âmbito reside primordialmente na ausência (por completo ou parcial) do nível de acesso, por parte dos funcionários da administração pública, a dados referentes à reserva da intimidade da vida privada e familiar.

C - A falta de literacia em matéria de proteção de dados pessoais

É indubitável que vivemos numa sociedade assente na tecnologia – e, por exemplo, basta pensar nas câmaras de videovigilância em grande parte do espaço público e privado; no modo como as instituições de crédito e sociedades financeiras sabem onde e como gastamos o nosso dinheiro (mais ainda, sabem como o ganhamos); como as grandes superfícies sabem os produtos que consumimos, quais os nossos gostos e tendências, ao ponto de poderem definir um perfil pessoal dos nossos hábitos e rotinas; os «*radares*» e a «*via verde*», que sabem por onde nos deslocamos e para

onde viajamos; máquinas de «*raio X*» nos aeroportos, que visualizam os nossos pertences (e até o nosso corpo); a utilização de «*cookies*», que permite determinar a nossa utilização e navegação na internet (a tão usualmente designada pegada digital) - estas, entre muitas outras situações, mostram a variedade de casos em que, voluntária ou involuntariamente, a nossa privacidade fica mitigada ou até mesmo comprometida.

Nos últimos anos tem-se assistido a um crescimento exponencial do volume de dados gerados por sistemas de informação, ligados em rede e que geram dados, de tráfego e de conteúdo, interligados e a uma velocidade não antes imaginável. Com efeito, o elevado número de recolha, tratamento e troca de dados pessoais que atualmente ocorre, advém da maior disponibilização de informações privadas, cedidas, voluntária ou involuntariamente, pelas próprias pessoas (pelos próprios titulares dos dados pessoais), nomeadamente nas redes sociais.

Atualmente, em todo o mundo, sobretudo nos países desenvolvidos, os cidadãos não só são perseguidos continuamente no dia-a-dia, como consentem, de livre vontade, na divulgação dos seus próprios dados, satisfazendo o «*voyeurismo*» da sociedade contemporânea. Não restem dúvidas: nas últimas décadas assistimos a uma revolução digital que tornou a sociedade numa sociedade de informação, mas também de exposição.

A tutela da vida privada exige, hoje, mais transparência e controlo no concernente ao tratamento de dados por empresas e autoridades públicas. Ainda assim, teremos de levar em linha de conta os comportamentos das pessoas, que paradoxalmente estão menos cientes do seu direito à privacidade, permitindo a divulgação, e divulgando ela mesmo, informações pessoais, sem consciência das reais implicações dos seus atos, em redes totalmente abertas, nas quais não há controlo nem fiscalização.

Consideramos que, é imprescindível sensibilizar os indivíduos para a autoproteção da privacidade; os utilizadores das novas tecnologias devem estar cientes dos perigos que estas comportam e, nomeadamente, devem ter consciência de que a divulgação de informações em redes abertas escapa ao seu controlo. Os seus dados, uma vez disponibilizados, estão para sempre disponíveis. Por isso mesmo, a privacidade, uma vez perdida, está perdida para sempre. Por isso, as novas tecnologias de informação impõem que o direito à privacidade seja repensado e reconfigurado como um direito ao anonimato.

De facto, nesta sociedade cada vez mais aberta, e adepta da era digital, onde se expõe com toda a abertura a vida privada, e até a vida familiar, deixou de fazer sentido a privacidade, tal como a conhecemos. Na verdade, assistimos a mudanças de mentalidade e de comportamento social em que o valor da proteção da privacidade deixou de ser um «*bem supremo*», deixando até desvanecer a noção e o valor de que a privacidade é um direito inerentemente humano e um pré-requisito para a manutenção da condição humana com dignidade e respeito. Cumpre, pois, refletir sobre a dimensão, jurídica, ética e social, desta realidade.

ANÁLISE BREVE DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA (*LGPD*) :

QUE IMPACTO TRAZ AOS NEGÓCIOS E ÀS PESSOAS?

VALÉRIA REANI RODRIGUES GARCIA [1]

1 Advogada, OAB/SP, Brasil. Especialista em Direito e Privacidade de Dados pela UNL - Universidade Nova Lisboa; em Direito Digital e "*Compliance"* – Faculdade Damásio; e em Direito Empresarial – PUC-Campinas-Pontifica Universidade Católica de Campinas. Coordenadora Pedagógica Científica e Docente dos Cursos de Direito Digital e Inovação da ESA- Escola Superior de Advocacia de Santos, Santo André e Campinas.
Contacto: valeriareani@primoecampos.com.br

INTRODUÇÃO

No dia 10 de julho de 2018, foi aprovado no plenário do Senado Federal o PLC 53/2018, o qual dispõe sobre a proteção de dados pessoais e altera a Lei 12.965/16 (Marco Civil da Internet), consolidando-se assim como a Lei Geral de Proteção de Dados brasileira (LGPD) [2].

A lei cria um novo regramento para o uso de dados pessoais no Brasil, tanto no âmbito *online q*uanto *offline,* nos setores privados e públicos, de forma a reforçar e complementar, a Legislação setorial, que já tratava de privacidade, como a própria Constituição Federal, Código de defesa do Consumidor, Código Civil e Marco Civil da Internet do Brasil, que justamente

2 Há mais 30 diplomas legais sobre o assunto – aí se inclui a própria Constituição Federal, o Marco Civil da Internet, Código de Defesa do Consumidor, Lei de Acesso à Informação, Lei do Cadastro Positivo, Código Civil. Na Constituição Federal logo em seu art. 1o, III, preceitua que um dos fundamentos do Estado Brasileiro é a dignidade da pessoa humana, para alguns doutrinadores, esse princípio é a guia para a tutela efetiva de todos os direitos fundamentais contidos na Carta Magna de 1988. Mais a frente, no mesmo diploma legal, em seu art. 5o, X, preceitua que "*são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*", ficando evidente a proteção dos direitos da personalidade, que também ficam claros no art. 21 do Código Civil, ao preceituar que "*A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma*", protegendo a intimidade e a vida privada, possuindo grande ligação com a questão da proteção dos dados pessoais sob a ótica européia, consubstanciada no art. 8, no 1 da Carta dos Direitos Fundamentais da União Européia.
A lei 8.078/90, Código de Defesa do Consumidor, em seu art. 43, trata da questão do acesso por parte do consumidor aos dados pessoais que estejam arquivados – "*O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes*", mostrando uma preocupação do legislador com essa questão, sendo que o referido artigo do CDC possui forte ligação com o art. 5o LXXII, ao prever o remédio constitucional conhecido como *habeas data,* ao preceituar que*: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo*. O remédio constitucional do Habeas Data não se mostrou de grande efetividade e eficácia no ordenamento jurídico pátrio, sendo pouco utilizado, sendo questionado, por alguns doutrinadores sobre a sua real importância como tutela efetiva de proteção de dados pessoais. Mais recentemente ocorreu a entrada em vigor da Lei 12.965/ 14, o Marco Civil da Internet, que poderia ter resolvido, de certa forma, esse vácuo legislativo existente no Brasil, já que o arcabouço jurídico pátrio não possui norma efetiva que tutele a proteção de dados pessoais e seu tratamento, porém limitou-se a tratar de forma tímida em seu art. 11 a questão da proteção dos dados pessoais, deixando, ainda, um campo aberto para regulação. Lei de Acesso à Informação (LAI), Lei nº 12.527/2011, decorrente do art. 5º, XXXIII, art. 37, § 3º, II e o art. 216, § 2º, todos da CF/88, com o direito constitucional da privacidade. O primeiro possibilita o recebimento de informações públicas dos órgãos estatais e propicia maior liberdade de opinião e de expressão. Enquanto o segundo protege e assegura os direitos à privacidade e à intimidade que provêm da própria natureza humana e daí o seu caráter inviolável, intemporal e universal, impedindo a devassa nas informações de cunho estritamente pessoal.

por ser setorial, trazia insegurança jurídica e tornava o país menos competitivo no contexto econômico Global cada vez mais movido a dados.

I. QUAL O OBJETIVO DA LEI GERAL DE PROTEÇÃO DE DADOS?

A lei objetiva garantir ao cidadão:

Direito à privacidade: garantir o direito à privacidade e à proteção de dados pessoais dos cidadãos ao permitir um maior controle sobre seus dados, por meio de práticas transparentes e seguras, visando garantir direitos e liberdades fundamentais.

Regras claras para empresas: estabelecer regras claras sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais para empresas.

Promover desenvolvimento: fomentar o desenvolvimento econômico e tecnológico numa sociedade movida a dados.

Direito do consumidor: garantir a livre iniciativa, a livre concorrência e a defesa do consumidor.

Fortalecer confiança: aumentar a confiança da sociedade na coleta e uso dos seus dados pessoais.

Segurança jurídica: aumentar a segurança jurídica como um todo no uso e tratamento de dados pessoais.

II. A IMPORTÂNCIA DE UMA LEI GERAL DE PROTEÇÃO DE DADOS:

Unificar regras: regras únicas e harmônicas sobre o uso de dados pessoais, independente do setor da economia.

Adequar as regras no Brasil: tornar o Brasil apto a processar dados oriundos de países que exigem um nível de proteção de dados adequados, o que pode fomentar, principalmente, os setores de tecnologia da informação.

Portabilidade: indivíduos poderão transferir seus dados de um serviço para outro, aumentando a competitividade no mercado.

III. A LGPD

A LGPD tem aplicação tanto no âmbito público e privado, *online* e *offline*. Ela versa sobre o conceito de dados pessoais;

- lista as bases legais que autorizam o seu uso a exemplo do consentimento, do titular dos dados pessoais, permitindo o uso de dados com base no legítimo interesse do controlador dos dados;
- Trata de princípios gerais, direitos básicos do titular – como acesso, exclusão dos dados e explicação sobre uso – obrigações e limites que devem ser aplicadas a toda entidade que se vale do uso de dados pessoais, seja como insumo do seu modelo de negócio, seja para a atividade de seus colaboradores.

IV. PRINCIPAIS PONTOS DA LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

- Aplicação transversal, multissetorial, a todos os setores da economia, tanto no âmbito público quanto privado, *online* e *offline*. Trocando em mudos, e a poucas exceções, toda e qualquer prática que se valer do uso de dados pessoais estará sujeita à lei.

- Aplicação extraterritorial: em moldes similares à regulamentação europeia, a ***General Data Protection Regulation*** - **GDPR,** a Lei Geral, ou seja, o dever de conformidade superará os limites geográficos do país. Toda empresa estrangeira que, com filial no Brasil, ou oferecer serviços ao mercado nacional e coletar e tratar dados de pessoais naturais localizadas no país estará sujeita à nova lei.

- Traz conceito amplo do que deve ser considerado dado pessoal informação relacionada à pessoa natural/física, identificada ou identificável. Ou seja, qualquer dado, que isoladamente ou agregado a outro possa permitir a identificação de uma pessoa natural, ou sujeitá-la a um determinado comportamento.

- Define **dados pessoais sensíveis**, como aqueles que pela sua própria natureza podem sujeitar o seu titular a práticas discriminatórias, tais como dados sobre a origem racial ou étnica, a convicção religiosa, a opinião política, dado referente à saúde ou à vida sexual; ou permitir a sua identificação de forma inequívoca e persistente, tais como dado genético ou biométrico. Por sua peculiaridade tais dados devem ser tratados de forma diferenciada, segurança adicionais.

- Conceitua dados **anonimizados** que seriam os relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Dados efetivamente anonimizados são essenciais para o funcionamento de tecnologias e na da Internet das Coisas, inteligência artificial, ***machine learning, smart cities***.

- Fala também de dados públicos, tais como os constantes de bases geridas por órgãos públicos, publicações oficiais e cartórios, ou os expressamente tornados públicos pelos seus titulares, como em perfis públicos em redes, ficando o uso desses dados, limitado às finalidades.

V. PROTEÇÃO DOS DADOS PESSOAIS DE CRIANÇAS?

Sim. A Lei estabelece que um termo de privacidade deverá existir toda vez que forem solicitados dados pessoais, seja nas plataformas *online* ou em lojas físicas, clínicas de saúde, entre outros estabelecimentos, objetivando manter a integridade dos pequenos, como nome, endereço, escolaridade, entre outros, que só poderão ser usados pelas empresas após consentimento dos responsáveis dos menores de 12. Maiores de 12 anos poderão consentir, desde que entendam do que se trata aquele termo. Por isso, eles devem ter linguagem clara e acessível.

VI. A LGPD LISTA 10 PRINCÍPIOS/razões que devem ser levados em consideração no tratamento de dados pessoais, tais como:

1) **Finalidade**: propósito legítimo para uso dos dados pessoais;

2) **Adequação**: compatibilidade de tratamento com a finalidade;

3) **Necessidade**: Uso e tratamento dos dados deve ser restrito ao mínimo necessário;

4) **Livre acesso**: garantia de consulta facilitada e gratuita sobre a integralidade de dados, forma e duração do tratamento;

5) **Qualidade dos dado**s: garantia de exatidão, clareza, relevância e atualização dos dados de acordo com a finalidade de seu tratamento:

6) **Transparência:** garantia de informação precisa sobre o tratamento dados;

7) **Segurança:** utilização de medidas técnicas capazes de garantir a Segurança do tratamento;

8) **Prevenção:** adoção de medidas para prevenir a ocorrência de danos, em função do tratamento inadequado;

9) **Não discriminação**: impossibilidade de tratamento para fins discriminatórios, ilícitos e abusivos;

10) **A responsabilização e prestação de contas**, que obriga o responsável pelo tratamento dos dados pessoais a demonstrar de forma cabal e transparente a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais previstas na lei.

VII. QUAIS SÃO OS DIREITOS BÁSICOS DOS TITULARES DE DADOS:

Dentre os direitos listados, destaca-se o de acesso aos dados, retificação, cancelamento ou exclusão, oposição ao tratamento, de informação e explicação sobre o uso dos dados. A grande novidade é o direito à portabilidade dos dados que, similar ao GDPR, pode ser feito entre diferentes empresas de telefonia e bancos, permite ao titular não só requisitar uma cópia da integralidade dos seus dados que facilite a transferência destes para outros serviços, mesmo para concorrentes.

Devido a sua natureza, este novo direito tem sido encarado como um forte elemento de competição entre diferentes empresas que oferecem serviços similares baseados no uso de dados pessoais.

Responsabilidade dos agentes de tratamento: os diferentes agentes envolvidos no tratamento de dados – o controlador e o operador – podem ser solidariamente responsabilizados por incidentes de segurança da informação e/ou o uso indevido e não autorizado dos dados, ou

pela não conformidade com a lei. Ressalte-se que a LGPD, determina a nomeação de um *Data Protection Officer* (DPO), cuja tradução e " encarregado", responsável pelo tratamento de dados pessoais dentro da organização.

VIII. QUAL O IMPACTO NOS NEGÓCIOS E ATIVIDADES?

A LGDP não afeta somente os grandes *players* do setor de tecnologia e serviços *online*, como aqueles oferecidos pelo *Google* e *Facebook*, mas também qualquer organização que realize uma operação de coleta, uso, processamento e armazenamento de dados pessoais.

Exemplos de aplicação da lei:

- Tratamento de dados no âmbito de atividades de bancos, corretoras, seguradoras, clinicas médicas, hospitais, e-commerce, varejo, hotéis, companhias aéreas, agências de viagens, restaurantes, academias, entre muitas outras, podem estar sujeitas a aplicação da lei, ainda que tais atividades ocorram exclusivamente fora do ambiente digital.

- Tratamento de dados pessoais em relações de clientes e fornecedores de produtos e serviços, prestadores e tomadores de serviços, empregados e empregadores, e demais relações nas quais dados pessoais sejam recebidos, enviados e/ou processados.

IX. QUEM ESTÁ SUJEITO A LGPD? QUAIS REGRAS DEVEM SER OBSERVADAS PELAS EMPRESAS DO SETOR PÚBLICO E PRIVADO?

De modo geral, a LGPD estabelece regras detalhadas que regulam qualquer operação de tratamento de dados, realizada por pessoas físicas ou jurídicas, no setor público ou privado e estabelece uma série de obrigações:

- a definição e documentação da base legal que autoriza o tratamento de dados (que podem incluir, mas não se limitam, a definir se o tratamento é realizado com base no consentimento, para fins de cumprimento de obrigação legal, para a execução de contrato, ou com base no interesses legítimo);

- o atendimento aos direitos concedidos aos titulares de dados, como o direito de obter informações sobre o tratamento de dados, realizar o acesso, retificação e eliminação de dados, direito à portabilidade a outro fornecer de produtos e serviços e obter a revisão de decisões automatizadas, dentre outros;
- a nomeação de um ENCARREGADO ou *Data Protection Officer* (DPO), responsável pelo tratamento de dados pessoais dentro da organização;
- a notificação a autoridade competente, em caso de incidente (divulgação e/ou uso não autorizado de dados pessoais);
- a adoção de medidas de (organizacionais e técnicas para) proteção de dados, a partir da criação de qualquer nova tecnologia ou produto (*privacy by design*); e,
- adequação das hipóteses que autorizam a transferência de dados para fora do país, quando aplicável.

X. QUAIS INFORMAÇÕES SÃO CONSIDERADAS COMO DADOS PESSOAIS?

Dados pessoais podem compreender qualquer informação relacionada à uma pessoa natural, identificada ou identificável. Neste sentido, dados de pessoas jurídicas não são cobertos pela LGPD, mas somente informações relacionadas às pessoas físicas. Um segundo aspecto importante é relacionado ao fato de que dados pessoais podem consistir em qualquer informação de pessoas identificadas ou identificáveis. **Dados pessoais de indivíduos identificados são aquelas informações que imediatamente podem identificar uma pessoa, como o nome, número de CPF e RG e informações de documentos pessoais**. Por outro lado, dados pessoais de indivíduos identificáveis são aquelas informações que não podem imediatamente identificar um indivíduo, mas que, ao serem alocadas juntamente com outras, podem passar a identificar e serem relacionadas a um indivíduo.

A LGPD regula o tratamento de dados pessoais em relações de clientes e fornecedores de produtos e serviços, prestadores e tomadores de serviços, empregados e empregadores, e demais relações nas quais dados pessoais sejam recebidos, enviados e/ou processados.

XI. AS ATIVIDADES DE PROCESSAMENTO DE DADOS DENTRO E FORA DO PAÍS ESTÃO SUJEITAS A LEI?

Operações de tratamento de dados realizadas dentro do território brasileiro estão sujeitas a aplicação da LGDP. Além de operações de tratamento realizadas dentro do país, quando o tratamento tiver por objetivo a oferta ou fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território brasileiro, a lei também pode se aplicar, ainda que a organização responsável por essa atividade esteja sediada ou localizada fora do país. Assim, o local onde os dados são tratados não é requisito único ou preponderante para aplicação da lei, sendo também importante identificar a localização do indivíduo cujos dados serão coletados.

XII. QUEM NÃO ESTÁ SUJEITO A LEI?

O uso pessoal para fins particulares e não econômicos, para fins jornalísticos, artísticos ou acadêmicos, não estão dentro do escopo da lei e, portanto, aos requisitos de tratamento de dados. Da mesma forma, o tratamento de dados para fins de segurança pública, defesa nacional, segurança do estado e/ou atividades de investigação e repressão de infrações penais também não estão sujeitos a LGPD, e estão sujeitos a regulação de legislação específica no tema. Dados provenientes e destinados a outros países, que apenas transitem pelo território nacional, sem que aqui seja realizada qualquer operação de tratamento podem eventualmente não estar sujeitos a aplicação da lei.

XIII. QUAL O RISCO DO NÃO CUMPRIMENTO DA LEI?

As penalidades por descumprimento da LGPD incluem advertência, obrigação de divulgação do incidente, eliminação de dados pessoais, bloqueio, suspensão e/ou proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados pessoais, multa, chegando ao valor limite de R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

Por fim, desde o último dia 14 de agosto o Brasil passou a ter não somente uma importante legislação específica que regulamenta o tratamento de dados pessoais, tanto pelo poder público quanto pela iniciativa privada que traz as novas regras criadas como meio de fortalecer a proteção da privacidade dos usuários, como também um grande desafio técnico, jurídico e cultural.

O “vacatio legis” é de 18 (dezoito) meses de sua publicação oficial, isto quer dizer que o interregno para a estruturação empresarial privado e público acontece nos próximos 18 meses, quando entrará em vigor a lei, mais precisamente, em fevereiro de 2020.

CONCLUSÃO

Assim, o Brasil conta com uma robusta legislação em termos de proteção de dados pessoais, o que possivelmente aprimorará o desenvolvimento tecnológico, práticas de negócios, crescimento do mercado digital e ao mesmo tempo proteção aos dados pessoais dos cidadãos em nosso país.

Outrossim, (logo que regularizada essa questão vetada) um cuidado que se deve ter, é com a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela supervisão, fiscalização e a disseminação de boas práticas entre as empresas públicas e privadas, sob pena de ausência de confiança do mercado, priorize um engajamento construtivo com a indústria, no seguinte sentido de que ao invés de inquisição e sanção, dar prioridade ao diálogo, apoio, mutua cooperação, orientação, conscientização e informação; além de estimular relações abertas e construtivas com negócios que lidem com dados pessoais, primando pela boa-fé das empresas e nos seus esforços em cumprir a lei; bem como propiciar a criação de ambientes para inovações responsáveis, como *"Regulatory Sandboxes"*, nos quais novos projetos podem ser testados em atmosferas controladas visando avaliar eventuais e futuras necessidades regulatórias, conforme o caso, mas *a posteriori*.

Salienta-se que as empresas que demonstrem vanguarda na adequação da LGPD, em agir de forma responsável, sejam encorajadas a demonstrar seus programas de privacidade, segurança da informação, códigos de conduta e gerenciamento de risco, visando gerar o reconhecimento do mercado por suas boas práticas, incluindo certificações, entre outros padrões de "*accountability".*

As sanções devem ser a "*ultima ratio*", principalmente e somente quando houver alguma violação dolosa, ou práticas exponencialmente negligentes, condutas reiteradas ou extremamente graves.

Ter um órgão controlador de todo esse processo é ideal e essencial para que ele seja sempre gerenciado conforme a lei. No entanto, enquanto uma nova agência é criada pelo Executivo e enquanto as empresas estão em período de preparação e adaptação às novas mudanças, é possível ir tomando medidas de auditorias dentro das próprias empresas sobre seus dados atuais, além da possibilidade da contratação de um ENCARREGADO – já que, assim, o oficial de dados atribui a responsabilidade de processadores e controladores de informações à uma pessoa.

Embora esse trabalho seja difícil e, muitas vezes, complexo, o desafio das empresas de estar em conformidade com a lei é importante e pode se tornar uma vantagem competitiva mais para a frente. Por isso, é importante olharmos para os passos que devem ser feitos até que ela se concretize, pensando sempre na importância da análise e de uma auditoria que controle a empresa, evitando que esteja fora da regulamentação.

Finalmente, é com muita satisfação que vejo a aprovação da nossa LGPD, trazendo um equilíbrio entre interesses sociais e econômicos; entre o poder público e o privado; entre liberdade, proteção e segurança, buscando tutelar, ao mesmo tempo, a proteção de dados pessoais, a dignidade da pessoa humana, a privacidade, a honra e a imagem das pessoas, assim como a livre iniciativa e o uso econômico dos dados, de forma legítima, séria, responsável, proporcional e razoável.

Referência Bibliográfica

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 - Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

CYBERLAW

by CIJIC

DOUTRINA

CYBERLAW by CIJIC

O "DIREITO À DESINDEXAÇÃO" DOS CONTEÚDOS OFENSIVOS NA INTERNET

The "right of deindexation": Repercussions of the González vs Google Spain case

MARCOS WACHOWICZ [1]

e

PEDRO HENRIQUE MACHADO DA LUZ [2]

1Professor de Direito da Universidade Federal do Paraná/Brasil. Doutor em Direito pela Universidade Federal do Paraná-UFPR. Coordenador do Grupo de Estudos em Direito Autoral e Industrial - GEDAI / UFPR. Professor da Cátedra de Propriedade Intelectual no Institute for Information, Telecommunication and Media Law - ITM da Universidade de Münster - ALEMANHA. Docente do curso políticas públicas y propiedad intelectual do Programa de Mestrado em Propriedade Intelectual na modalidade à distância na Faculdade Latino-americana de Ciências Sociais - FLACSO/ARGENTINA. Contacto: marcos.wachowicz@gmail.com

2 Mestrando em Direito do Estado pela Universidade Federal do Paraná - UFPR. Especialista em Direito Constitucional pela Academia Brasileira de Direito Constitucional. Contacto: pedrohmluz@gmail.com

RESUMO

O objetivo deste artigo é estudar a decisão que ficou conhecida como o caso *González vs Google Espanha*. Inicialmente, fez-se uma análise jurídico-sociológica da chamada "sociedade informacional". Em seguida, promoveu-se uma análise da referida decisão proferida pelo Tribunal de Justiça da União Europeia. Neste julgado, foi determinada ao provedor de busca uma obrigação de fazer, qual fosse a que desindexasse os resultados contendo uma dívida já extinta em nome do autor da ação; isso fez surgir uma nova possibilidade de tutela aos direitos da personalidade, denominada de "direito à desindexação". A desindexação, então, figura como um meio de dificultar o acesso às informações nocivas aos aludidos direitos. O estudo empreende considerações críticas acerca da sobredita decisão, utilizando o método hipotético-dedutivo. Finalmente, apontaram-se os desafios no tocante ao tema, eis que o legislador e o julgador brasileiro, na função de operadores do direito, parecem não conseguir absorver as contribuições da realidade europeia.

Palavras-chave: Direito de Desindexação; *González vs Google Espanha*; motores de busca; direitos fundamentais; proteção de dados pessoais

ABSTRACT

The objective of this article is to study the contours and intricacies of the decision handed down in 2014 by the Court of Justice of the European Union in what is known as González v. Google Spain. Initially, it was made a juridical-sociological analysis of a new moment crossed by the society, coined by Castells as the "Network Society". An analysis of the decision of the Court of Justice of the European Union was then carried out. In this judgment, the search provider was given an obligation to do, which would disindex the results containing a debt already extinct in the name of the author of the action; this has given rise to a new possibility for the protection of personality rights, known as the "right to deindexation". Deindexation, then, appears as a means of making access to information harmful to the aforementioned rights difficult. The study undertakes critical considerations about the above decision, using the hypothetico-deductive method. Finally, the challenges were raised in this area, since the legislator and the Brazilian judge, in their duty as operators of the law, seem to be unable to absorb the contributions of the European reality.

Keywords: deindexation; *González vs Google Spain*; search engines; fundamental rights; personal data protection

SUMÁRIO: Introdução; 1. A sociedade informacional novos desafios para o direito; 2. A privacidade em risco 3. Direito ao esquecimento no Brasil; 4. O Direito de Desindexação; 4.1. Caso *González vs Google Espanha*. 4.2. Os fundamentos da decisão; 4.3. Análise crítica do julgado; 5. Novas perspectivas e desafios; 6. Considerações Finais; Referências Bibliográficas.

INTRODUÇÃO

Diversos autores das mais diversas áreas do saber debruçaram-se a estudar um novo momento histórico que surgiu a partir do último quarto do século passado[1].

Este novo cenário, permeado por incertezas e alvo das mais diferentes denominações[2], deu-se, principalmente, com a evolução tecnológica e da comunicação, responsável por desvelar novos contornos à sociedade, pautando uma verdadeira revolução comparável, por exemplo, ao que a máquina a vapor representou para a Revolução Industrial (CASTELLS, 1999, p. 74).

Aliás, além de precursor do movimento que hoje vivemos, cunhado por CASTELLS de "sociedade informacional" (CASTELLS, 1999, p. 57), o industrialismo trouxe importantes lições sobre como a manipulação da tecnologia pode ter, a um só tempo, tanto efeitos positivos quanto deletérios.[3]

Nessa novel realidade, a informação passou a ocupar local de primazia tanto pelo seu significativo valor econômico, servindo portanto como base da gestão de negócios de empresas tais como o *Facebook* e o *Google*, quanto pela possibilidade que seu mau uso acarretou para provocar danos irreversíveis a uma plêiade de direitos, especialmente aqueles gestados pela luta histórica dos povos, como é ocorre com os direitos da

1 CASTELLS (1999, p. 91-92) aponta: "Acho que podemos dizer, sem exagero, que a revolução da tecnologia da informação propriamente dita nasceu na década de 1970, principalmente se nela incluirmos o surgimento e difusão paralela da engenharia genética mais ou menos nas mesmas datas e locais (...)".

2 Jean-François LYOTARD, em sua obra "A Condição Pós-Moderna", nomina esse novo momento de "sociedade pós-industrial". (LYOTARD, 1979). Adam SCHAFF, por seu turno, chama o novo paradigma de "sociedade informática". (SCHAFF, 1995).

3 Frisa-se, portanto, que embora tenha havido um vertiginoso acréscimo da expectativa de vida média no contexto da Revolução Industrial, autores como Karl Marx e Engeles apontaram um cenário geral de acirramento das desigualdades. Segundo MARX e ENGELS: "A sociedade burguesa moderna, que brotou das ruínas da sociedade feudal, não suplantou os velhos antagonismos de classe. Ela colocou no lugar novas classes, novas condições de opressão, novas formas de luta." (MARX; ENGELS, 1975)

personalidade em geral e com a privacidade em particular, cuja fragilidade e volatilidade já havia sido antevista há mais de um século (WARREN; BRANDEIS, 1890).

Avanços tecnológicos, portanto, não representam necessariamente um maior grau de emancipação do ser na expansão e concretização de direitos fundamentais.

Nessa conjuntura, o direito, com sua função primordial de ordenação social (GROSSI, 2016, p. 13) é requisitado para trazer certa pacificação aos conflitos advindos desse atrito.

O foco do presente estudo diz respeito a um caso datado de 2014, que chegou às portas do Tribunal de Justiça da União Europeia e envolvia, de um lado, os direitos da personalidade de um cidadão espanhol e, de outro, as pretensões econômicas de uma das maiores empresas do mundo: o *Google*.

O julgado ficou conhecido como *González vs Google Espanha* e teve como principal efeito o advento de um "direito à desindexação" de dados de pesquisa, a fim de tutelar a privacidade.

Tratou-se, neste estudo interdisciplinar, de apresentar um relatório do caso sobredito e construir-se uma crítica norteada por contribuições do direito civil, do direito constitucional e de outros ramos do saber, tais como a ciência da computação e a sociologia.

Assim, foi possível observar quais as principais questões imanentes na área jurídica nacional e internacional, que já enfrenta e enfrentará cada vez mais casos desafiadores que costuram a nova realidade "informacional" em sua feição conflituosa com direitos fundamentais.

Ressalte-se que, no contexto brasileiro, não havendo regulação específica atinente aos dados pessoais [4] e inexistindo um efetivo ônus argumentativo exercido pelos julgadores, defende-se que a atividade judiciária pondere exaustivamente, de forma

4 O Projeto de Lei nº 5276/2016 figura como uma promessa de normatização, mas ainda a depender dos anseios e conveniências do Poder Legislativo.

atenta às peculiaridades de cada caso, quais valores estão em jogo para, só após elencá-los, decidir qual detém prevalência parcial ou total.

1. A SOCIEDADE INFORMACIONAL NOVOS DESAFIOS PARA O DIREITO

O que caracteriza precisamente a sociedade do século XXI? De que maneira seus modos de produção, paradigmas filosóficos, cosmovisões mundanas e conformações institucionais interferem na vida cotidiana de seus sujeitos? Essas questões, longe de apresentarem-se na condição de indagações inéditas, são levantadas no frontispício deste trabalho a fim de que, com o aporte teórico de Manuel Castells, a noção de "sociedade informacional" seja explorada em seus principais desdobramentos.

O ponto central para entender essa revolução paradigmática diz respeito à reformulação sofrida pelo capitalismo, em um processo de "flexibilização". Para Castells, essa transformação tem como características "maior flexibilidade de gerenciamento; descentralização das empresas e sua organização em redes (...); intervenção estatal para desregular os mercados de forma seletiva e desfazer o estado de bem-estar social com diferentes intensidades e orientações [...]" (CASTELLS, 1999, p. 39-40).

Essa reestruturação do modelo capitalista, ocorrida em grande medida após a crise do petróleo de 1973[5], culminou, enfim, na integração global de mercados em redes, entre diversas outras decorrências típicas do novo modelo "flexível". E no cerne de todo esse referido modelo está a informação, que hoje está em pé de equivalência com o que a eletricidade representou na Era Industrial (CASTELLS, 2003, p. 7).

Impende ressaltar ainda que a rede, definida por Castells como "um conjunto de nós interconectados (CASTELLS, 2003, p. 7), que sempre foi uma constante observável inclusive na natureza, transmuta-se em uma rede informacional, propulsionada pelo advento da Internet. Todo esse conjunto de fatores consubstancia uma nova forma de sociedade — a sociedade informacional (CASTELLS, 2003, p. 8).

5 No caso do Brasil, essa crise foi particularmente relevante, eis que colocou um corte no período de extravagante crescimento econômico que permeava o Brasil na ditadura militar, fase chamada de "milagre econômico". Para mais: PIMENTEL, Fernando. O fim da era do petróleo e a mudança de paradigma energético mundial: perspectivas e desafios para a atuação diplomática brasileira. Brasília: Fundação Alexandre de Gusmão, 2011. p. 20.

De forma conexa ao pensamento de Castells, Ronaldo Porto Macedo Júnior atesta que "boa parte do poder econômico se manifesta em uma série de empresas ou grupos econômicos de forma concreta: na capacidade de formar redes, criar instituições e se organizar em processos cognitivos" (MACEDO JÚNIOR, 2006, p. 31).

A nova organização social com reflexo de processos econômicos bastante específicos repercute de forma incisiva no direito.

A título exemplificativo, Castells aponta que temas como soberania, ligados a bases físicas bastante nítidas (territórios), encontra uma certa crise com a sociedade disposta em uma organização em rede, na medida que a geometria geopolítica é desterritorializada, afirmando que "a governação é realizada numa rede, de instituições políticas que partilham a soberania em vários graus, que se reconfigura a si própria numa geometria geopolítica variável". (CASTELLS, 2005, p. 26).

No que toca à proteção de direitos fundamentais historicamente consagrados, o paradigma de rede faz surgir um cabedal de novos problemas de efetivação desses direitos. Focando a atenção detidamente ao contexto brasileiro, a Constituição Brasileira de 1988 veio como um documento repleto de promessas e projetos a cumprir, pautada em um alto grau de abstração normativa, com a preferência por cláusulas abertas, como, por exemplo, com a dignidade da pessoa humana, núcleo temático da Carta de 1988 (REIS; ZIEMANN, 2016, p. 4).

Através desse fio condutor, o foco do ordenamento jurídico passa a ser na pessoa, entendida como valor fonte das relações jurídicas (REALE, 2003, p. 75).

Ademais, as referidas cláusulas abertas que permeiam o texto constitucional deixam um espaço razoável para que o sistema jurídico adapte-se às mudanças ocorridas em outras áreas do saber, como por exemplo na economia, na política e na tecnologia.

Desse modo, o próximo item verificará brevemente o percurso do direito fundamental à privacidade desde sua concepção norte-americana de um direito meramente subjetivo "a ser deixado em paz" até sua positivação e reconfiguração na Constituição Federal de 1988.

2. A PRIVACIDADE EM RISCO

Dentre as inovações tecnológicas ocorridas no século XX e XXI, como por exemplo a digitalização, o armazenamento barato de informações, a facilidade no acesso e o alcance

global das redes (MAYER-SCHONBERGER, 2009) fizeram transparecer novos desafios no que atine à proteção da privacidade.

Afinal, já há dois séculos uma dupla de autores norte-americanos anunciava, em tom profético, o fato de que novos predadores trariam dilemas nunca antes enfrentados para a seara da privacidade (WARREN E BRANDEIS, 1890).

À época de escrita do emblemático "The Right to Privacy", a principal preocupação dos referidos juristas centrava-se na nociva intervenção da imprensa na esfera privada, o que fez com que estes conclamassem a existência, no contexto da *common law*, de um direito de "ser deixado em paz"[6].

Passados exatos 127 anos da marcante obra, a premissa suscitada por Warren e Brandeis permanece incólume.

O segundo pós-guerra trouxe uma nova aproximação do direito civil (especialmente com os direitos de personalidade) com a constituição e, por conseguinte, com a noção de dignidade da pessoa humana[7], pautando o movimento cunhado pela doutrina de "repersonalização do direito civil"[8] (FACHIN, 1992).

Nesse contexto, os direitos da personalidade no geral e a privacidade em específico ganham novos contornos, perpassando uma esfera clássica meramente individualista e ascendo para uma forma de preocupação coletiva, própria de um Estado tido como (também) social, cujo foco centra-se na regulação econômica e da sociedade (LOBO, 2002).

---

6 Os autores apontam (1890, p. 3): "Recentes invenções e métodos de negócios chamam atenção para o próximo passo que deve ser tomado para a proteção da pessoa e asseguramento ao indivíduo do que o Juiz Cooley chama de o direito de "ser deixado só". Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone". Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."

7 BITTAR atesta (2015, p. 42): "[...] Os estudos mais recentes no campo do Direito Civil, em sua aproximação com o Direito Constitucional, na esteira dos trabalhos de Ingo Wolfgang Sarlet, têm tornado possível afirmar a unidade do tratamento da matéria e a desnecessidade de advogar de modo forte a posição positivista ou a posição jusnaturalista, como opostas. Seja a busca de unidade entre ramos do direito, seja a busca de unidade entre linhas de análise, têm proporcionado a possibilidade de afirmar na dignidade da pessoa humana, decorrente da Constituição de 1988, e decorrente da Declaração Universal dos Direitos Humanos de 1948, a forma pela qual se dá tratamento e se confere fundamentação aos direitos humanos, aos direitos fundamentais e, por consequência, aos direitos de personalidade."

8 Afirma FACHIN (2003, p. 218): "O Direito Civil deve, com efeito, ser concebido como 'serviço da vida', a partir de sua real raiz antropocêntrica, não para repor em cena o individualismo do século XVIII, nem para retomar a biografia do sujeito jurídico da Revolução Francesa, mas sim para se afastar do tecnicismo e do neutralismo. O labor dessa artesania de 'repersonalização' e 'reetização' leva em conta um sistema aberto e rente à vida."

3. DIREITO AO ESQUECIMENTO NO BRASIL

O Direito ao esquecimento ainda que sem uma regulamentação legal, foi objeto de demandas judiciais, tendo por diversas vezes o Poder Judiciário e a Doutrina analisado casos específicos e prolatado decisões favoráveis.

No Judiciário um dos primeiros casos em que foi assegurado o Direito ao esquecimento pelo Superior Tribunal de Justiça, por decisão unânime do colegiado da 4ª Turma, em dois recursos contra as reportagens da TV Globo, em que se relatavam cenas de violências que chocaram o país.[9]

Na Doutrina brasileira também o Direito ao Esquecimento foi objeto de análise e de entendimento favorável desde a edição do Enunciado 531, da VI Jornada de Direito Civil do Conselho de Justiça Federal (CJF), quando em 2016, assim se posicionou:

"*ENUNCIADO 531 – A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. Artigo: 11 do Código Civil Justificativa: Os danos provocados pelas novas tecnologias de informação vêm-se acumulando nos dias atuais. O direito ao esquecimento tem sua origem histórica no campo das condenações criminais. Surge como parcela importante do direito do exdetento à ressocialização. Não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos pretéritos, mais especificamente o modo e a finalidade com que são lembrados.*"[10]

Assim o Direito ao esquecimento se presta tanto para regular coletas de dados como para assegurar a possibilidade da indivíduo discutir a utilização, modo e finalidade com que os dados pretéritos sobre sua pessoa são fixados na Internet e a maneira pela qual são lembrados.

Contudo, a aplicação do Direito ao esquecimento pelo Judiciário requer um estudo mais atendo na ponderação dos interesses individuais do cidadão em oposição aos direitos coletivos de acesso a informação por parte da sociedade.

A questão central aqui se verifica quando determinadas pessoas que exerceram cargos públicos estiveram envolvidas em acusações de crimes poderão pleitear a desindexação de tais

9 "Foram dois recursos ajuizados contra reportagens da TV Globo, um deles por um dos acusados mais tarde absolvidos pelo episódio que ficou conhecido como a Chacina da Candelária, no Rio de Janeiro. O outro, pela família de Aída Curi, estuprada e morta em 1958 por um grupo de jovens. Os casos foram à Justiça porque os personagens das notícias no caso de Aída, os familiares sentiram que não havia necessidade de resgatar suas histórias, já que aconteceram há muitos anos e não faziam mais parte do conhecimento comum da população." Acesso na Internet 28 de agosto de 2018, disponível no link: https://amagis.jusbrasil.com.br/noticias/100548144/stj-aplica-direito-ao-esquecimento-pela-primeira-vez

10 http://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/enunciados-vi-jornada/view

fatos nos buscadores na Internet retirando o conteúdo da possibilidade de acesso da coletividade sobre fatos pretéritos que as denigrem, isso mesmo que tenham sido absolvidas.

Será então possível, admitir-se que, no exercício de funções públicas os atos praticados pelos agentes públicos, sejam estes eleitos ou servidores públicos de carreira, haverão de ter limitada a aplicação do direito de desindexação, na exata medida que prevalecerá o interesse coletivo em ter acesso à informação sobre as ações realizadas.

O interessado na desindexação de determinado conteúdo na INTERNET, deverá notificar judicialmente o provedor de conteúdo como determina o Marco Civil da Internet (artigo 19, parágrafo 1º da Lei 12.965/2014), apontando claramente os elementos que considera ofensivos, fornecendo o URL (*Uniform Resource Locator*)[11] indicando ao provedor de conteúdo que tais informações estão hospedadas deverão ser desindexadas.[12]

A ausência da indicação precisa não implica em impedimento da interposição da medida judicial, porém, poderá gerar dificuldades para o efetivo cumprimento da decisão, acarretando novas controvérsias.

Atentando ao contexto brasileiro, a Constituição Federal de 1988 foi responsável por positivar no seio do texto constitucional, de forma inédita, uma plêiade de dispositivos que enfatizam os direitos da personalidade, edificando sua essência jusfundamental sobretudo no artigo 5º, X, que traz proteção à intimidade, à vida privada, à honra e à imagem das pessoas, assegurando ainda os meios cabíveis de reparação civil.

A postura do constituinte em dispor explicitamente acerca dos direitos de personalidade no catálogo formal de direitos fundamentais revela uma arguta percepção dos novos tempos, também servindo como vias de compatibilizar o texto constitucional com uma visão emancipatória (CLÉVE, 2012), atento à pessoa em sentido amplo.

Em que pese notáveis mudanças tenham ocorrido, portanto, no que tange à tutela da personalidade[13], norteados ora pela criação de novos direitos[14], ora por sua modificação e sutil

---

11 URL é o endereço de um recurso disponível em uma rede, seja a rede internet ou intranet, e significa em inglês Uniform Resource Locator, e em português é conhecido por Localizador Padrão de Recursos. ... Url também pode ser o link ou endereço de um site.

12 Neste sentido ver o julgado: "A jurisprudência do STJ, em harmonia com o artigo 19, § 1º, da Lei 12.965/2014 (Marco Civil da Internet), entende necessária a notificação judicial ao provedor de conteúdo ou de hospedagem para retirada de material apontado como infringente, com a indicação clara e específica da URL." (STJ. 3º T., REsp 1.568.935 – RJ, Rel. Min. Ricardo Villas Bôas Cueva, julg. 05.04.16)

13 Passando, portanto, de um direito meramente liberal e, portanto, individual, para uma faceta social ou coletiva de proteção contra o arbítrio do Estado e também de outros sujeitos.

14 Cita-se, a título exemplificativo, o advento do chamado direito ao esquecimento, que possibilita a seu titular, o não conhecimento, por outrem, de algum fato pretérito de sua vida, mesmo que verdadeiro. Tal direito surge justamente por intermédio de um estreitamento na relação entre os direitos da personalidade e a dignidade da pessoa humana.

evolução, o direito encontra-se sempre em "perene desenvolvimento" (FERREIRA FILHO, 2009), tendo de regular novos fenômenos na velocidade galopante das inovações tecnológicas, sociais e econômicas, o que sabemos ser tarefa raramente tangível pelo paquidérmico sistema jurídico.

A grande preocupação deste estudo atine a este novo cenário, especificamente na rotineira prática, protagonizada principalmente por empresas, de coleta massificada de dados[15], inclusive pessoais, atividade na maior parte das vezes promovida sem a anuência de seu titular.

Nesse contexto de incertezas o direito é convocado para não apenas regular temas polêmicos como a coleta de dados, mas sobretudo a fim de sancionar e obrigar os novos *players* a adotarem determinadas posturas ou cumprirem com obrigações específicas.

Foi exatamente isso que ocorreu em 2014, quando o Tribunal de Justiça da União Europeia julgou o emblemático caso *González vs. Google Espanha*, que será o foco de estudo a partir de agora.

4. DIREITO DE DESINDEXAÇÃO

A título de exemplificação pode-se hipnotizar a seguinte situação: após contrair uma dívida com um banco determinada pessoa tem o seu nome a figurar no cadastro nacional de inadimplentes e esse fato é noticiado em jornais locais.

O mutuário prontamente quita a dívida; entretanto, embora não haja mais obrigação alguma com a instituição bancária, a notícia permanece para quem quiser buscá-la e, ao reboque de insistentes pedidos de retirada, o jornal nega a requerida remoção, alegando para si um direito de liberdade de imprensa.

Após vislumbrar como infrutífera qualquer comunicação com o aludido jornal, o mutuário, na condição de autor do processo contra a instituição financeira, resolve solicitar ao Google que omita os resultados de busca envolvendo a dívida já adimplida. Em breve síntese, foi isso que ocorreu no caso que será melhor estudado adiante.

Questiona-se: haveria, no caso narrado, um direito do autor em pedir para o *Google* desindexar as buscas em seu desfavor? Qual seria a extensão dessa decisão?

15 A doutrina calhou chamar tal fenômeno de "*big data"*. (MAYER-SCHONBERGER e CUKIER, 2014)

A ideia central, cumpre salientar, é de que informações veiculadas licitamente passam, com o tempo, a perder relevância e interesse público, possibilitando sua remoção ou desindexação.

4.1. Caso *González vs Google Espanha*

O caso *González vs Google* Espanha, julgado em 2014 pelo Tribunal de Justiça da União Europeia, foi um marco no que toca ao tema da proteção da personalidade.

Isso, pois trouxe ao centro da dogmática jurídica uma nova ferramenta útil à tutela desse bem, qual seja a desindexação[16] dos dados agrupados por motores de busca.

A princípio, evidencia-se que o caso sob análise é um verdadeiro marco decisional que revela a grande preocupação dos países europeus em regular os aspectos mais polêmicos no tocante à proteção da personalidade, criando inclusive figuras jurídicas inéditas aliadas a soluções técnicas bastante criativas, tudo com o fito de (tentar) disciplinar as relações sociais na internet.

Na data de 5 de março de 2010, o *Sr. Costeja González*, cidadão espanhol, ingressou com uma reclamação judicial contra o *La Vanguardia Ediciones SL*, jornal de grande circulação na região da Catalunha; na mesma ação, também acionou judicialmente o *Google Spain* e o *Google Inc.*

A ação originou-se do fato de que, ao buscar-se o nome completo do *Sr. González* na ferramenta de pesquisa do *Google*, os resultados traziam duas páginas do referido jornal *La Vanguardia*, datadas de 19 de janeiro e 9 de março de 1998, em que o nome de *González* estava relacionado com procedimentos de execução fiscal de débitos de seguridade social[17].

Em sua argumentação, o reclamante apontou que tal dívida havia sido quitada há anos.

O pedido centrou-se, portanto: a) na remoção ou alteração dessas páginas, pelo jornal *La Vanguardia*, a fim de que os dados pessoais relacionados ao nome do autor não mais aparecessem nas buscas; b) na remoção ou omissão dos dados de busca envolvendo seu nome no mecanismo de busca *Google Spain* e *Google Inc.*

16 A ciência da computação, como ramo autônomo do saber, pouco utiliza o termo "desindexação" no Brasil, pois prefere recorrer à expressão "indexação de dados" ou somente "indexação", cujos pilares são os metadados, os buscadores, os usuários e o posicionamento *web*. Para um estudo mais aprofundado, consultar: GIL-LEIVA, Isidoro. A indexação na internet. Brazilian Journal of Information Science. v.1, n.2, p.47-68, jul./dez. 2007. ISSN: 1981-1640

17 EUROPA. Tribunal de Justiça da União Europeia. Processo C-131/12. Pesquisa de Jurisprudência. 13 de maio de 2014. Acórdão disponível em: <http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065>. Acesso em 30/05/2017.

No âmbito administrativo, em 30 de julho de 2010, a Agência Espanhola de Proteção de Dados rejeitou o pleito, esclarecendo que, no tocante ao pedido dirigido ao *La Vanguardia* (a), a publicação estava juridicamente justificada pois deu-se após ordem do Ministro do Trabalho e Justiça Social, que intentava dar a maior publicidade possível aos débitos sociais.

Todavia, atinente ao pedido (b), a referida agência sustentou que motores de busca como o *Google* estão sujeitos aos ditames das leis de proteção de dados, eis que são *responsáveis pelo processamento de dados* e atuam como intermediários da informação.

Em seu argumento fulcral, o órgão administrativo externou a visão de que poderia requerer a retirada de dados e a proibição de acesso a determinados dados por motores de busca quando a localização e disseminação de tais dados atentasse contra o direito fundamental de proteção de dados e a dignidade da pessoa *lato sensu*.

O mecanismo para atingir esse fim não seria necessariamente a remoção dos dados, mas sim a *desindexação das buscas*.

Irresignado com a suprarreferida decisão, o *Google Spain* e a *Google Inc.* ajuizaram recursos na Audiência Nacional, um órgão judiciário espanhol com competência sobre todo o território do país[18], que subiriam para o Supremo Tribunal da Espanha.

Em sua argumentação defensiva, apontavam que o *Google* não faz tratamento de dados nas aplicações de internet[19] em relação a terceiros.

E, mesmo que tratasse diretamente desses dados, a reclamada não poderia ser responsabilizada pelo seu teor, pois não teria conhecimento e nem controle sobre eles.

Por entender que a matéria de fundo do julgamento envolvia a interpretação da Diretiva 95/46[20], a Audiência Nacional declinou de sua competência e devolveu o processo ao Tribunal de Justiça da União Europeia, órgão judiciário de cúpula no contexto da UE[21].

---

18 Seria o equivalente ao Superior Tribunal de Justiça no Brasil. RODRIGUES JÚNIOR, Otavio Luiz. Direito de apagar dados e a decisão do tribunal europeu no caso Google Espanha. 2014. Disponível em <http://www.conjur.com.br/2014-mai-21/direito-apagar-dados-decisao-tribunal-europeu-google-espanha>. Acesso em 30/05/2017.

19 Uma definição de aplicações de internet pode ser encontrada no artigo 5º, VII, do Marco Civil da Internet: "aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet".

20 Tal diretiva, datada de 24 de outubro de 1995, tem aplicação sobre todos os países da União Europeia e refere-se à proteção de pessoas naturais no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Interessante notar, portanto, que os países integrantes da União Europeia tem regramento próprio sobre o tema desde 1995, enquanto o Brasil ainda não editou uma lei específica acerca da proteção de dados pessoais. Ademais, a Espanha, como já citado, tem na estrutura de sua administração pública uma autarquia, a Agência Espanhola de Proteção de Dados, incumbida dessa matéria. Notório o déficit brasileiro no tema. Diretiva disponível em < http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em 30/05/2017.

21 A partir de então, alguns estudiosos do caso passaram a nominá-lo de *González e AEPD vs. Google Espanha*, pelo fato de que o órgão administrativo europeu havia respaldado uma das pretensões do autor, qual seja a de considerar a empresa ré como gestora de dados, atribuindo-se-lhe responsabilidade diferenciada.

4.2. Os fundamentos da decisão prolatada

A ação foi finalmente julgada pelo Tribunal de Justiça da União Europeia em 13 de maio de 2014. Os objetos de análise foram especificamente os artigos 2º, alíneas "b" e "d", também o artigo 4º, inciso 1, alíneas "a" e "c", o artigo 12, alínea "b", e finalmente o artigo 14, §1º, alínea "a", todos da já citada Diretiva 95/46/CE, bem como do artigo 8º da Carta de Direitos Fundamentais da União Europeia.

A principal discussão, portanto, seria se motores de busca como o Google realizam tratamento de dados e, caso assim considerado, se haveria responsabilidade por parte da empresa nesse trato, mediante exegese da referida diretiva.

Neste ponto, o órgão decisório consignou:

Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data.[22]

Desse modo, o primeiro ponto assentado na decisão foi de que o Google realiza efetivamente o tratamento de dados, nos moldes do texto previsto na Diretiva 95/46/CE.

No atinente à responsabilidade da empresa decorrente desse tratamento, o Tribunal de Justiça da União Europeia asseverou, no ponto 33 das questões prejudiciais, que: *"It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d)*"[23].

---

22 "Assim, deve ser considerado que, por explorar a internet de forma automática, constante e sistemática em busca da informação que é publicada lá, o operador de um mecanismo de busca 'coleta' tal data que é subsequentemente 'recuperada', 'registrada' e organizada na estrutura de seus programas de indexação, também 'guardada' em seus servidores e, dependendo do caso, 'divulgada' e 'disponibilizada' para seus usuários na forma de listas com resultados de pesquisa. De modo que tais operações constam expressamente e incondicionalmente no artigo 2º, alínea b, da Diretiva 95/46, elas devem ser classificadas como 'tratamento' no sentido daquela provisão, independente do fato de que o operador dos mecanismos de busca também realiza essas mesmas operações no tocante a outros tipos de informação e não realiza a distinção entre o último e os dados pessoais" (tradução livre).

23 "[…] é o operador do motor de busca que determina as finalidades e os meios dessa atividade e, deste modo, do tratamento de dados pessoais que ele próprio efetua no contexto dessa atividade e que deve, consequentemente, ser considerado 'responsável' por esse tratamento por força do referido artigo 2.°, alínea d)" (tradução livre)

Não obstante, pelo fato de que as atividades dos motores de busca podem afetar sobremaneira direitos fundamentais, mormente a privacidade e a proteção de dados pessoais, aquele que opera este motor deve assegurar que sua atividade esteja em acordo com o disposto na Diretiva 95/46.

Consequentemente, concluiu o tribunal que haveria responsabilidade do motor de busca na formatação de dados pessoais pela possibilidade latente de que sua atividade viesse a afetar bens jusfundamentais[24].

Superadas tais questões, passa-se ao eixo decisório central, que guarda maior pertinência com este estudo: o reconhecimento ou não da existência um direito à desindexação ou exclusão de referências ou *links* nos mecanismos de busca (SARLET, 2015).

Nessa senda, estava-se a julgar se a conduta de indexação dos resultados de busca envolvendo o nome de González seria ilícita, ou seria apenas a divulgação da notícia do La Vanguardia que mereceria reprimenda do direito.

O argumento encontrado pelo Tribunal de Justiça da União Europeia foi de que, ao explorar economicamente a informação[25] por intermédio de listas de resultados, haveria uma especificidade na atuação do Google em comparação com o La Vanguardia[26].

Foi levantando também o argumento de que a desindexação das buscas figura como ação muito menos restritiva do que a remoção de determinada página da internet.

De forma corajosa, mas não menos criticável, o órgão decisório determinou ao Google a desindexação dos resultados de busca relacionando o nome de *González* ao débito já saldado.

Superadas as questões que visavam esclarecer sobre o caso paradigmático, promover-se-á uma análise crítica do teor da decisão.

4.3. Análise crítica do julgado

A decisão proferida no *caso González* é de importância monumental para as futuras discussões acerca dos temas esquecimento, direitos da personalidade na internet e responsabilidade dos provedores de busca.

---

24 Esse é um caso interessante para se estudar a eficácia horizontal dos direitos fundamentais no âmbito europeu, apesar desse não ser o foco do presente trabalho. Bens jusfundamentais são o cerne de proteção dos direitos fundamentais. Ex: direito à saúde pode proteger a vida, a escolha do tratamento, a dignidade, entre outros bens.

25 Novamente, rememora-se que a informação ocupa papel central na sociedade informacional, por ser o principal *commoditie* ou a principal matéria-prima produtiva. Ademais, por constituir-se como a base material dessa nova sociedade, o modelo negocial de diversas empresas como o facebook e o google baseiam-se na coleta e sistematização de dados. (CASTELLS, 1999).

26 Assim, o site de buscas seria responsável, após pedido do autor, por desindexar os resultados contestados. Esse é um ponto importante, pois seria bastante temerário exigir que o Google desindexasse tais informações de ofício, pois essa conduta poderia gerar verdadeira censura.

A argumentação despendida pelo órgão decisório tentou e efetivamente conseguiu equilibrar diversos valores importantes pertencentes ao patrimônio jurídico tanto da parte autora quanto da ré.

Assim, a desindexação apresenta-se como um engenhoso e promissor mecanismo de proteção à personalidade na internet, sendo inclusive meio menos restritivo em comparação com, por exemplo, a remoção de uma página, pois, ao simplesmente desindexar, não ocorrerá a supressão material do dado, mas apenas construir-se-á uma barreira artificial ao seu acesso.

Tomando uma analogia bastante elucidativa, seria o mesmo que colocar um livro no fundo de uma prateleira de uma biblioteca; a obra continuaria ali, para todos que quisessem acessá-la, mas haveria uma dificuldade mais latente em sua busca.

É de se criticar, contudo, a ligeira e acrítica aproximação entre a decisão proferida no caso *González vs Google* e a polêmica figura do direito ao esquecimento, como se o objeto central da sentença proferida pelo aludido Tribunal fosse estritamente ligado a uma pretensão de esquecimento do autor.

A máxima não procede porquanto a decisão foco de estudo citou o *Right to be forgottten* apenas 3 vezes, de modo *en passant*, representando um apêndice e não o coração do acórdão.

Esse ponto deve ser colocado: esquecimento na internet, completo e sem repercussões, é tarefa impossível; o que pode ser feito, a depender de forte ônus argumentativo e ponderação com demais princípios colidentes no caso concreto, é a desindexação de determinada informação atentatória a um dos direitos de personalidade, contanto que haja possibilidade concreta para tanto.

Também é de se ter bastante cuidado na importação automática da desindexação para o cenário jurídico brasileiro, pelos seguintes motivos: a) não temos uma lei específica de proteção de dados pessoais como ocorre no contexto europeu, portanto qualquer decisão nesse sentido seria, do ponto de vista hermenêutico, ativista; b) existe uma prática autoritária de desindexação de dados que detém interesse público ou constituem a história dos povos, portanto qualquer aplicação deste novel instituto obriga necessariamente uma análise aprofundada e que utilize da melhor técnica da proporcionalidade e da ponderação de princípios. [27]

27WACHOWICZ, Marcos; LUZ; Pedro. O "DIREITO À DESINDEXAÇÃO": repercussões do caso Gonzáles vs Google Espanha. In Revista Espaço Jurídico *Journal of Law* | EJJL |vol. 19. Número 2 , ano 2018, pg. disponível no link: https://editora.unoesc.edu.br/index.php/espacojuridico/article/view/16492

5. NOVAS PERSPECTIVAS E DESAFIOS

Alertando-se a esse conturbado cenário pelo qual os direitos da personalidade perpassam, que fez surgir uma possibilidade bastante peculiar de sua tutela, principalmente após 2014 com o emblemático julgado *González vs Google*, algumas dúvidas ainda permanecem e serão apresentadas neste capítulo, mormente aquelas relacionadas à eventual aplicação do instituto da desindexação de dados em solo brasileiro.

a) Insuficiência do Marco Civil da Internet (Lei nº 12.965/2014):

Inicialmente, convém destacar aspectos relacionados ao Marco Civil da Internet, regramento fruto de ampla discussão no cenário brasileiro. Conforme já apontei anteriormente: "O fato é que a Lei do Marco Civil da Internet vem preencher uma lacuna no ordenamento jurídico brasileiro, vez que inexistia qualquer norma dispusesse sobre os princípios, direitos e deveres dos usuários na Internet" (WACHOWICZ, 2015, p. 236).

Embora o novo diploma legislativo tenha representado um retumbante avanço da regulação do direito no ambiente dinâmico da internet, fato é que, no tratamento de dados pessoais, a legislação é bastante vaga e, por conseguinte, insuficiente. Apesar de a proteção de dados constar nitidamente como um princípio, alocado no art. 3º, inexiste qualquer disciplina sobre a responsabilidade dos mecanismos de busca e nem sobre como eles deveriam proceder para efetuarem a desindexação de dados[28] de pesquisa.

Nessa esteira, impende salientar que o Brasil é um dos poucos países ainda carentes de uma legislação específica sobre proteção de dados pessoais (MORGADO, 2009), o que prejudica e muito a discussão de certos temas, como por exemplo a corriqueira e odiosa prática de mercantilização de dados pessoais pelas empresas, violadora de diversos princípios constitucionais. Tudo pra dizer, então, que em matéria de proteção de dados pessoais a discussão e regulação do tema ainda engatinham em solo pátrio, na contramão do que muitos países — principalmente europeus — vêm fazendo.

28 Acreditamos que necessariamente haveria de ter uma ordem judicial, sob risco de a desindexação *ex officio* tornar-se censura por parte dos mecanismos de busca.

b) Os casos penumbra ou a falibilidade do direito em regular ambientes tão dinâmicos como a internet:

A segunda inquietação se apresenta na seguinte questão: mesmo que por ventura exista uma regulação legal bastante específica e protetiva em matéria de proteção de dados pessoais, sanando portanto os problemas trazidos no tópico passado, a seguinte dúvida permanece: o direito consegue ou conseguiria tutelar a personalidade do cidadão no contexto da internet, em que milhões de páginas são criadas e acessadas a cada minuto? Em suma: a proteção da personalidade seria compatível com a arquitetura da rede? (LESSIG, 2006)

Além disso, em alguns casos a simples desindexação não seria suficiente a fim de tutelar os direitos da personalidade. Como seria possível desindexar milhões de páginas agrupadas em diferentes mecanismos de busca? Afinal, embora no caso *González* a ordem tenha sido dirigida ao Google, existem diversos outros *sites* que prestam serviços parecidos. Ademais, a própria desindexação pode apresentar outros problemas; no caso do Google, ela deveria ser feita apenas para o endereço virtual local do Google — "google.com.br" — ou também para o domínio global — "google.com"?

Apesar da dúvida parecer, inicialmente, meramente lateral, ela implica em diferentes resultados práticos. Ao adotar-se apenas uma exclusão no domínio local, o resultado da busca ainda apareceria para usuários de outros países ou, ainda, para nacionais que utilizassem programas que mascaram a identidade na internet, chamados de *VPN*[29].

Em síntese, de nada adiantaria uma decisão ordenando a desindexação de determinado conteúdo violador dos direitos da personalidade se a execução da decisão não fosse factível ou se seus efeitos não pudessem ser determináveis. O revés apontado, por tocar nas próprias bases do direito e seu papel de regulador social, no contexto de um ambiente dinâmico como a internet, é um dos, senão o maior obstáculo a ser superado no tema. Desse modo, essas questões ainda permanecem espinhosas, devendo ser atendidas por tratados internacionais e regulações próprias do direito internacional.

29 Um VPN, ou *Virtual Private Network*, é uma rede privada virtual que tem por objetivo estabelecer conexões seguras através de protocolos não seguros. Vide: SARLO, Lino da Silva. VPN: Aprenda a Construir Redes Privadas Virtuais em Plataformas Linux e Windows. São Paulo, Novatec, 2003.

c) Conflitos principiológicos: o cuidado com banalizações

A tarefa de desindexação deve constituir-se sempre como exceção e não como regra. Isso quer dizer que, havendo qualquer solução diversa que se apresenta mais pacífica para os princípios constitucionais em jogo, a desindexação deverá ser desconsiderada[30]. É o caso, por exemplo, de quando uma informação constrangedora pode ser removida pelo próprio usuário, no caso de quando este detém seu controle, por estar, a título exemplificativo, em sua página pessoal do *Facebook*.

Conforme já aventado, também deve ser promovido um sábio cotejo entre todos os princípios que estão em jogo. De um lado, as empresas podem deter um legítimo interesse em informar e dissipar informações das mais variadas, atendendo ao relevante valor da liberdade de imprensa; de outro, o sujeito, que também pode ser uma pessoa jurídica, pode considerar que essa informação é atentatória por exemplo a sua imagem, pleiteando a devida reparação. É preciso dosar, com um forte ônus argumentativo, qual o lado preponderante da balança. Para tanto, exige-se uma decisão firme, que primeiro evoque explicitamente os princípios em choque e, somente então, decida pela opção menos ruidosa.

30 E, ainda, é preferível que a desindexação tenha uma precedência à obliteração ou remoção de páginas virtuais.

6. CONSIDERAÇÕES FINAIS

Apresentadas as considerações iniciais acerca da privacidade e sua nova configuração nos séculos XX e XXI, tratou-se do problema que o direito enfrenta em regular e tentar das respostas satisfatórias a esse novo modelo de sociedade pautado pela primazia da informação, cujas mudanças obrigam a readaptação de velhos institutos do sistema jurídico e a criação de tantos outros, sob pena de que direitos fundamentais historicamente conquistados sejam rapidamente erodidos.

O caso *González vs Google* representa bem, então, o conflito de interesses entre um titular de um direito de personalidade alegadamente violado e, no outro polo, a sanha de uma empresa em permanecer com um modelo de negócios pautado na coleta e indexação desenfreada de dados, inclusive pessoais.

O referido julgado representou o nascimento de um direito à desindexação de resultados de busca na União Europeia, mediante o entendimento de que a empresa Google, por realizar uma atividade de exploração econômica ligada a coleta de dados, era efetivamente uma tratadora desses dados, devendo arcar com a responsabilidade alocada nas disposições normativas da Resolução 95/46/CE.

A magnitude do caso, portanto, ecoa inclusive no contexto brasileiro, que infelizmente ainda não se encontra preparado para tratar casos dessa estirpe, por dois principais motivos: o primeiro é a falta de qualquer regulação específica para os dados pessoas – tanto legal quanto, por exemplo, por intermédio de agências reguladoras. O segundo, por uma má aplicação da ponderação principiológica pelos julgadores, o que poderia tornar a desindexação um mecanismo de censura e retrocesso, justamente o contrário do que o presente artigo visou a defender.

REFERÊNCIAS BIBLIOGRÁFICAS

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8. ed. São Paulo: Saraiva, 2015.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

_____. **Compreender a Transformação Social**. p.17-30. Artigo escrito para Conferência de 4 e 5 de Março de 2005, em Portugal-Lisboa.

CLÉVE, Clèmerson Merlin. **Para uma dogmática constitucional emancipatória**. 1ª. ed.

EUROPA. Tribunal de Justiça da União Europeia. Processo C-131/12. **Pesquisa de Jurisprudência.** 13 de maio de 2014. Acórdão disponível em: <http://curia.europa.eu/juris/document/document_print.jsfdoclang=EN&docid=15206>. Acesso em 30/05/2017.

FACHIN, Luiz Edson. Limites e possibilidades da nova Teoria Geral do Direito Civil. **Revista Jurídica da Faculdade de Direito da UFPR**, n. 27, 1992/93, p. 49-60, 1992.

_____. **Comentários ao Código Civil**. Parte Especial. Direito das coisas. São Paulo: Saraiva, 2003.

FERREIRA FILHO, Manoel Gonçalves. Parecer referente a consulta da Câmara dos Deputados acerca de verbas parlamentares. **Lex**. São Paulo: jun. 2009.

GIL-LEIVA, Isidoro. A indexação na internet. **Brazilian Journal of Information Science.** v.1, n.2, p.47-68, jul./dez. 2007. ISSN: 1981-1640

GROSSI, Paolo. **Primeira lição de direito**. Rio de Janeiro: Editora Forense, 2006.

LESSIG, Lawrence. **Code**: version 2.0. New York: Basic Books, 2006.

LÔBO, Paulo Luiz Netto. Constitucionalização do Direito Civil. **Revista de Informação Legislativa**, v. 36, n. 141, p. 99-109, jan/mar. 1999.

MACEDO JÚNIOR, Ronaldo Porto. "in" **Poder econômico:** direito, pobreza, violência, corrupção/organizadores Tercio Sampaio Ferraz Junior, Calixto Salomão Filho, Fabio Nusdeo. — Barueri, SP: Manole, 2009.

MAYER-SCHONBERGER, Viktor. **Delete**: The Virtue of Forgetting in the Digital Age. Princeton, New Jersey: Princeton University Press, 2009.

_____; CUKIER, Kenneth. **Big Data**: A Revolution That Will Transform How We Live, Work and Think. Eamon Dolan/Houghton Mifflin Harcourt Press, 2014.

MORGADO, Laerte Ferreira. **O cenário internacional de proteção de dados pessoais.** Necessitamos de um Código Brasileiro? Disponível em <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=6336>. Acesso em 24/06/2017.

PIMENTEL, Fernando. **O fim da era do petróleo e a mudança de paradigma energético mundial**: perspectivas e desafios para a atuação diplomática brasileira. Brasília: Fundação Alexandre de Gusmão, 2011.

REALE, Miguel. **A teoria tridimensional do Direito**. Lisboa: Imprensa Nacional: Casa da Moeda, 2003.

REIS, Jorge Renato dos; ZIEMANN, Aneline dos Santos. Direitos fundamentais na Sociedade da Informação e a influência dos blogs. **Seminário Nacional Demandas Sociais e Políticas Públicas na Sociedade Contemporânea**, 2016.

RODRIGUES JÚNIOR, Otavio Luiz. **Direito de apagar dados e a decisão do tribunal europeu no caso Google Espanha**. 2014. Disponível em <http://www.conjur.com.br/2014-mai-21/direito-apagar-dados-decisao-tribunal-europeu-google-espanha>. Acesso em 30/05/2017.
SARLO, Lino da Silva. **VPN**: Aprenda a Construir Redes Privadas Virtuais em Plataformas Linux e Windows. São Paulo, Novatec, 2003.

WACHOWICZ, Marcos. **Cultura Digital e Marco Civil da Internet: contradições e impedimentos jurídicos no acesso à informação**. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Ferreira de. **Direito & Internet**. São Paulo: Editora Quartier Latin, 2015. p. 236.

WACHOWICZ, Marcos; LUZ; Pedro. **O "DIREITO À DESINDEXAÇÃO": repercussões do caso Gonzáles vs Google Espanha**. In Revista Espaço Jurídico Journal of Law | EJJL |vol. 19. Número 2 , ano 2018

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. **The Right to Privacy**. Harvard Law Review. Cambridge: Harvard University Press. IV, nº 5, p. 193-217, 1890.

ALGUMAS REFLEXÕES EM MATÉRIA APREENSÃO DE CORREIO ELETRÓNICO E REGISTOS DE COMUNICAÇÃO DE NATUREZA SEMELHANTE

O Acórdão do Tribunal da Relação de Lisboa de 6 de fevereiro de 2018

DUARTE RODRIGUES NUNES [1]

1 Juiz de Direito. Doutor em Direito pela Faculdade de Direito da Universidade de Lisboa. Contacto: duarterodriguesnunes@hotmail.com.

RESUMO

O Tribunal da Relação de Lisboa, no seu Acórdão de 6 de fevereiro de 2018, considerou que o regime da apreensão de correspondência previsto no Código de Processo Penal é aplicável na sua totalidade à apreensão de correio eletrónico e comunicações de natureza semelhante. Os criminosos utilizam as vantagens proporcionadas pelas novas tecnologias para preparar ou executar crimes e suprimir as provas do seu cometimento, usufruindo da rapidez e da volatilidade das novas formas de comunicação à distância. O artigo 17.º da Lei n.º 109/2009, de 15 de setembro, equipara o correio eletrónico e as comunicações de natureza semelhante (SMS e MMS, conversações no *Messenger*, mensagens de voz relativas a comunicações ou arquivos de som e/ou imagem via *Whatsapp, Viber, Skype, Facebook*, etc.) ao correio tradicional para efeitos de apreensão. Pelas enormes diferenças entre o correio eletrónico e o correio tradicional e pelas dificuldades que a aplicação do regime da apreensão de correspondência suscita, a apreensão de correio eletrónico e comunicações de natureza semelhante deveria ser regulada pelo regime geral da apreensão de dados informáticos. O regime da apreensão da correspondência previsto no Código de Processo Penal deverá ser aplicado *cum grano salis* e *mutatis mutandis* à apreensão de correio eletrónico e registos de comunicação de natureza semelhante.

Palavras-Chave: Cibercrime – Prova digital – Correio eletrónico – Apreensão – Direito à intimidade/privacidade.

ABSTRACT

In its Judgment of February 6th, 2018, the Lisbon Court of Appeal found that the seizure of correspondence provided for in the Code of Criminal Procedure is applicable in its entirety to the seizure of electronic mail and communications of a similar nature. Criminals use the advantages offered by new technologies to prepare or execute crimes and suppress evidence, taking advantage of the speed and volatility of new forms of distance communication. Article 17 of Law no. 109/2009, of September 15th, equates electronic mail and communications of a similar nature (SMS and MMS, conversations in *Messenger*, voice messages related to communications or sound files and/or picture via *Whatsapp, Viber, Skype, Facebook*, etc.) to traditional mail for the purpose of seizure. Due to the enormous differences between electronic mail and traditional mail and the difficulties that the application of the regime of seizure of correspondence gives rise to, the seizure of electronic mail and communications of a similar nature should be governed by the general regime for the seizure of computer data. The rules of seizure of correspondence provided for in the Code of Criminal Procedure should be applied *cum grano salis* and *mutatis mutandis* to the seizure of electronic mail and communication records of a similar nature.

Keywords:Cybercrime – Digital evidence – E-mail – Seizure – Privacy.

SUMÁRIO: 1. Introdução. 2. As circunstâncias do caso concreto. 3. A utilidade/necessidade da apreensão de correio eletrónico e registos de comunicação de natureza semelhante para a investigação criminal. 4. O regime da apreensão de correio eletrónico no Direito português. 5. A evolução da regulamentação da apreensão de correio eletrónico no Direito português. 6. Da (des)adequação da equiparação do correio eletrónico ao correio tradicional. 7. Todos os aspetos do regime da apreensão de correspondência deverão ser aplicados, e nos mesmos tempos, à apreensão de correio eletrónico e registos de comunicação de natureza semelhante? 8. Conclusões. Bibliografia. Jurisprudência.

1. INTRODUÇÃO

O Tribunal da Relação de Lisboa, no seu Acórdão de 6 de fevereiro de 2018 (Processo 1950/17.0 T9LSB-A.L1-5)[1], concedeu provimento ao recurso interposto pelo Ministério Público, revogando o despacho recorrido e determinando a sua substituição por outro que determine que o Juiz de Instrução Criminal seja a pessoa a tomar conhecimento em primeiro lugar do correio eletrónico apreendido, disponível, copiado pelo perito, em ficheiros legíveis.

Para tal, o Tribunal entendeu que, sujeitando o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, a apreensão de mensagens de correio eletrónico ou registos de comunicações de natureza semelhante ao regime de apreensão de correspondência previsto no Código de Processo Penal, o n.º 3 o artigo 179.º desse Código estabelece que o juiz que tiver autorizado ou ordenado a diligência é a primeira pessoa a tomar conhecimento do conteúdo da correspondência apreendida, o que, por conseguinte, se aplica ao correio eletrónico já convertido em ficheiro legível, constituindo ato da competência exclusiva do Juiz de Instrução Criminal, nos termos da al. d) do n.º 1 do artigo 268.º do Código de Processo Penal. A inobservância de tal formalidade constitui a sua violação nulidade expressa absoluta e que se reconduz, afinal, ao regime de proibição de prova; ademais, a falta de exame da correspondência pelo juiz constitui uma nulidade prevista na al. d) do n.º 2 do artigo 120.º do Código de Processo Penal, porque se trata de um ato processual legalmente obrigatório.

Mais afirma o Tribunal da Relação de Lisboa que, em caso de urgência, isto é de possível perda de informações úteis à investigação de um crime em caso de demora, o juiz pode

1 *In www.dgsi.pt.*

sempre autorizar a abertura imediata de correspondência (assim como de correio eletrónico) pelo órgão de política criminal, que também poderá ordenar a suspensão da remessa de qualquer correspondência nas estações de correios e de telecomunicações, nos termos dos n.ºs 2 e 3 do artigo 252.º do Código de Processo Penal, devendo a ordem policial ser convalidada no prazo de 48 horas, sob pena de devolução ao destinatário caso não seja atempadamente convalidada, ou caso seja rejeitada a convalidação.

E, em conclusão, afirma-se no aresto sob análise que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, remete expressamente para o regime da apreensão de correspondência previsto no Código de Processo Penal, sem redução do seu âmbito, impondo-se, por isso, a aplicação de tal regime na sua totalidade.

O entendimento do Tribunal da Relação suscita, na nossa ótica, desde logo, as questões (1) da bondade da opção do legislador em submeter a apreensão de correio eletrónico já recebido ao regime da apreensão de correspondência e (2), independentemente de tal bondade, se a remissão que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, opera para o regime de apreensão de correspondência previsto no Código de Processo Penal inclui todo e qualquer aspeto deste regime.

2. AS CIRCUNSTÂNCIAS DO CASO CONCRETO

Com relevância para o presente artigo, as circunstâncias do caso concreto são as seguintes:

a) Por despacho proferido a 16 de março de 2017, o Ministério Público ordenou a realização de buscas não domiciliárias e concedeu autorização para pesquisa, em suportes informáticos, com vista à apreensão de documentação guardada em suporte digital e armazenada em sistema informático;
b) No dia 24 de março de 2017 foram realizadas as buscas ordenadas durante as quais foi efetuada apreensão de variado material informático, dentre ele, computadores, *tablets*, discos externos e efetuada pesquisa informática em equipamentos portáteis, discos e *pen's*;
c) Foi efetuada cópia desses ficheiros com a advertência explícita de que, caso fossem encontradas mensagens de correio eletrónico em tais suportes, as mesmas deveriam ser gravadas em suporte autónomo sem qualquer acesso ou

visualização do respetivo conteúdo, em consonância com o que havia sido judicialmente determinado nos mandados de buscas domiciliárias;

d) A 18 de agosto de 2017, foram copiadas mensagens de correio eletrónico, através de ficheiros encapsulados, para disco rígido autónomo, sem qualquer visionamento do respetivo conteúdo, selado para posterior apreciação judicial;

e) O Ministério Público, a 25 de outubro de 2017, determinou a apresentação de todos os elementos de correio eletrónico colocado em suporte autónomo e revelados pelos exames, para que o Juiz de Instrução Criminal deles tomasse conhecimento em primeiro lugar;

f) O Juiz de Instrução Criminal proferiu o seguinte despacho: «*Tendo sido os e-mails apreendidos na sequência de busca realizada por determinação do Ministério Público tal não significa, por razões de coerência sistemática, que os mesmos tenham de ser visualizados em primeiro lugar pelo Juiz de Instrução Criminal.*

Na verdade, caso os mesmos tivessem sido objecto de intercepção nos termos dos arts. 187.° n° 1 al. a) e 189.° do CPP, poderiam ter sido visualizados pelo OPC e pelo Ministério Público em primeiro lugar, sendo apresentados já após selecção ao Juiz de Instrução Criminal para ulterior validação em conformidade com o art. 188.° n°s 4 e 6 do CPP.

Assim, sendo não se vislumbra fundamento de ordem interpretativa ou sistemática para que os e-mails apreendidos nos termos do art. 17.° da Lei 109/2009 de 15.09 sejam objecto de tratamento diverso, mais garantístico do que o relativo à apreensão directa de telecomunicações, por aplicação estrita do regime do art. 179.° do CPP, remissão que deve ser entendida apenas garante do sigilo profissional, designadamente de Advogado.
Pelo exposto, deverá o OPC proceder à visualização dos e-mails e demais dados apreendidos, devendo apresentar relatório para validação após tal diligência, nos termos e para os efeitos do art. 188.° n°s 4 e 6 do CPP.»;

g) O Ministério Público interpôs recurso de tal despacho, esgrimindo, entre outros, os seguintes argumentos:

- O entendimento plasmado no despacho recorrido viola o disposto nos artigos 17.º da Lei 109/2009, de 15 de setembro, e 179.º, n.º 3 do Código de Processo Penal, normas que exigem que o juiz seja o primeiro a tomar conhecimento do

correio eletrónico copiado, a fim de expurgar dos autos todos os elementos cujo conhecimento esteja vedado aos demais sujeitos processuais;

- A remissão operada pelo artigo 17.º da Lei 109/2009, de 15 de setembro, não poderá significar outra coisa que não a aplicação dos procedimentos para a apreensão de correspondência para a obtenção de prova válida no que respeita ao correio eletrónico;

- O legislador processual separou na Lei do Cibercrime dois regimes distintos, cabendo um para as interceções de correio eletrónico, ao qual são aplicáveis as regras relativas a interceções telefónicas do Código de Processo Penal e o segundo, para as apreensões de correspondência eletrónica, ao qual, também por remissão, são aplicadas as normas de apreensão de correspondência do Código de Processo Penal, pelo que, crendo que o legislador se soube exprimir convenientemente, a cada regime pertencerá um procedimento diverso, não havendo como considerar que um é menos garantístico que o outro, sendo apenas diverso;

3. A UTILIDADE/NECESSIDADE DA APREENSÃO DE CORREIO ELETRÓNICO E REGISTOS DE COMUNICAÇÃO DE NATUREZA SEMELHANTE PARA A INVESTIGAÇÃO CRIMINAL

Como se afirma no Relatório Explicativo da Convenção sobre o Cibercrime[2], «*A revolução nas tecnologias da informação operou mudanças fundamentais na sociedade e irá provavelmente continuar a fazê-lo num futuro previsível. Foram inúmeras as tarefas cuja execução se tornou mais fácil. Enquanto, inicialmente, apenas alguns sectores específicos da sociedade procederam a uma racionalização dos seus métodos de trabalho, com a ajuda das tecnologias da informação, atualmente, não existe praticamente nenhum sector da sociedade que não tenha sido abrangido pelas mesmas. As tecnologias da informação vieram, de uma forma ou de outra, conferir novos contornos a quase todos os aspetos das atividades do Homem.*

2 *In https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf* (pesquisa em 06/06/2018).

Uma característica notável da tecnologia da informação reside no impacto que esta teve, e ainda virá a ter certamente, na evolução da tecnologia das telecomunicações. Os clássicos sistemas telefónicos, envolvendo a transmissão da voz do Homem, foram suplantados por sistemas de permuta de grandes quantidades de dados, incluindo sob a forma de voz, texto e música, assim como de imagens estáticas e móveis. Esta permuta não se dá apenas entre os seres humanos, mas também entre estes e os computadores, e ao nível dos sistemas de computadores entre si. As ligações por comutação de circuitos foram substituídas por ligações por comutação de pacotes. Nos dias de hoje, já não é importante o facto de se poder ou não estabelecer uma ligação direta; basta que os dados em questão sejam introduzidos numa rede com um endereço de destino ou que sejam disponibilizados a todos quantos desejem aceder-lhes.

A utilização universal do correio eletrónico e o acesso aos inúmeros sites através da Internet constituem o exemplo desses desenvolvimentos que tão profundamente contribuíram para a mudança ocorrida na nossa sociedade.

A fácil acessibilidade e pesquisa da informação contida em sistemas informáticos, aliada às possibilidades quase ilimitadas relativamente à sua permuta e difusão, não obstante as distâncias geográficas, traduziu-se por um crescimento explosivo da quantidade de informação disponível e do conhecimento que daí advém.

Estes desenvolvimentos deram origem a mutações sociais e económicas sem precedentes, mas apresentam simultaneamente uma faceta negativa: a emergência de novos tipos de criminalidade, bem como a prática dos crimes tradicionais com recurso às novas tecnologias. Além disso, as consequências do comportamento de índole criminosa poderão ser mais extensas e ter um maior alcance uma vez que não são restringidas por quaisquer limites geográficos ou fronteiras nacionais. A recente disseminação de vírus informáticos prejudiciais, um pouco por todo o mundo, comprova esta realidade. As medidas de carácter técnico que visam proteger os sistemas informáticos deverão, pois, ser tomadas concomitantemente com medidas de natureza jurídica a fim de evitar e deter a prática de crimes.».

De facto, as vantagens proporcionadas pelas novas tecnologias tanto podem ser aproveitadas para fins lícitos como para fins ilícitos, Com efeito, de acordo com o saber adquirido, o correio eletrónico e outros meios de comunicação similares (SMS e MMS, conversações no *Messenger*, mensagens de voz relativas a comunicações ou arquivos de som e/ou imagem via *Whatsapp, Viber, Skype, Facebook*) são amplamente utilizados pelos criminosos para preparar e executar crimes e para suprimir as provas do seu cometimento,

usufruindo da rapidez, anonimato e volatilidade das comunicações informáticas, o que dificulta de sobremaneira a sua deteção e, quando sejam utilizadas medidas antiforenses como a encriptação das mensagens ou o recurso à *Dark Web*, a sua interceção e gravação. Ademais, o correio eletrónico e outros meios de comunicação similares, pela sua natureza de meios de comunicação à distância, permitem suplantar a distância (muitas vezes, na ordem de centenas ou milhares de quilómetros) entre os criminosos comparticipantes e/ou entre os criminosos e as vítimas, para comunicarem entre si ou para cometer crimes que, de outro modo, jamais conseguiriam cometer[3].

Assim, o correio eletrónico e outros meios de comunicação similares, ao permitirem enviar todo o tipo de anexos, poderão ser utilizados para difundir/instalar em sistemas informáticos alheios toda a espécie de *malware*[4], que, uma vez instalado nesses sistemas informáticos, permitirá obter credenciais de acesso (ao *home banking*, a cartões de débito ou crédito, ao *e-mail*, a redes sociais ou a *sites* de natureza reservada que requerem a introdução de uma *password*), copiar ou aceder a dados armazenados nesse sistema (por exemplo, para exercer chantagem sobre a vítima ou para espionagem industrial) ou vigiar toda a atividade aí desenvolvida[5]. E também para abordar as vítimas para, posteriormente, as burlar (como sucedeu com as famosas "Cartas da Nigéria" ou burlas 4-1-9[6]).

Do mesmo modo, no caso da criminalidade organizada transnacional (onde podemos incluir o terrorismo internacional e a grande criminalidade económica, que tende a ser levada a cabo em vários países, incluindo paraísos fiscais), estando os criminosos em países diversos terão de recorrer a meios de comunicação à distância para comunicarem entre si, mas não só.

---

3 *V.g.* burlas cometidas através da Internet ou *phishing*, em que, por exemplo, o criminoso poderá estar num dado país da Europa e as vítimas (muitas vezes, centenas ou milhares de pessoas) poderão estar em qualquer outra parte do Mundo.

De facto, utilizando sistemas informáticos e a Internet, os Cibercriminosos conseguem, fruto da possibilidade de envio de *e-mails* em massa, infetar milhares de sistemas informáticos em todo o Mundo num relativamente curto espaço de tempo. Do mesmo modo, os ataques do tipo DoS (*Denial of Service*) ou DDoS (*Distributed Denial of Service*), que consistem no envio massivo, em simultâneo, de pedidos para um dado sistema informático (ou vários sistemas, no caso do DDoS), só serão possíveis com a utilização de meios que permitam esse envio massivo simultâneo, de molde a que o sistema informático fique desativado por via desse envio massivo de pedidos, que "consome" o CPU e a memória.

4 O *malware* é um programa informático que visa permitir a quem o utiliza infiltrar-se num sistema informático alheio, com o intuito de causar prejuízos ou de obter informações (confidenciais ou não), que, de outro modo, não poderia obter. O *malware* pode aparecer sob a forma de código executável, scripts de conteúdo ativo, etc.

5 Cfr. ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, pp. 24, 35 e 59, e MISHA GLENNY, Darkmarket, p. 11.

6 Relativamente às "burlas 4-1-9-", *vide*, entre outros, ALBANESE, Organized Crime in Our Times, 5.ª Edição, pp. 224-225, e ABADINSKY, Organized crime, 9.ª Edição, p. 206.

Assim, no caso de organizações criminosas transnacionais que se expandem para outros países, muitas vezes utilizando a emigração de nacionais do seu país de origem, os membros da cúpula tendem a estar no país de origem, existindo depois "células" da organização noutros países. Mas também pode suceder que, por via de uma repressão eficaz no país de origem, a "cúpula" da organização tenha de se deslocar para um outro Estado em que a repressão seja menos eficaz ou não exista e tenha necessidade de comunicar com os membros que ficaram no país de origem. E também não podemos esquecer que as organizações criminosas, para se protegerem da atuação das autoridades, costumam manter reservada a identidade dos membros que ocupam as posições mais elevadas na hierarquia, mesmo relativamente aos demais membros ou aos colaboradores externos.

E, no caso das organizações terroristas, o recurso às novas tecnologias de comunicação tanto pode servir para a proteção da organização como para a prossecução da sua finalidade terrorista (*v.g.* para realizar ataques terroristas, propaganda, captação de futuros membros e simpatizantes da causa, comunicação entre o núcleo central as várias "células" independentes e coordenação entre os vários componentes da organização, obtenção de informações úteis para a organização, transferência de capitais, obtenção de lucro por via de burlas cometidas através da Internet, etc.), conferindo uma enorme rapidez e um anonimato absoluto ou quase absoluto às comunicações, potenciando a capacidade operacional da organização e dificultando enormemente a tarefa das entidades cuja missão é evitar os atentados terroristas, desmantelar organizações terroristas e perseguir e punir os seus membros e apoiantes.

Um dos domínios em que mais se lança mão dos meios informáticos para a proteção de criminosos face às autoridades é ao nível do branqueamento de capitais, ao ponto de se afirmar que a informática é um meio *essencial* para o branqueamento e que o branqueamento só se consolidou como atividade conatural da criminalidade organizada com a possibilidade recorrer às novas tecnologias e de se entender que existe uma relação de "conexão necessária" entre a criminalidade organizada, o branqueamento de capitais e a criminalidade informática[7].

Por isso, houve que adaptar as leis penais a estas novas realidades, de molde a permitir a sua regulação jurídica, desde logo mediante a criação de novos tipos de crime informático-digitais (designadamente os previstos nos artigos 4.º a 9.º da revogada Lei n.º 109/91, de 17 de agosto e, atualmente, nos artigos 3.º a 8.º da Lei n.º 109/2009, de 15 de setembro). E, para além

7 Cfr. GUTIÉRREZ FRANCÉS, "Las altas tecnologías de la información al servicio del blanqueo de capitales transnacional", *in* Blanqueo de Dinero y Corrupción en el Sistema Bancario, Delitos Financieros, Fraude y Corrupción en Europa, II, pp. 194-196 e 209.

da alteração das leis penais, houve que criar regras processuais penais, onde se incluem as relativas a meios de obtenção de prova específicos para a investigação destes tipos de crime. Com efeito, dificilmente meios de obtenção de prova criados para obter informações constantes de suportes corpóreos serão adequados para obter informações incorpóreas como aquelas que constam de dados informáticos[8].

Um dos meios de comunicação proporcionados pelas novas tecnologias da informação e comunicação é o correio eletrónico, que, seguindo o conceito legal constante da al. b) do n.º 1 do artigo 2.º da Lei n.º 41/2004, de 18 de agosto, na redação que lhe foi dada pela Lei n.º 46/2012, de 29 de agosto, definimos como «*qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha*». E, *ad latus* do correio eletrónico, encontramos outros veículos de comunicação como as SMS e MMS, conversações

8 Na aceção da al. b) do artigo 2.º da Lei n.º 109/2009, de 15 de setembro, onde se definem dados informáticos como «*qualquer representação 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*».

Na verdade, como se afirma no Relatório Explicativo da Convenção sobre o Cibercrime, « *O presente Artigo visa a modernização e a harmonização das legislações nacionais relativamente à busca e apreensão de dados informatizados armazenados, para fins de obtenção de provas relacionadas com investigações criminais ou ações penais específicas. Qualquer legislação interna em matéria de direito processual penal, contempla os poderes relativos à busca e apreensão de objetos tangíveis. Contudo, em muitos Estados ou jurisdições, os dados informatizados armazenados, por si só, não serão considerados como algo tangível, pelo que não poderão ser adquiridos a título de investigações criminais e ações penais da mesma forma que os bens corpóreos, a não ser através da obtenção do suporte no qual se encontram armazenados os dados. O objetivo do Artigo 19º da presente Convenção é o de estabelecer um poder equivalente relativo aos dados armazenados. (…).*

Todavia, no que se refere à investigação de dados informatizados, são necessárias disposições processuais complementares, a fim de assegurar que os dados informatizados podem ser obtidos com a mesma eficácia de uma operação de busca e apreensão de suportes de dados tangíveis. Existem diversas razões para este facto: em primeiro lugar, os dados são intangíveis, como é o caso dos dados sob a forma eletromagnética. Em segundo lugar, enquanto que os dados podem lidos através da utilização de um equipamento informático, o mesmo não se passa relativamente à apreensão e transporte desses mesmos dados, tal como acontece com um documento em suporte papel. O suporte físico no qual se encontram armazenados os dados intangíveis (por exemplo, o disco rígido de um computador ou uma disquete) deverá ser apreendido e retirado do local, ou deverá ser efetuada uma cópia dos dados, quer sob uma forma tangível (por exemplo, uma impressão feita a partir de um computador) quer sob uma forma intangível, num suporte físico (por exemplo, uma disquete), antes que o suporte tangível que contém a cópia possa ser apreendido e transportado para fora do local. Nos dois últimos casos enunciados, em que são efetuadas cópias dos dados, permanecerá no sistema informático ou na unidade de armazenamento uma cópia dos dados. A legislação nacional deverá instituir o poder relativo à realização das ditas cópias. Em terceiro lugar, devido à conectividade dos sistemas informáticos, os dados poderão não se encontrar armazenados no computador alvo de busca, podendo ser facilmente acessíveis a partir desse mesmo sistema. Os dados poderão ser armazenados numa unidade de armazenamento de dados associada, que se encontre diretamente ligada ao computador, ou indiretamente ligada ao mesmo através do recurso a sistemas de comunicação, tais como a Internet. Tal poderá requerer ou não a implementação de novas leis no sentido de alargar a extensão da busca ao sistema no qual os dados se encontrem efetivamente armazenados (ou da extração dos dados do local em questão para o computador alvo de busca), ou de maneira a permitir a utilização dos tradicionais poderes de investigação, com uma maior rapidez e uma melhor coordenação, em ambos os locais.».

no *Messenger*, mensagens de voz relativas a comunicações ou arquivos de som e/ou imagem via *Whatsapp, Viber, Skype, Facebook,* etc.

Ora, como referimos, no caso de criminosos que se encontrem em locais diversos[9] ou que, por qualquer razão, optem por comunicar entre si à distância em lugar de se encontrarem presencialmente, estes meios de comunicação, pela sua rapidez (permitindo suplantar milhares de quilómetros em apenas alguns segundos), volatilidade e dificuldade de deteção e interceção/gravação são mecanismos que irão ser certamente utilizados. E também poderá ser utilizado para infetar sistemas informáticos com *malware* para obter credenciais de acesso, copiar ou aceder a dados informáticos ou vigiar toda a atividade desenvolvida em sistemas informáticos alheios. Por isso mesmo, a obtenção do conteúdo dessas comunicações será tendencialmente decisivo para o êxito das investigações.

Ciente desta realidade, o legislador português regulou, na Lei n.º 109/2009, de 15 de setembro, diversos meios de obtenção de prova que permitam a tomada de conhecimento do conteúdo dessas comunicações, como sucede com os meios de obtenção de prova previstos nos artigos 17.º (apreensão de correio eletrónico e registos de comunicações de natureza semelhante) e 18.º (interceção de comunicações) dessa Lei. A diferença entre ambos os meios de obtenção de prova radica no facto de, enquanto, no caso da interceção de comunicações, a obtenção de tais informações ocorre no decurso do processo comunicacional, na apreensão de correio eletrónico e registos de comunicações de natureza semelhante [10], o processo comunicacional já terminou.

No presente artigo iremos apenas analisar a apreensão de correio eletrónico e registos de comunicações de natureza semelhante, prevista no artigo 17.º da Lei n.º 109/2009, de 15 de setembro.

9 *V.g.* os membros de uma organização criminosa que se encontrem no país de origem dessa organização face aos membros de células dessa organização que se encontram em países estrangeiros, onde se instalaram aproveitando-se da emigração de nacionais do país onde a organização está sedeada.

10 Cfr. PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, p. 510, RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 274, PEDRO DIAS VENÂNCIO, Lei do Cibercrime, pp. 100 e 116, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, pp. 117 e ss., e Acórdãos da Relação de Lisboa de 11/01/2011 e 29/03/2012, da Relação do Porto de 07/07/2016, da Relação de Évora de 06/01/2015 e 20/01/2015 e da Relação de Guimarães de 29/03/2011, *in www.dgsi.pt*.

4. O REGIME DA APREENSÃO DE CORREIO ELETRÓNICO NO DIREITO PORTUGUÊS.

Nos termos do artigo 17.º da Lei n.º 109/2009, de 15 de setembro, «*Quando, no decurso de uma pesquisa informática ou outro acesso legítimo a um sistema informático, forem encontrados, armazenados nesse sistema informático ou noutro a que seja permitido o acesso legítimo a partir do primeiro, mensagens de correio eletrónico ou registos de comunicações de natureza semelhante, o juiz pode autorizar ou ordenar, por despacho, a apreensão daqueles que se afigurem ser de grande interesse para a descoberta da verdade ou para a prova, aplicando-se correspondentemente o regime da apreensão de correspondência previsto no Código de Processo Penal.*»[11].

Assim, de acordo com o referido preceito, a apreensão de correio eletrónico e registos de comunicações de natureza semelhante (como SMS, MMS, conversações no *Messenger*, mensagens de voz relativas a comunicações via *Whatsapp, Viber, Skype, Facebook, etc.*) que se encontrem armazenados no sistema informático que tenha sido acedido pelas autoridades terá de ser autorizada pelo Juiz, sempre que essa apreensão se mostre de grande interesse para a descoberta da verdade ou para a prova e esteja em causa a investigação de crimes previstos na Lei n.º 109/2009, de 15 de setembro, cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico[12], sendo aplicável o regime da apreensão da correspondência, previsto nos artigos 179.º e 252.º do Código de Processo Penal[13]. Porém, pela especificidade do correio eletrónico face ao correio tradicional, consideramos que a remissão que artigo 17.º da Lei n.º 109/2009, de 15 de setembro, opera para o regime da apreensão da correspondência previsto no Código de

11 Contudo, sempre que a pessoa que tenha recebido as mensagens de correio eletrónico ou os registos de comunicações de natureza semelhante preste consentimento para que as autoridades tomem conhecimento do teor das mesmas e sejam transcritas e juntas aos autos ou proceda ela própria à junção aos autos da mensagem em causa, não há que aplicar o regime do artigo 17.º da Lei n.º 109/2009, de 15 de setembro (cfr. Acórdãos da Relação de Lisboa de 29/03/2012 e da Relação do Porto de 22/05/2013, *in www.dgsi.pt*).

12 Ou seja, este meio de obtenção de prova poderá ser aplicado a um universo de crimes aberto (cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 147, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, p. 98, e Acórdãos da Relação de Évora de 06/01/2015 e 20/01/2015, *in www.dgsi.pt*).

13 Cfr. PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, p. 510, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, p. 118, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 765, e Acórdãos da Relação de Lisboa de 11/01/2011 e 06/02/2018, *in www.dgsi.pt*; contra, ARMANDO RAMOS, "Do *periculum in mora* da atuação da Autoridade Judiciária ao *fumus boni iuris* da intervenção policial", *in* IV Congresso de Processo Penal, pp. 56-57.

Processo Penal deverá ser lida *cum grano salis* e *mutatis mutandis*[14] e sem prejuízo de tal opção legislativa ser de bondade muito duvidosa.

5. A EVOLUÇÃO DA REGULAMENTAÇÃO DA APREENSÃO DE CORREIO ELETRÓNICO NO DIREITO PORTUGUÊS

A Lei n.º 109/2009, de 15 de setembro, regulou, pela primeira vez, no nosso ordenamento jurídico, meios de obtenção de prova em matéria de Cibercrime[15], apesar de a Convenção sobre o Cibercrime já datar de 23/11/2001 (tendo sido assinada por Portugal nessa mesma data) e ter entrado em vigor em 01/07/2004[16] e de ser inequívoca a insuficiência dos meios de obtenção de prova previstos no Código de Processo Penal (claramente pensados para a obtenção de provas "corpóreas") para investigar eficazmente a criminalidade informática, mas não só.

Antes da entrada em vigor da Lei n.º 109/2009, de 15 de setembro, e até à entrada em vigor das alterações introduzidas no Código de Processo Penal pela Lei n.º 48/2007, de 29 de agosto, na ausência de regulamentação em matéria de apreensão de correio eletrónico, a

14 No que tange ao regime jurídico da apreensão de correio eletrónico e registos de comunicações de natureza semelhante, com maiores desenvolvimentos, *vide* DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, pp. 139 e ss.

15 Em que, adotando um conceito amplo, incluímos os crimes que ofendem bens diretamente ligados ao meio informático (*v.g.* o acesso ilegítimo), que visam proteger o próprio uso da informática e os seus aspetos característicos como o *software* e a navegação na Internet, bem como os crimes que lesam bens jurídicos "tradicionais" (*v.g.* a honra ou o património), mas que são cometidos através do uso de sistemas informáticos (o que aumenta especialmente a perigosidade ou danosidade para os bens jurídicos lesados e dificulta a deteção do seu cometimento e da identidade do agente, justificando a especial atenção do Direito penal). De resto, fazendo cada vez menos sentido diferenciar o plano do Direito penal material do plano do Direito processual penal, a delimitação do conceito de Cibercrime deverá ter em conta, por um lado, a determinação das condutas criminosas que devam ser incluídas no âmbito da criminalidade informática e, por outro, a determinação das condutas criminosas relativamente às quais se mostre necessário lançar mão de meios investigatórios especificamente direcionados para a obtenção de prova digital.

E, se atentarmos na Lei n.º 109/2009, de 15 de setembro, verificamos que o legislador adotou um conceito amplo de Cibercrime, pois, por um lado, apenas incluiu nela condutas criminosas em que o elemento digital surge como parte integradora do tipo legal e como seu objeto de proteção, mas, na vertente processual penal, determinou, no n.º 1 do artigo 11.º, que, salvo no caso da interceção de comunicações eletrónicas (artigo 18.º) e das ações encobertas em ambiente informático-digital (artigo 19.º), os meios de obtenção de prova aí previstos aplicam-se a processos relativos a crimes previstos nessa lei e também a crimes cometidos por meio de um sistema informático e a crimes em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

E o mesmo sucede com os autores da Convenção sobre o Cibercrime, atento o elenco legal de condutas cuja criminalização é imposta e o âmbito das disposições processuais penais e relativas à cooperação judiciária em matéria penal.

16 Sendo que a introdução na nossa ordem jurídica, de meios de obtenção de prova específicos para a investigação do Cibercrime não dependia, nem da entrada em vigor da Convenção nem da sua transposição para o Direito português.

Doutrina e a Jurisprudência defendiam a aplicação dos meios de obtenção de prova "tradicionais" (designadamente os previstos no Código de Processo Penal) na investigação do Cibercrime, sendo que, no que tange à apreensão de mensagens de correio eletrónico, defendia-se a equiparação, em termos de regime jurídico, do correio eletrónico ao correio tradicional[17].

Na medida em que, pela generalização do uso deste meio de comunicação à distância, a apreensão de correio eletrónico se revelava cada vez mais essencial para investigar a prática de crimes, era esta a única forma de, de acordo com a lei vigente, viabilizar a utilização deste meio de obtenção de prova.

Ciente da necessidade de regular a apreensão do correio eletrónico, o legislador, com a reforma de 2007 do Código de Processo Penal, regulou pela primeira vez a apreensão de correio eletrónico. Assim, no n.º 1 do artigo 189.º, determinou que a apreensão de correio eletrónico, ainda que armazenado em suporte digital[18], é regulada pelo regime das escutas telefónicas, operando, desse modo, uma equiparação do correio eletrónico às escutas telefónicas. No fundo, o legislador submeteu ao regime das escutas telefónicas, quer a interceção em tempo real quer a apreensão das mensagens de correio eletrónico, ou seja, submeteu ao regime de um meio de obtenção de prova cuja utilização implica uma intervenção num processo comunicacional alheio (as escutas telefónicas) uma situação em que ocorre uma tal intervenção (interceção em tempo real de mensagens de correio eletrónico) e outra em que tal não ocorre (apreensão das mensagens de correio eletrónico).

Todavia, apesar de ser louvável a intenção do legislador de regular a apreensão (e a interceção) de correio eletrónico, um tal regime só poderia ter-se por desajustado no que tange à apreensão de correio eletrónico já recebido pelo destinatário, por várias razões.

---

17 Cfr. PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 165, e também em "Apreensão de correio electrónico em Processo Penal", *in* Revista do Ministério Público, *passim*, MOURAZ LOPES, Garantia Judiciária no Processo Penal, p. 43, PEDRO DIAS VENÂNCIO, Breve introdução da questão da investigação e meios de prova na criminalidade informática, pp. 22-23, e Acórdãos da Relação de Lisboa de 13/10/2004 e 15/07/2008 e da Relação de Coimbra de 29/03/2006, *in www.dgsi.pt*.

18 CARLOS ADÉRITO TEIXEIRA, "Escutas Telefónicas: A Mudança de Paradigma e os Velhos e os Novos Problemas", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 283, e PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, pp. 166-168, entendiam que, no caso de mensagens já impressas e que fossem apreendidas em suporte papel, não havia lugar à aplicação do artigo 189.º do Código de Processo Penal, uma vez que, para além de já não se tratar de uma comunicação, os dados de conteúdo não estavam guardados em suporte digital; em tais casos, haveria que aplicar o regime das apreensões. De todo o modo, como refere DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, pp. 90 e ss., não se percebe o porquê de o n.º 1 do artigo 189.º do Código de Processo Penal apenas abranger o armazenamento em suporte digital quando muitos escritos ou imagens em suporte papel podem apresentar características idênticas aos guardados em suporte digital no que diz respeito às relações de confiança comunicacional.

Em primeiro lugar, uma comunicação é, por natureza, uma realidade dinâmica (tratando-se de um processo comunicacional, que vai de um lado ao outro, desde o emissor ao recetor) e não estática e, como tal, não poderá estar guardada; quando muito, o que poderá estar guardado é o seu registo ou o seu produto[19].

Em segundo lugar, uma vez chegada a comunicação à "esfera de domínio" do destinatário, o processo comunicacional extingue-se e os dados de conteúdo da comunicação ficam armazenados como qualquer outro documento (no caso do correio eletrónico, o ficheiro do *e-mail* recebido é, em tudo, semelhante a um qualquer outro ficheiro guardado no computador, devendo ser tratado como um mero documento[20]), sendo, por isso, apreendidos e não intercetados[21].

Em terceiro lugar, o regime também era aplicável a comunicações já "abertas" (*i.e.* cujo conteúdo já é do conhecimento do destinatário[22]), ou seja, num momento em que já não existe qualquer tutela no âmbito do direito à inviolabilidade da correspondência e de outros meios de comunicação privada, pois já não se está naquela "específica situação de perigo" e de carência de tutela da proteção constitucional deste direito fundamental de que fala COSTA ANDRADE; ora, daqui resultava a manutenção do sigilo das comunicações *ad aeternum*, de que resultava uma enorme disfuncionalidade entre regimes paralelos (o regime das apreensões e o regime da intervenção nas comunicações)[23], que, por motivos óbvios, é de evitar ao máximo.

Em quarto lugar, este regime criava enormes dificuldades operacionais de implementação perfeitamente evitáveis e que podiam ter graves repercussões (negativas) ao nível da investigação criminal[24]. Assim, se, no decurso de uma busca, fosse apreendido um

19 Cfr. PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 164, e também em "A Reforma Penal Portuguesa e o Cibercrime", *in* Revista do Ministério Público, n.º 108, p. 121, e SANTOS CABRAL, "Art. 189º", *in* Código de Processo Penal, pp. 835-836.

20 Assim, COSTA ANDRADE, "Art. 194.º", *in* Comentário Conimbricense, I, 2.ª Edição, p. 1097, SANTOS CABRAL, "Art. 189º", *in* Código de Processo Penal, pp. 835-836, e PEDRO VERDELHO, "A Reforma Penal Portuguesa e o Cibercrime", *in* Revista do Ministério Público, n.º 108, p. 121.

21 Cfr. PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 164, e SANTOS CABRAL, "Art. 189º", *in* Código de Processo Penal, pp. 835-836.

22 E, como tal, perfeitamente similar a uma carta já aberta e lida pelo destinatário, em que já não se aplica o regime da apreensão da correspondência.

23 Cfr. PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 165, e também em "A Reforma Penal Portuguesa e o Cibercrime", *in* Revista do Ministério Público, n.º 108, p. 122.

24 Assim, COSTA ANDRADE, "Bruscamente no Verão Passado", pp. 185-186, PEDRO VERDELHO, "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, n.º 9, p. 165, e também em "A Reforma Penal Portuguesa e o Cibercrime", *in* Revista do Ministério Público, n.º 108, p. 123, ANDRÉ LAMAS LEITE, "Entre Péricles e Sísifo: o novo regime legal das escutas telefónicas", *in* Revista

computador, no qual estivessem guardadas mensagens de correio eletrónico, haveria que solicitar ao Juiz de Instrução Criminal autorização para proceder à "leitura" dessas mensagens, o que, implicando alguma perda de tempo entre o momento em que a apreensão era feita e o momento em que o acesso fosse autorizado, poderiam ocorrer perdas graves ao nível da eficácia da investigação.

Com a entrada em vigor da Lei n.º 109/2009, de 15 de setembro, o legislador optou por, no artigo 17.º, determinar a aplicação do regime da apreensão de correspondência à apreensão de correio eletrónico e registos de comunicação de natureza semelhante, sancionando a equiparação do correio eletrónico ao correio tradicional e abandonando a equiparação às escutas telefónicas que tinha operado no Código de Processo Penal. Contudo, apesar da entrada em vigor da Lei n.º 109/2009, de 15 de setembro, a redação do n.º 1 do artigo 189.º do Código de Processo Penal manteve-se inalterada. De todo o modo, consideramos que o n.º 1 do artigo 189.º do Código de Processo Penal, na parte em que se refere a correio eletrónico e aos registos de comunicação de natureza semelhante foi tacitamente revogado pelos artigos 17.º e 18.º da Lei n.º 109/2009, de 15 de setembro, pelo que o legislador optou por abandonar a equiparação da apreensão de correio eletrónico às escutas telefónicas.

Esta opção do legislador não corresponde à transposição de qualquer norma da Convenção sobre o Cibercrime[25], sendo uma criação do legislador português ao abrigo da sua liberdade de conformação. De seguida, analisaremos criticamente esta opção legislativa.

6. DA DESADEQUAÇÃO DA EQUIPARAÇÃO DO CORREIO ELETRÓNICO AO CORREIO TRADICIONAL

A primeira reflexão que o aresto em análise nos suscita prende-se com a adequação, ou não, da equiparação do correio eletrónico ao correio tradicional em termos de regime, sendo que a opção legislativa contida no artigo 17.º da Lei n.º 109/2009, de 15 de setembro, ao proceder a tal equiparação, se nos afigura pouco acertada.

Portuguesa de Ciência Criminal, 2007, p. 662, e MAGISTRADOS DO MINISTÉRIO PÚBLICO DO DISTRITO JUDICIAL DO PORTO, Código de Processo Penal, p. 508.

25 Porém, PEDRO DIAS VENÂNCIO, Lei do Cibercrime, p. 116, considera que o artigo 17.º, conjuntamente com os artigos 15.º e 16.º da Lei n.º 109/2009, engloba-se no artigo 19.º da Convenção sobre o Cibercrime.

Assim, desde logo, a apreensão de correspondência regulada no Código de Processo Penal consiste na retirada do circuito normal do correio[26] do suporte através do qual se efetua uma comunicação postal ou telegráfica, impedindo que chegue ao seu destinatário (e, por isso, o processo comunicacional terá de estar em curso[27]), pelo que restringe o direito à inviolabilidade da correspondência[28]. Por isso, a apreensão da correspondência ainda não enviada pelo remetente, entregando-a de qualquer forma (*v.g.* depositando-a no marco do correio) ao operador do serviço postal não segue o regime especial da apreensão da correspondência[29], pois o processo comunicacional ainda não se iniciou e, como tal, o suporte que corporiza a comunicação não está protegido pelo direito à inviolabilidade da correspondência. E o mesmo se aplica à que já foi recebida pelo destinatário[30].

Ora, diversamente da apreensão de correspondência, a apreensão de correio eletrónico e registos de comunicação de natureza semelhante não se aplica à obtenção, em tempo real, de correio eletrónico, SMS, etc. (que serão obtidos através da interceção de comunicações, regulada no artigo 18.º da Lei n.º 109/2009, de 15 de setembro), mas à obtenção de correio eletrónico, SMS, etc. que já foi recebido pelo destinatário e que estão armazenados no sistema informático que foi legitimamente acedido pelas autoridades. Daí que a apreensão de correio eletrónico e registos de comunicação de natureza semelhante restrinja os direitos à intimidade/privacidade, à palavra virtual e à autodeterminação informacional, mas não o direito à inviolabilidade das comunicações[31]. Na verdade, o direito à inviolabilidade da

---

26 Cfr. PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, p. 509, e BENJAMIM SILVA RODRIGUES, Das Escutas Telefónicas, II, p. 72.

27 Cfr. DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, p. 117, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 765, e SCHÄFER, "§99", *in* Löwe-Rosenberg Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 2.º Vol., 25.ª Edição, pp. 306 e 309-310.

28 Cfr. ROXIN/SCHÜNEMANN, Strafverfahrensrecht, 27.ª Edição, p. 281, MEYER-GOSSNER, Strafprozessordnung, 56.ª Edição, p. 367, BENJAMIM SILVA RODRIGUES, Das Escutas Telefónicas, II, p. 72, SIMAS SANTOS/LEAL-HENRIQUES, Código de Processo Penal Anotado, Vol. I, 3.ª Edição, p. 1154, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 763, e Acórdãos do Supremo Tribunal de Justiça de 18/05/2006 e da Relação de Lisboa de 20/12/2011, *in www.dgsi.pt*.

29 Cfr. ROXIN/SCHÜNEMANN, Strafverfahrensrecht, 27.ª Edição, p. 283, BENJAMIM SILVA RODRIGUES, Das Escutas Telefónicas, II, p. 72, SCHÄFER, "§99", *in* Löwe-Rosenberg Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 2.º Vol., 25.ª Edição, pp. 306 e 309-310, e CORDERO, Procedura Penale, 8.ª Edição, p. 843.

30 Cfr. COSTA ANDRADE, "Art. 194.º", *in* Comentário Conimbricense, I, 2.ª Edição, p. 1087, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 763, BENJAMIM SILVA RODRIGUES, Da Prova Penal, II, p. 330, RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 187, e EISENBERG, Beweisrecht der StPO, 5.ª Edição, p. 811.

31 Cfr. PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 509 e 542, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, pp. 117-118, COSTA ANDRADE, "Bruscamente no Verão Passado" pp. 159-160, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, pp. 763 e 765, CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 40-41, e Acórdãos da Relação de Lisboa de 02/03/2011, 29/03/2012 e 24/09/2013, da Relação do Porto de 07/07/2010 e 22/05/2013 e da Relação de Guimarães de 15/10/2012, *in www.dgsi.pt*.

correspondência e de outros meios de comunicação privada consiste na proibição de terceiros[32] se intrometerem, tomarem conhecimento, registarem, utilizarem ou divulgarem o conteúdo de comunicações privadas[33] realizadas por qualquer meio[34] que tenham um emissor e um recetor ou círculo de recetores previamente determinado[35], terminando a tutela deste direito fundamental no momento em que o processo comunicacional termina, *i.e.* quando a comunicação chega ao "aparelho terminal" (*Endgerät*) ou é entregue ao destinatário[36].

Assim, ocorrendo a apreensão num momento em que o processo comunicacional já terminou e, como tal, quando já não existe a específica situação de perigo e de carência da proteção constitucional da inviolabilidade das comunicações, a apreensão de correio eletrónico e registos de comunicação de natureza semelhante não restringe o direito à inviolabilidade da correspondência e de outros meios de comunicação privada. E, por isso, não se justifica a sujeição de um meio de obtenção de prova que não configura qualquer intromissão num processo comunicacional alheio ao regime de um meio de obtenção de prova cuja utilização passa precisamente por uma tal intromissão.

Também não vemos em que medida o correio eletrónico já recebido será diferente de outros dados informáticos (*v.g.* ficheiros contendo documentos resultantes de um processador

32 Daí que quando um dos interlocutores da conversação ou comunicação grava a mesma ou conta às autoridades aquilo que ouviu dizer ao outro interlocutor não ocorre nenhuma lesão deste direito (cfr. COSTA ANDRADE, "Bruscamente no Verão Passado" pp. 158-159, sendo que a inviolabilidade das comunicações nada tem a ver com a garantia de que o outro interlocutor mantenha reserva sobre o conteúdo da comunicação, o que, por sua vez, nada tem a ver com a inviolabilidade da correspondência e de outros meios de comunicação (cfr. COSTA ANDRADE, *Op. e Loc. Cit.*).

33 GOMES CANOTILHO/VITAL MOREIRA, Constituição Anotada, I, 4.ª Edição, pp. 544-546.

34 Cfr. GERMANO MARQUES DA SILVA/FERNANDO SÁ, "Art. 34.º", *in* Constituição Anotada, I, 2.ª Edição, p. 772. Assim, incluem-se aqui os mais sofisticados meios de comunicação de mensagens e os respetivos dados eletrónicos (cfr. JARASS/PIEROTH, Grundgesetz Kommentar, pp. 305-306, CONDE CORREIA, "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art. 32.º, n.º 8, 2.ª parte, da CRP)?", *in* Revista do Ministério Público, n.º 79, p. 51, DORSCH, Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, p. 7, GONZÁLEZ-CUÉLLAR SERRANO, "Garantías constitucionales de la persecución penal en el entorno digital", *in* Prueba y Proceso Penal, p. 165, e Acórdão Wieser e Bicos Beteiligungen GmbH c. Áustria do TEDH, *in www.echr.coe.int*).

35 Cfr. GOMES CANOTILHO/VITAL MOREIRA, Constituição Anotada, I, 4.ª Edição, p. 544, GERMANO MARQUES DA SILVA/FERNANDO SÁ, "Art. 34.º", *in* Constituição Anotada, I, 2.ª Edição, p. 772, e Acórdãos do Tribunal Constitucional n.º 403/2015, *in www.tribunalconstitucional.pt*, do Supremo Tribunal de Justiça de 03/03/2010 e da Relação do Porto de 22/05/2013 e 03/12/2013, *in www.dgsi.pt*.

36 Cfr. PINTO DE ALBUQUERQUE, Comentário do Código de Processo Penal, 4.ª Edição, pp. 509 e 542, FRIGOLS I BRINES, "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", *in* La Protección Jurídica de la Intimidad, pp. 55 e 62 e ss., SCHROEDER, Strafprozessrecht, 4.ª Edição, p. 82, BÄR, TK-Überwachung, p. 36, DURNER, "Art. 10", *in* Maunz-Dürig Grundgesetz Kommentar, II, pp. 47-48 e 52, Acórdãos da Relação de Lisboa de 02/03/2011, da Relação do Porto de 03/04/2013, 24/04/2013, 22/05/2013 e 03/12/2013 e da Relação de Coimbra de 02/03/2005, *in www.dgsi.pt*, e Sentença do *Grosse Senat für Strafsachen do Bundesgerichtshof* de 13/05/1996, *in* BGHSt, 42, pp. 139 e ss.

de texto, folha de cálculo ou de um programa para criação ou apresentação digital de *slides*[37]), cuja apreensão ocorre à luz do regime do artigo 16.º da Lei n.º 109/2009) e que também poderão incluir informações de cariz privado ou até íntimo, não se percebendo o porquê de o Ministério Público poder autorizar a apreensão de correspondência ou de uma cópia em suporte papel de um *e-mail* guardado num cofre e ser necessária autorização do Juiz de Instrução Criminal para se apreender um *e-mail* guardado num computador[38].

Nem podemos olvidar que poderão estar armazenados no sistema informático outros dados informáticos de conteúdo muito mais sensível, em termos de intimidade/privacidade, do que as mensagens de correio eletrónico e, no entanto, o legislador optou por submeter a sua apreensão à disciplina do artigo 16.º da Lei n.º 109/2009, de 15 de setembro, considerando que o mecanismo previsto no n.º 3 desse preceito é suficiente para a salvaguarda do direito à intimidade/privacidade e do direito à autodeterminação informacional. De resto, nos casos previstos no n.º 3 do artigo 16.º da Lei n.º 109/2009, de 15 de setembro, a intervenção do Juiz apenas poderá ocorrer *a posteriori* do conhecimento desses dados informáticos pelo órgão de polícia criminal (pois só o seu conhecimento poderá levar a concluir que contém dados pessoais ou íntimos e que, como tal, a sua junção aos autos terá de ser judicialmente autorizada), pese embora se possa tratar de dados de cariz muito mais sensível do que muitas, porventura a maioria das mensagens de correio eletrónico.

E a aplicação do regime da apreensão de correspondência gera uma descontinuidade, em termos de regime legal, entre a correspondência física aberta e lida pelo destinatário e o correio eletrónico recebido e lido pelo destinatário, pois, após ser recebida, a correspondência física torna-se num mero documento e está sujeita a apreensão nos termos gerais, ao passo que a apreensão do correio eletrónico continua sujeita ao regime muito mais garantístico da apreensão de correspondência[39]. E será certamente por isso que, a fim de minimizar os efeitos nefastos da opção legislativa, não falta quem, considerando que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, deverá ser interpretado de forma hábil, entenda que a remissão para o regime da apreensão de correspondência só deverá ter lugar nos casos em que o *e-mail*, SMS, MMS, etc., apesar de já recebidos, ainda não tenham sido abertos pelo destinatário, como sucede com a correspondência (que, uma vez aberta pelo destinatário, poderá ser apreendida

37 Cfr. ROGÉRIO BRAVO, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in* Polícia e Justiça, n.º 7, p. 209.
38 Cfr. CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, p. 41.
39 Cfr. RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 277.

nos termos gerais como qualquer outro documento e não à luz do artigo 179.º do Código de Processo Penal)[40], entendimento que subscrevemos *de jure condito*. E, do mesmo modo, subscrevemos o entendimento de SANTOS CABRAL quando afirma que, «*A mensagem recebida em telemóvel, atenta a natureza e finalidade do aparelho e o seu porte pelo arguido no momento da revista, é de presumir que, uma vez recebida, foi lida pelo seu destinatário*»[41].

E, para além de não se justificar aplicar um meio de obtenção de prova que configura uma intervenção nas comunicações a uma situação em que inexiste qualquer intervenção nas comunicações, não podemos olvidar que, no plano das consequências, tal opção do legislador acaba por gerar enormes dificuldades à investigação, quando a finalidade da Lei n.º 109/2009, de 15 de setembro, era (também) simplificar a investigação do Cibercrime.

Assim, do ponto de vista operacional, será extremamente difícil aplicar o regime da apreensão de correspondência à abertura e tomada de conhecimento do teor das comunicações eletrónicas[42], pois, podendo os *e-mails* ser em grande número e apenas alguns terem relevância para a investigação, a sua prévia abertura, leitura e posterior seleção para servirem como prova por parte do juiz tenderá a ser uma tarefa verdadeiramente titânica e, no caso de ocorrer na fase de inquérito, os investigadores (polícias) terão um muito melhor conhecimento da investigação (o que muito auxiliará na hora de selecionar quais os *e-mails* cujo conteúdo é relevante para a investigação) do que o Juiz de Instrução Criminal, que apenas intervém pontualmente[43].

E, se a apreensão ocorrer no local onde estão guardados os dados, os investigadores teriam de, à cautela, ser acompanhados pelo Juiz de Instrução Criminal ou, logo que detetassem a existência de correio eletrónico, teriam de contactar o Juiz de Instrução Criminal para este se deslocar ao local ou teriam de apreender e transportar os computadores, para o Juiz de Instrução Criminal poder visionar os *e-mails*, o que, em termos logísticos é dificilmente exequível. De resto, na medida em que a apreensão terá lugar na sequência de uma pesquisa informática ou

40 PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Edição, pp. 509 e 542, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, pp. 117-118, COSTA ANDRADE, "Bruscamente no Verão Passado" pp. 159-160, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, pp. 763 e 765, CONDE CORREIA, "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 40-41, e Acórdãos da Relação de Lisboa de 02/03/2011 e 24/09/2013, e da Relação de Guimarães de 15/10/2012, *in www.dgsi.pt*; contra, Acórdãos da Relação do Porto de 12/09/2012 e da Relação de Guimarães de 29/03/2011, *in www.dgsi.pt*.

41 SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 765.

42 Cfr. RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, pp. 185 e 275.

43 Daí que, neste ponto, o regime do artigo 17.º da Lei n.º 109/2009, de 15 de setembro, seja ainda mais nocivo para a investigação do que o regime das escutas telefónicas, tendo em conta o disposto nos n.ºs 1 a 5 do artigo 188.º do Código de Processo Penal.

de outro acesso legítimo a um sistema informático[44] e porque o modo habitual de apreensão dos dados informáticos existentes num sistema informático no decurso dessa diligência é realizando um "clone" do suporte que contém esses dados, sendo que a ferramenta forense utilizada não irá distinguir entre mensagens de correio eletrónico e outros dados informáticos e só quando o perito procede à análise dos dados apreendidos é que deparará com as mensagens de correio eletrónico[45]. E essa circunstância é claramente visível na situação *sub juditio* no aresto de cuja análise nos ocupamos, em que a cópia dos dados existentes no sistema informático foi realizada logo no dia em que a pesquisa foi realizada (24/03/2017) e a extração/gravação dos dados que respeitavam a mensagens de correio eletrónico apenas foi realizada no dia 18/08/2017, certamente quando se procedeu à análise dos dados apreendidos.

Igualmente do ponto de vista técnico, também não se justifica equiparar o correio eletrónico a realidades análogas à correspondência "tradicional". Na verdade, fruto da sua natureza digital, a abertura de um *e-mail* nada tem a ver com a abertura de um sobrescrito contendo uma carta[46] e a cifra nada tem a ver com um envelope ou outro invólucro corpóreo[47], sendo que, no plano estritamente técnico, um *e-mail* jamais poderá ser equiparado à correspondência "tradicional"[48], como demonstram à saciedade aspetos como a filtragem de mensagens, a possibilidade de envio em massa de mensagens de correio eletrónico, as mensagens recebidas (e abertas) por engano ou as mensagens privadas enviadas através de *Webmail*[49]. O correio eletrónico não utiliza as redes postais públicas, mas serviços de comunicações eletrónicas acessíveis ao público. Do mesmo modo, atento o elenco de realidades que podem ser objeto de apreensão de correspondência (cartas, encomendas, valores, telegramas), o artigo 179.º do Código de Processo Penal está claramente pensado para

44 A que poderemos subsumir a recolha dos dados informáticos por um especialista no local onde se encontra o sistema informático ou o suporte autónomo, a busca "tradicional" ou a revista (nos termos dos artigos 174.º e ss. do Código de Processo Penal) ou o acesso ao sistema informático ou ao suporte autónomo por via de uma injunção para apresentação ou concessão do acesso a dados (cfr. DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 118, e DAVID RAMALHO, Métodos Ocultos de Investigação Criminal em Ambiente Digital, pp. 133-134).

45 Cfr. ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, p. 94.

46 Cfr., entre outros, COSTA ANDRADE, "Bruscamente no Verão Passado" p. 159, BENJAMIM SILVA RODRIGUES, Das Escutas Telefónicas, II, pp. 341 e ss., ARMANDO RAMOS, "Do *periculum in mora* da atuação da Autoridade Judiciária ao *fumus boni iuris* da intervenção policial", *in* IV Congresso de Processo Penal, p. 56 (nota 21), e também em A prova digital em processo penal: O correio eletrónico, pp. 47 e ss., e ROGÉRIO BRAVO, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in* Polícia e Justiça, n.º 7, *passim*.

47 Cfr. ROGÉRIO BRAVO, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in* Polícia e Justiça, n.º 7, p. 212.

48 *Vide* os argumentos de caráter técnico aduzidos por ROGÉRIO BRAVO, "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in* Polícia e Justiça, n.º 7, pp. 214 e ss., e ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, pp. 58 e ss.

49 Cfr. ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, pp. 56 e ss.

a apreensão de realidades físicas e não virtuais[50] e não nos parece que, após ter sido visionado e considerado irrelevante para a investigação, o correio eletrónico possa ser restituído na verdadeira aceção da palavra ao destinatário (que poderá aceder-lhe sem necessidade de restituição e independentemente de ter sido alvo de apreensão)[51]. De resto, em termos de específica situação de perigo e de carência da proteção constitucional da inviolabilidade das comunicações, ao contrário do que sucede com a correspondência física, o destinatário, ao receber a mensagem, pode dispor de meios de autodefesa para se proteger de infiltrações de terceiros, como a instalação de sistemas de segurança, programas antivírus, codificação críptica, *firewalls* ou o apagamento ou a destruição dos dados, que nada têm a ver com uma caixa de correio equipada com fechadura, sendo que, no caso do correio eletrónico, só poderá ser recebido por via de um sistema informático que poderá estar equipado com os mencionados dispositivos, ao passo que o correio tradicional até poderá ser entregue em mão a um terceiro que, depois, o entregará ao destinatário.

Por isso, *de jure condendo*, a apreensão de correio eletrónico e comunicações de natureza semelhante deveria ocorrer à luz do artigo 16.º da Lei n.º 109/2009, de 15 de setembro (constituindo o seu n.º 3 salvaguarda suficiente em matéria de correio eletrónico e realidades análogas), pois já não nos encontramos no âmbito de um processo comunicacional[52]. De todo o modo, como referimos, mesmo *de jure condito*, a fim de minimizar os efeitos nefastos da opção legislativa, entendemos que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, deverá ser interpretado de forma hábil, só se aplicando o regime da apreensão de correspondência nos casos em que o *e-mail*, SMS, MMS, etc., apesar de já recebido, ainda não tenha sido aberto pelo destinatário, sendo de presumir que, uma vez recebido, já foi lido pelo seu destinatário.

50 Cfr. RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 185, que refere que, em face dos exemplos dados pelo legislador, a "qualquer outra correspondência" não incluirá realidades meramente virtuais.
51 Cfr. RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 185.
52 No mesmo sentido, ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, p. 113.

7. TODOS OS ASPETOS DO REGIME DA APREENSÃO DE CORRESPONDÊNCIA DEVERÃO SER APLICADOS, E NOS MESMOS TEMPOS, À APREENSÃO DE CORREIO ELETRÓNICO E REGISTOS DE COMUNICAÇÃO DE NATUREZA SEMELHANTE?

A segunda reflexão que o aresto sob análise suscita é relativa à questão de saber se a remissão que artigo 17.º da Lei n.º 109/2009, de 15 de setembro, opera para o regime da apreensão da correspondência previsto no Código de Processo Penal abrange todos os aspetos desse regime e se tal regime deverá ser aplicado à apreensão de correio eletrónico e registos de comunicação de natureza semelhante nos mesmos termos em que se aplica à apreensão da correspondência "tradicional".

Antes de entrarmos na análise da questão, desde já diremos que, pelas grandes diferenças entre a correspondência "tradicional" e o correio eletrónico que elencámos (e que desaconselham qualquer equiparação em termos de regime jurídico), essa remissão deverá ser sempre lida *cum grano salis* e *mutatis mutandis*.

Assim, no que tange à competência autorizativa, ainda que a remissão não a abranja (pois a autorização judicial é expressamente referida no artigo 17.º da Lei n.º 109/2009, de 15 de setembro), no caso da apreensão de correspondência, a autorização terá de ser prévia à realização da diligência, o que será sempre possível, dado que a diligência é especificamente dirigida à apreensão da correspondência. Diversamente, no caso da apreensão de correio eletrónico e registos de comunicação de natureza semelhante, a apreensão tem lugar na sequência de uma pesquisa informática ou de outro acesso legítimo a um sistema informático, que, no inquérito, são autorizados pelo Ministério Público, sendo que não se sabe se, na sequência dessa pesquisa ou acesso serão apreendidos mensagens de correio eletrónico ou registos de comunicação de natureza semelhante ou se apenas serão apreendidos dados informáticos de outro tipo (submetidos ao regime do artigo 16.º da Lei n.º 109/2009, de 15 de setembro, sendo que a intervenção do Juiz prevista no n.º 3 desse preceito apenas ocorre após a apreensão e terem sido detetados dados de cariz pessoal ou íntimo).

Para além disso, o modo habitual de apreensão dos dados informáticos existentes num sistema informático no decurso dessa diligência é realizando um "clone" do suporte que contém esses dados, sendo que a ferramenta forense utilizada não irá distinguir entre mensagens de correio eletrónico e outros dados informáticos e só quando o perito procede à análise dos dados

apreendidos é que deparará com as mensagens de correio eletrónico[53], pelo que só nesse momento as autoridades serão confrontadas com a necessidade da autorização judicial (situação em tudo similar à prevista no n.º 3 do artigo 16.º da Lei n.º 109/2009, de 15 de setembro).

Por isso, consideramos que a autorização do Juiz só poderá ser concedida *a posteriori* face à chegada das mensagens ao conhecimento de quem conduz a investigação[54].

Do mesmo modo, no caso da apreensão de correspondência, nos termos do n.º 3 do artigo 179.º do Código de Processo Penal, se a correspondência não for relevante para a prova, deverá ser restituída, pelo que a carta, encomenda, etc. entregues ao seu legítimo destinatário. Diversamente, no caso da apreensão de correio eletrónico e registos de comunicação de natureza semelhante, fruto das evidentes diferenças face à correspondência "tradicional", não será possível dar cumprimento à parte final do disposto no aludido n.º 3 do artigo 179.º do Código de Processo Penal quanto à restituição[55], embora o juiz fique vinculado a guardar segredo relativamente àquilo de que tiver tomado conhecimento e não tiver interesse para a prova.

Para além disso, na apreensão de correspondência, nos termos do n.º 3 do artigo 179.º do Código de Processo Penal, juiz terá de ser a primeira pessoa a tomar conhecimento do conteúdo da correspondência; diversamente, no caso da apreensão de correio eletrónico e registos de comunicação de natureza semelhante o juiz não terá de ser (nem poderia ser) a primeira pessoa a tomar conhecimento das mensagens de correio eletrónico ou realidades análogas (embora seja quem decide da junção, ou não, das mensagens ao autos)[56]. Na verdade, sem prejuízo de os investigadores deverem ter especiais cuidados para não tomarem conhecimento do conteúdo das comunicações sem que o Juiz o faça em primeiro lugar, pode muito bem suceder que uma mensagem de correio eletrónico tenha sido guardada como um documento de outra natureza (*v.g.* como documento de *MSWord*) e não como um ficheiro de correio eletrónico e só quando o perito que procede ao exame abre o ficheiro é que se apercebe de que se trata de um *e-mail*, sendo que, num tal caso, não faz sentido considerar a prova nula.

53 Cfr. ARMANDO RAMOS, A prova digital em processo penal: O correio eletrónico, p. 94.
54 Cfr. PEDRO VERDELHO, "A nova Lei do Cibercrime", *in* Scientia Ivridica, Tomo LVIII, p. 743, e DUARTE RODRIGUES NUNES, Os meios de obtenção de prova previstos na Lei do Cibercrime, p. 153.
55 No mesmo sentido, RITA CASTANHEIRA NEVES, As Ingerências nas Comunicações Electrónicas em Processo Penal, p. 275.
56 No mesmo sentido, PEDRO VERDELHO, "A nova Lei do Cibercrime", *in* ScIvr, T. LVIII, pp. 744-745.

E também não podemos deixar de ter em conta que, no caso da interceção de correio eletrónico e comunicações similares em tempo real, em que existe inclusivamente uma intervenção nas comunicações (sendo, por isso, muito mais gravoso do que no caso da apreensão desses dados após terem sido recebidos pelo destinatário), nos termos dos n.ºs 1 a 5 do artigo 188.º do Código de Processo Penal, aplicável *ex vi* do n.º 4 do artigo 18.º da Lei n.º 109/2009, de 15 de setembro, quem primeiro toma conhecimento do teor dessas comunicações é o órgão de polícia criminal, seguidamente o magistrado do Ministério Público e só depois é que o Juiz toma conhecimento. Ademais, no caso da apreensão de dados informáticos que incida sobre dados íntimos/privados ou pessoais (que terão um conteúdo mais sensível do que muitas mensagens de correio eletrónico), o Juiz apenas toma conhecimento do conteúdo depois de os órgãos de polícia criminal o terem feito. E, se assim é num caso em que existe uma restrição de direitos fundamentais muito mais intensa e a exigência de ser o Juiz a tomar primeiro conhecimento do teor da correspondência ("tradicional") radica na necessidade de uma mais intensa tutela de direitos fundamentais, não nos repugnaria que o artigo 17.º Lei n.º 109/2009, de 15 de setembro, pudesse ser alvo de uma interpretação hábil, no sentido de a exigência de ser o Juiz o primeiro a tomar conhecimento do teor da correspondência "tradicional", nos termos do n.º 3 do artigo 179.º do Código de Processo Penal, não ser aplicável à apreensão de mensagens de correio eletrónico ou de registos de comunicações de natureza semelhante, com evidentes ganhos em termos operacionais e sem maior detrimento para a tutela de direitos fundamentais.

No que tange às medidas cautelares e de polícia, como vimos, por força da remissão do artigo 17.º da Lei n.º 109/2009, de 15 de setembro, para o regime da apreensão de correspondência do Código de Processo Penal, será possível aplicar o artigo 252.º deste Código em sede de apreensão de correio eletrónico e registos de comunicação de natureza semelhante[57]. Contudo, pela especificidade do correio eletrónico face ao correio tradicional, não nos parece que a medida cautelar e de polícia prevista no n.º 2 do artigo 252.º do Código de Processo Penal possa ser aplicada à apreensão de correio eletrónico e registos de comunicação de natureza semelhante[58]. Com efeito, tal medida não está prevista para qualquer

57 Cfr. PINTO DE ALBUQUERQUE, Comentário ao Código de Processo Penal, 4.ª Ed., p. 510, DÁ MESQUITA, Processo Penal, Prova e Sistema Judiciário, p. 118, SANTOS CABRAL, "Art. 179º", *in* Código de Processo Penal, p. 765, e Acórdãos da Relação de Lisboa de 11/01/2011 e 06/02/2018, *in www.dgsi.pt*; contra, ARMANDO RAMOS, "Do *periculum in mora* da atuação da Autoridade Judiciária ao *fumus boni iuris* da intervenção policial", *in* IV Congresso de Processo Penal, pp. 56-57.
58 Contra, Acórdão da Relação de Lisboa de 06/02/2018, *in www.dgsi.pt*.

forma de correspondência, mas apenas para encomendas e valores fechados, sendo que, no âmbito correio eletrónico e dos registos de comunicação semelhantes, inexiste qualquer modalidade que possa ser equiparada a tais realidades, mas tão-só a cartas, telegramas ou realidades análogas. Deste modo, pela restrição às encomendas e valores fechados, a medida cautelar e de polícia prevista no n.º 2 do artigo 252.º do Código de Processo Penal não poderá ser aplicada à apreensão de correio eletrónico e registos de comunicação de natureza semelhante.

Mas já será possível aplicar a medida cautelar e de polícia prevista no n.º 3 do artigo 252.º do Código de Processo Penal, contanto que tal seja tecnicamente viável, ordenando o órgão de polícia criminal ao fornecedor de serviço a não remessa do correio eletrónico, das SMS, etc., para o destinatário, devendo a ordem ser convalidada pelo Juiz de Instrução Criminal, mediante despacho fundamentado, no prazo de 48 horas e, caso tal não suceda, a ordem de suspensão fica sem efeito e o correio eletrónico ou realidade análoga são remetidos ao destinatário.

Deste modo, consideramos que o regime da apreensão da correspondência previsto no Código de Processo Penal deverá ser aplicado *cum grano salis* e *mutatis mutandis* à apreensão de correio eletrónico e registos de comunicação de natureza semelhante, existindo aspetos do regime da apreensão da correspondência que não são aplicáveis à apreensão de correio eletrónico e registos de comunicação de natureza semelhante ou, sendo-o, não o são nos mesmos termos em que são aplicáveis à apreensão de correspondência "tradicional".

8. CONCLUSÕES

i. O Tribunal da Relação de Lisboa, no seu Acórdão de 6 de fevereiro de 2018 (Processo 1950/17.0 T9LSB-A.L1-5), considerou que o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, remete expressamente para o regime da apreensão de correspondência previsto no Código de Processo Penal, sem redução do seu âmbito, impondo-se, por isso, a aplicação de tal regime na sua totalidade;

ii. As vantagens proporcionadas pelas novas tecnologias tanto podem ser aproveitadas para fins lícitos como para fins ilícitos;

iii. Os criminosos utilizam as novas tecnologias da informação e comunicação para preparar ou executar crimes, bem como para suprimir as provas do seu cometimento, usufruindo da rapidez, anonimato e volatilidade das novas formas de comunicação à distância, que dificultam de sobremaneira a sua deteção e, quando sejam utilizadas medidas antiforenses, a sua interceção e gravação;

iv. O correio eletrónico é «*qualquer mensagem textual, vocal, sonora ou gráfica enviada através de uma rede pública de comunicações que possa ser armazenada na rede ou no equipamento terminal do destinatário até que este a recolha*».

v. O artigo 17.º da Lei n.º 109/2009, de 15 de setembro, equipara o correio eletrónico e as comunicações de natureza semelhante (SMS e MMS, conversações no *Messenger*, mensagens de voz relativas a comunicações ou arquivos de som e/ou imagem via *Whatsapp*, *Viber*, *Skype*, *Facebook*, etc.) ao correio tradicional;

vi. Pelas enormes diferenças existentes entre o correio eletrónico e o correio tradicional, bem como pelas disfunções que gera em termos de regime jurídico e pelas dificuldades operacionais que a aplicação do regime da apreensão de correspondência suscita, não se justifica equiparar o correio eletrónico ao correio tradicional;

vii. O artigo 17.º da Lei n.º 109/2009, de 15 de setembro, deveria ser revogado, passando a aplicar-se à apreensão de correio eletrónico e comunicações de natureza semelhante o regime artigo 16.º dessa Lei (constituindo o seu n.º 3 salvaguarda suficiente para a proteção da intimidade/privacidade);

viii. *De jure condito*, a fim de minimizar os efeitos nefastos da opção legislativa, o artigo 17.º da Lei n.º 109/2009, de 15 de setembro, deverá ser interpretado de

forma hábil, apenas sendo aplicável nos casos em que o *e-mail*, SMS, MMS, etc., ainda não tenham sido abertos pelo destinatário;

ix. A medida cautelar e de polícia prevista no n.º 3 do artigo 252.º do Código de Processo Penal é aplicável à apreensão de correio eletrónico e registos de comunicação de natureza semelhante, mas o mesmo não acontece com a medida prevista no n.º 2 desse preceito;

x. O regime da apreensão da correspondência previsto no Código de Processo Penal deverá ser aplicado *cum grano salis* e *mutatis mutandis* à apreensão de correio eletrónico e registos de comunicação de natureza semelhante, existindo aspetos do regime da apreensão da correspondência que não são aplicáveis à apreensão de correio eletrónico e registos de comunicação de natureza semelhante ou, sendo-o, não o são nos mesmos termos em que são aplicáveis à apreensão de correspondência "tradicional".

BIBLIOGRAFIA

Abadinsky, Howard – Organized Crime, 9.ª Edição, Wadsworth Cengage Learning, Belmont, 2007.

Albanese, Jay S. – Organized Crime in Our Times, 5.ª Edição, Matthew Bender & Company, Newark, 2007.

Albuquerque, Paulo Pinto de – Comentário ao Código de Processo Penal à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem, Universidade Católica Editora, 4.ª Edição, Lisboa, 2011.

Andrade, Manuel da Costa – "Bruscamente no Verão Passado", a reforma do Código de Processo Penal, Observações críticas sobre uma Lei que podia e devia ter sido diferente, Coimbra Editora, Coimbra, 2009.

Andrade, Manuel da Costa – "Art. 194º", *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo I, 2.ª Edição, pp. 1080 e ss., Coimbra Editora, Coimbra, 2012.

Bär, Wolfgang – TK-Überwachung, §§100a-101 StPO mit Nebengesetzen Kommentar, Carl Heymanns Verlag, Colónia e Munique, 2010.

Bravo, Rogério – "Da não equiparação do correio-electrónico ao conceito tradicional de correspondência por carta", *in* Polícia e Justiça, n.º 7, pp. 207 e ss., Coimbra Editora, Coimbra, 2006.

Cabral, José António Santos – "Art. 179º", *in* Código de Processo Penal Comentado, pp. 762 e ss., Almedina, Coimbra, 2014.

Cabral, José António Santos – "Art. 189º", *in* Código de Processo Penal Comentado, pp. 833 e ss., Almedina, Coimbra, 2014.

Canotilho, José Joaquim Gomes /Moreira, Vital – Constituição da República Portuguesa Anotada, Volume I, 4.ª Edição, Coimbra Editora, Coimbra, 2007.

Conselho da Europa – Relatório Explicativo da Convenção sobre o Cibercrime, *in https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf* (pesquisa em 06/06/2018).

Correia, João Conde – "Qual o significado de abusiva intromissão na vida privada, no domicílio, na correspondência e nas telecomunicações (art. 32.º, n.º 8, 2.ª parte, da CRP)?", *in* Revista do Ministério Público, n.º 79, pp. 45 e ss., Lisboa, 1999.

Correia, João Conde – "Prova digital: as leis que temos e a lei que devíamos ter", *in* Revista do Ministério Público, n.º 139, pp. 29 e ss., Lisboa, 2014.

Dorsch, Claudia – Die Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO, Duncker&Humblot, Berlim, 2005.

Durner, Wolfgang – "Art. 10", *in* Maunz-Dürig Grundgesetz Kommentar, Volume II (Art. 6-15), Fascículo 57 (Janeiro de 2010), pp. 1 e ss., Verlag C.H.Beck, Munique, 2010.

Eisenberg, Ulrich – Beweisrecht der StPO, 5.ª Edição, Spezialkommentar, C.H.Beck Verlag, Munique, 2006.

Frigols I Brines, Eliseu – "La protección constitucional de los datos de las comunicaciones: delimitación de los ámbitos de protección del secreto de las comunicaciones y del derecho a la intimidad a la luz del uso de las nuevas tecnologías", *in* La Protección Jurídica de la Intimidad, pp. 37 e ss., Iustel, Madrid, 2010.

Glenny, Misha – Darkmarket, Como os Hackers se tornaram a nova Máfia, Civilização, Lisboa, 2012.

González-Cuéllar Serrano, Nicolás – "Garantías constitucionales de la persecución penal en el entorno digital", *in* Prueba y Proceso Penal, Análisis especial de la prueba prohibida en el sistema español y en el derecho comparado, pp. 149 e ss., Tirant lo blanch, Valência, 2008.

Gutiérrez Francés, Mariluz – "Las altas tecnologías de la información al servicio del blanqueo de capitales transnacional", *in* Blanqueo de Dinero y Corrupción en el Sistema Bancario, Delitos Financieros, Fraude y Corrupción en Europa, Vol. II, pp. 193 e ss., Ediciones Universidad de Salamanca, Salamanca, 2002.

Jarass, Hans D./Pieroth, Bodo – Grundgesetz für die Bundesrepublik Deutschland Kommentar, 11.ª Edição, Verlag C.H. Beck, Munique, 2011.

Leite, André Lamas – "Entre Péricles e Sísifo: O Novo Regime Legal das Escutas Telefónicas", *in* Revista Portuguesa de Ciência Criminal, Ano 17, Fascículo 4.º, pp. 613 e ss., Coimbra Editora, Coimbra, 2007.

Lopes, José Mouraz – Garantia Judiciária no Processo Penal, Do Juiz e da Instrução, Coimbra Editora, Coimbra, 2000.

Magistrados do Ministério Público do Distrito Judicial do Porto – Código de Processo Penal, Comentários e Notas Práticas, Coimbra Editora, Coimbra, 2009.

Mesquita, Paulo Dá – Processo Penal, Prova e Sistema Judiciário, Coimbra Editora, Coimbra, 2010.

Meyer-Gossner, Lutz – Strafprozessordnung mit GVG und Nebengesetzen, 56.ª Edição, Verlag C.H.Beck, Munique, 2013.

Neves, Rita Castanheira – As Ingerências nas Comunicações Electrónicas em Processo Penal, Natureza e respectivo regime jurídico do correio electrónico enquanto meio de obtenção de prova, Coimbra Editora, Coimbra, 2011.

Nunes, Duarte Rodrigues – Os meios de obtenção de prova previstos na Lei do Cibercrime, Gestlegal, Coimbra, 2018.

Ramalho, David Silva – Métodos Ocultos de Investigação Criminal em Ambiente Digital, Almedina, Coimbra, 2017.

Ramos, Armando Dias – A prova digital em processo penal: O correio eletrónico, Chiado Editora, Lisboa, 2014.

Ramos, Armando Dias – "Do *periculum in mora* da atuação da Autoridade Judiciária ao *fumus boni iuris* da intervenção policial", *in* IV Congresso de Processo Penal, pp. 49 e ss., Almedina, Coimbra, 2016.

Rodrigues, Benjamim Silva – Das Escutas Telefónicas À Obtenção da Prova [em Ambiente Digital], Tomo II, Coimbra, 2008.

Rodrigues, Benjamim Silva – Da Prova Penal, Tomo II, Bruscamente…A(s) Face(s) Oculta(s) dos Métodos Ocultos de Investigação Criminal, 1.ª Edição, Rei dos Livros, Lisboa, 2010.

Roxin, Claus/Schünemann, Bernd – Strafverfahrensrecht, 27.ª Edição, C.H.Beck, Munique, 2012.

Schäfer, Gerhard – "§99", *in* Löwe-Rosenberg Die Strafprozessordnung und das Gerichtsverfassungsgesetz, 2.º Volume, 25.ª Edição, pp. 303 e ss., De Gruyter, Berlim, 2004.

Schroeder, Friedrich-Christian – Strafprozessrecht, 4.ª Edição, CH Beck, Munique, 2007.

Silva, Germano Marques da /Sá, Fernando – "Art. 34.º", *in* Constituição Portuguesa Anotada, Tomo I, 2.ª Edição, pp. 755 e ss., Coimbra Editora, Coimbra, 2010.

Simas Santos, Manuel/Leal-Henriques, Manuel – Código de Processo Penal Anotado, Volume I, 3.ª Edição, Editora Rei dos Livros, Lisboa, 2008.

Teixeira, Carlos Adérito – "Escutas Telefónicas: A Mudança de Paradigma e os Velhos e os Novos Problemas", *in* Revista do Centro de Estudos Judiciários, Número 9 (Especial), Jornadas sobre a revisão do Código de Processo Penal", pp. 243 e ss., Centro de Estudos Judiciários, Lisboa, 2008.

Venâncio, Pedro Dias – Breve introdução da questão da investigação e meios de prova na criminalidade informática, *in* *www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf* (pesquisa em 14/06/2018).

Venâncio, Pedro Dias – Lei do Cibercrime, Anotada e Comentada, Coimbra Editora, Coimbra, 2011.

Verdelho, Pedro – "Apreensão de correio electrónico em Processo Penal", *in* Revista do Ministério Público, n.º 100, pp. 153 e ss., Lisboa, 2004.

Verdelho, Pedro – "A Reforma Penal Portuguesa e o Cibercrime", *in* Revista do Ministério Público, n.º 108, pp. 97 e ss., Lisboa, 2006.

Verdelho, Pedro – "Técnica do novo CPP: Exames, Perícias e Prova Digital", *in* Revista do Centro de Estudos Judiciários, Número 9 (Especial), Jornadas sobre a revisão do Código de Processo Penal", pp. 145 e ss., Centro de Estudos Judiciários, Lisboa, 2008.

Verdelho, Pedro – "A nova Lei do Cibercrime", *in* Scientia Ivridica, T. LVIII (2009), pp. 717 e ss., Universidade do Minho, Braga, 2009.

JURISPRUDÊNCIA

Tribunal Europeu dos Direitos do Homem

Acórdão Wieser e Bicos Beteiligungen GmbH c. Áustria (de 16 de outubro de 2007), *in www.echr.coe.int*.

PORTUGAL

Tribunal Constitucional

Acórdão n.º 403/2015, *in www.tribunalconstitucional.pt*.

Supremo Tribunal de Justiça

Acórdão de 18 de maio de 2006 (Processo 06P1394), *in www.dgsi.pt.*

Acórdão de 3 de março de 2010 (Processo 886/07.8PSLSB.L1.S1), *in www.dgsi.pt.*

Tribunal da Relação de Coimbra

Acórdão de 2 de março de 2005 (Processo 3756/04), *in www.dgsi.pt.*

Acórdão de 29 de março de 2006 (Processo 607/06), *in www.dgsi.pt.*

Tribunal da Relação de Évora

Acórdão de 6 de janeiro de 2015 (Processo 6793/11.6TDLSB-A.E1), *in www.dgsi.pt.*

Acórdão de 20 de janeiro de 2015 (Processo 648/14.6GCFAR-A.E1), *in www.dgsi.pt.*

Tribunal da Relação de Guimarães

Acórdão de 29 de março de 2011 (Processo 738/10.0GAPTL-A.G1), *in www.dgsi.pt.*

Acórdão de 15 de outubro de 2012 (Processo 68/10.1GCBRG.G1), *in www.dgsi.pt.*

Tribunal da Relação de Lisboa

Acórdão de 13 de outubro de 2004 (Processo 5150/2005-3), *in www.dgsi.pt.*

Acórdão de 15 de julho de 2008 (Processo 3453/2008-5), *in www.dgsi.pt.*

Acórdão de 11 de janeiro de 2011 (Processo 5412/09.3TDLSB-A.L1-5), *in www.dgsi.pt.*

Acórdão de 2 de março de 2011 (Processo 463/07.3TAALM-A.L1-3), *in www.dgsi.pt.*

Acórdão de 20 de dezembro de 2011 (Processo 36/11.6PJOER-A.L1-5), *in www.dgsi.pt.*

Acórdão de 29 de março de 2012 (Processo 744/09-1S5LSB-A.L1-9), *in www.dgsi.pt.*

Acórdão de 24 de setembro de 2013 (Processo 145/10.9GEALM.L2-5), *in www.dgsi.pt.*

Acórdão de 6 de fevereiro de 2018 (Processo 1950/17.0T9LSB-A.L1-5), *in www.dgsi.pt.*

Tribunal da Relação do Porto

Acórdão de 7 de julho de 2010 (Processo 1978/09.4JAPRT-B.P1), *in www.dgsi.pt.*

Acórdão de 3 de abril de 2013 (Processo 856/11.1PASJM.P1), *in www.dgsi.pt.*

Acórdão de 24 de abril de 2013 (Processo 585/11.6PAOVR.P1), *in www.dgsi.pt.*

Acórdão de 22 de maio de 2013 (Processo 74/07.3PASTS.P1), *in www.dgsi.pt.*

Acórdão de 3 de dezembro de 2013 (Processo 37/12.7TBALJ-A.P1), *in www.dgsi.pt.*

Acórdão de 7 de julho de 2016 (Processo 2039/16.0JAPRT.P1), *in www.dgsi.pt.*

Acórdão de 7 de dezembro de 2016 (Processo 1689/16.4JAPRT-A.P1), *in www.dgsi.pt.*

ALEMANHA

Bundesgerichtshof

Jurisprudência Uniformizada

Sentença do Grosse Senat für Strafsachen de 13 de maio de 1996, *in* Entscheidungen des Bundesgerichtshofes in Strafsachen, 42, pp. 139 e ss., Carl Heymanns Verlag KG, Colónia e Berlim, 1997.

CYBERLAW
by CIJIC

OS DRONES: RESPONSABILIDADE CIVIL, ROBÓTICA E PROPRIEDADE INTELECTUAL

ALYNE ANDRADE [1]

1 Doutoranda em Direito e Economia e Mestre em Direito Intelectual pela Faculdade de Direito da Universidade de Lisboa. Presidente do Instituto Brasileiro de Direito da Informática (IBDI). Coordenadora do Núcleo de Direito Empresarial da ESA/OAB-PE. Advogada. Contacto: alyne@alyneandrade.com.br

RESUMO

O maior aeroporto português teve seu tráfego aéreo interrompido novamente, no presente Setembro de 2018, em decorrência de um drone que sobrevoou a pista. As regras sobre a utilização dos drones no espaço aéreo português bem como questões de responsabilidade civil foram regulamentadas em Portugal. Os incidentes, porém, continuam a suceder.

O Parlamento Europeu mostra-se interessado em abordar questões sobre robótica e inteligência artificial. Destarte, abordaremos nesse sentido o crescente mercado da economia da robótica na União Europeia e respectiva proteção pelo Direito de Propriedade Intelectual.

Palavras-Chave: Drones; regulação; robôs; responsabilidade civil; Parlamento Europeu; inteligência artificial; propriedade intelectual.

ABSTRACT

The largest Portuguese airport had its air traffic interrupted in September 2018, due to a drone. Recent regulations on the use of drones in portuguese airspace and its civil liability issues were foreseen in Portugal. Nevertheless, incidents continue to occur.

The European Parliament is active in addressing issues on robotics and artificial intelligence. We will address the growing market for the robotics economy in the European Union and the protection of Intellectual Property rights.

Keywords: Drones; regulation; robots; civil liability; European Parliament; artificial intelligence; intellectual property

1. INTRODUÇÃO

No dia 20 de Setembro de 2018, um drone interrompeu por 10 minutos operações no Aeroporto de Lisboa[1].

Interromper um aeroporto de grande movimentação por 10 minutos causa alguns constrangimentos, podendo pôr em causa a segurança de pessoas, bens e outras aeronaves. Os países europeus não dispõem de uma legislação harmonizada sobre robótica e drones, mas em Portugal encontram-se vigentes estruturas regulatórias como Regulamento n.º 1093/2016, de 24 de Novembro de 2016 em vigor desde 13 de Janeiro de 2017[2] e o Decreto-Lei n.º 58/2018, de 23 de Julho.

2. REGULAMENTAÇÃO EM PORTUGAL

O Regulamento n.º 1093/2016, de 14 de Dezembro, relativo às condições de operação aplicáveis aos sistemas de aeronaves civis pilotadas remotamente (RPAS, *Remotely Piloted Aircraft Systems*, "Drones"[3]), da Autoridade Nacional da Aviação Civil, elenca um conjunto de regras e obrigações para todos os que pretendem utilizar os RPAS[4], quer numa perspectiva

1 Disponível em: <https://24.sapo.pt/atualidade/artigos/drone-interrompeu-por-10-minutos-operacao-no-aeroporto-de-lisboa-na-quarta-feira>.

2 Regulamento n.º 1093/2016, de 24 de Novembro de 2016, publicado no Diário da República, 2.ª Série, n.º 238, de 14 de Dezembro, que entrará em vigor a 13 de Janeiro de 2017. Além do Regulamento, a ANAC publicou o chamado "Código Drone". A ANAC também publicou o Guia de Utilização do Espaço Aéreo que é apenas uma ferramenta de auxílio aos operadores de drones para identificarem visualmente as áreas referidas (no que se refere ao espaço aéreo, áreas de proteção operacional, áreas de proteção de aeródromos e heliportos, dentro e fora do espaço aéreo controlado), os seus limites verticais e de algum modo dar a conhecer os vários tipos de espaço aéreo localizados em Portugal. Disponível em: <https://www.voanaboa.pt/regulamento>; <https://www.voanaboa.pt/codigo-drone> e <https://www.voanaboa.pt/Files/downloads/Guia-Utilizacao-Espaco-Aereo.pdf>.

3 Vejamos os seguintes artigos do Regulamento: art. 2.º, h: "«Aeronave pilotada remotamente (RPA, *Remotely Piloted Aircraft*), aeronave não tripulada que é pilotada a partir de uma estação de piloto remoto" e art. 2º, cc "*cc*) «Sistema de aeronave pilotada remotamente (RPAS, *Remotely Piloted Aircraft System*)», sistema que compreende a aeronave pilotada remotamente, a estação de piloto remoto associada, os canais de comunicação para comando e controlo requeridos e quaisquer outros componentes, conforme especificado no projeto do sistema;".

4 O artigo 11.º estipula as restrições à operação ou voo de RPAS

"1 - Uma RPA não pode voar:

a) Nas áreas definidas no Anexo ao presente Regulamento como sendo proibidas;

b) Sobre concentrações de pessoas ao ar livre, entendendo -se como tal mais do que 12 pessoas, salvo se expressamente autorizado pela ANAC;

lúdica ou desportiva, quer numa perspectiva profissional, ao garantir segurança operacional do espaço aéreo português[5].

Os "drones" são considerados como aeronaves civis não tripuladas e não é necessária qualquer licença individual para operá-los. Entretanto, há situações que carecem de autorização por parte da Autoridade Nacional da Aviação Civil (ANAC) e estão identificadas no Regulamento acima mencionado. E antes de pôr o drone a voar, é fundamental o usuário informar-se de todas as situações em que necessita de autorização da Autoridade Nacional da Aviação Civil, consultando o Código Drone e o Regulamento de Drones no Espaço Aéreo.

As regras do Regulamento tornam mais segura a utilização do espaço aéreo, de modo a não conflituar com a aviação tripulada. Com este Regulamento estabelece-se a regra geral que confere liberdade para os utilizadores de drones efetuarem voos diurnos, à linha de vista, até uma altura de 120 metros (400 pés) e desde que as aeronaves não se encontrem a sobrevoar pessoas ou áreas sujeitas a restrições ou na proximidade de infraestruturas aeroportuárias[6]. Ou seja, não devem estar na proximidade de aeródromos e heliportos, e se não estiverem em áreas proibidas, restritas ou reservadas[7].

Há uma exceção para as aeronaves brinquedo[8] em que é estipulada a proibição de sobrevoar concentrações de pessoas e de exceder os 30 metros acima da superfície, bem

c) Em zonas de sinistro onde se encontrem a decorrer operações de proteção e socorro, salvo se o comandante das operações de socorro autorizar expressamente o voo, devendo em tais casos:
i) Ser assegurado o cumprimento das regras do presente Regulamento, nomeadamente as respeitantes às alturas máximas de voo permitidas; e
ii) Ser assegurado que, simultaneamente, não se encontra a sobrevoar a zona de sinistro nenhuma aeronave tripulada".

5 Quem pretende comprar um drone, em lojas como a Worten, por exemplo, há as regras previstas para a utilização do drone. Disponível em: <https://www.worten.pt/regulamento-anac-drones>.

6 O artigo 3.º, do Regulamento prevê as regras gerais de operação:
"1 - As RPA apenas podem efetuar voos diurnos, em operações VLOS, até 120 metros acima da superfície (400 pés), à exceção das aeronaves brinquedo, que não devem exceder 30 metros de altura (100 pés);
2 - A operação de RPAS deve ser executada de forma a minimizar riscos para as pessoas, bens e outras aeronaves;
3 - As RPA devem manter uma distância segura de pessoas e bens patrimoniais, de forma a evitar danos em caso de acidente ou incidente;
4- O piloto remoto deve dar prioridade de passagem às aeronaves tripuladas e afastar -se das mesmas sempre que, por qualquer razão, as aeronaves tripuladas estejam excecionalmente a voar a uma altura próxima da RPA."

7 Há um mapa interativo que contém as várias limitações aplicáveis aos voos de aeronaves pilotadas remotamente, consoante o local onde se pretenda voar. Nomeadamente com os aeroportos e respectivas áreas de proteção operacional, com todos os aeródromos certificados nacionais, com as áreas proibidas e com as áreas restritas ou temporariamente reservadas de natureza militar. O mapa contempla também os heliportos hospitalares, utilizados em missões de proteção civil ou sob gestão, comando ou responsabilidade de entidades públicas com funções de manutenção da ordem pública, segurança, fiscalização e investigação criminal. Disponível em: <https://www.voanaboa.pt/codigo-drone>.

8 Artigo 2.º, *e*, do Regulamento da ANAC define a «Aeronave brinquedo» como "uma aeronave pilotada remotamente, não equipada com motor de combustão e com peso máximo operacional inferior a 0,250 kg, concebida ou destinada, exclusivamente ou não, a ser utilizada para fins lúdicos por crianças de idade inferior a 14 anos".

como a obrigatoriedade de guardar uma distância mínima, medida na horizontal, em relação a pessoas e bens, de 30 metros.

O disposto no Regulamento da ANAC não dispensa o cumprimento dos outros regimes jurídicos eventualmente aplicáveis no que respeita à utilização de aeronaves pilotadas remotamente. A título de exemplo, se pretender utilizar uma aeronave pilotada remotamente para efetuar recolha e divulgação de imagens e fotografias aéreas, deverá contatar previamente a Autoridade Aeronáutica Nacional/Força Aérea para obtenção de autorização[9]. Destaca-se também a necessidade de respeitar o Regulamento Geral de Proteção de Dados[10] e de respeitar a privacidade e a vida privada dos demais cidadãos[11].

Sugere-se igualmente que, caso pretenda voar sobre alguma reserva ou parque natural, contate-se previamente a respectiva entidade responsável por tais parques, para aferir de tal possibilidade (poderá ser obtida informação ou poderá ser contatado o Instituto da Conservação da Natureza e das Florestas[12], uma vez que cada parque ou reserva natural tem legislação própria)[13].

Os drones estão mais sofisticados e autônomos, são dotados de *sofwtares* poderosos que lhe possibilitam explorar uma liberdade de plano de voo. Esta liberdade despertou a imposição de limites à liberdade com controle de operação dos drones pelas condutas de seus usuários[14].

---

9 Disponível em: <https://www.aan.pt>.

10 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.
Observar o Considerando 20, das recomendações à Comissão sobre disposições de Direito Civil sobre Robótica, do Relatório de 27 de Janeiro de 2017, do Parlamento Europeu que dispõe: "Salienta que o direito à proteção da vida privada e o direito à proteção dos dados pessoais – consagrados nos artigos 7.º e 8.º da Carta, bem como no artigo 16.º do Tratado sobre o Funcionamento da União Europeia (TFUE) – aplicam-se a todas as áreas da robótica e que o quadro jurídico da União em matéria de proteção de dados deve ser plenamente respeitado; solicita, a este respeito, a revisão das normas e dos critérios relativos à utilização de câmaras e sensores em robôs; insta a Comissão a garantir o respeito dos princípios da proteção dos dados, tais como os princípios da privacidade desde a concepção e por defeito, os princípios da minimização dos dados e da limitação da finalidade, bem como dos mecanismos de controlo da transparência para os titulares de dados e de soluções adequadas em conformidade com a legislação da União em matéria de proteção de dados, e ainda a promoção e a integração de recomendações e normas adequadas nas políticas da União".

11 O artigo 13.º do Regulamento prevê a violação de determinações, instruções ou ordens da ANAC:
"A violação de determinações, instruções ou ordens da ANAC constantes do presente Regulamento, bem como todas aquelas que sejam inerentes ao cumprimento do mesmo, constitui contraordenação aeronáutica civil grave ou muito grave, nos termos do artigo 7.º do Decreto –Lei n.º 10/2004, de 9 de Janeiro".

12 Disponível em: < https://www.icnf.pt>.

13 Disponível em: <https://www.drone-vision.com/legislacao>.

14 *"Law is the most obvious example of regulation, but behaviour is also influenced by other intentionally used mechanisms. Lessig identifies four tools in the regulatory tool-box: law; social norms; market; and architecture (i.e. technology as a regulatory tool). The law often plays a role in the other regulatory instruments as well, as a contextual or facilitating factor (for example, through creating a basis or framework for competition or backing up social norms). From the perspective of the regulator facing challenges posed by robotics, each modality of*

Em 28 de Julho de 2018, entrou em vigor o Decreto-Lei n.º 58/2018, de 23 de Julho, que torna obrigatório o registro destes aparelhos com mais de 250 gramas, a contratualização de um seguro de responsabilidade civil para "drones" acima dos 900 gramas e estipula "um quadro sancionatório aplicável a quem violar estas obrigações, de forma a dissuadir e censurar adequada e proporcionalmente condutas de risco que podem colocar em causa a segurança de todos"[15].

O comportamento do drone é condicionado à conduta humana. O usuário do drone deve agir com precaução e procurar saber quais são as regras de utilização através do site do revendedor do drone, do produtor do drone e da ANAC. A responsabilidade civil poderá recair sobre o usuário ou proprietário do drone. Se houver falha do produto, haverá responsabilidade do produtor a se averiguar[16].

Em paralelo aos drones que podem interromper a operação de aeroportos[17], o aeroporto de Changi, em Singapura, eleito o melhor do mundo nos últimos seis anos pela Skytrax, está buscando o objetivo de automação extensiva do aeroporto que construiu um terminal inteiro para ajudar a testar os robôs do aeroporto do futuro[18].

---

regulation is relevant to consider – including the contextual role of the law if policy measures use other regulatory modalities than primarily legal interventions – but no regulatory modality is ideally fit to deal with the regulatory challenges of robotics". LEENES, Ronald; et.al. *Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues*. In: Law, Innovation and Technology, v. 9, nº 9, Ano 2017, 1-44.

15 Os artigos 3º e 4º deste Decreto-Lei tratam do registro obrigatório e do procedimento de registro da «Aeronave não tripulada (UA, *Unmanned Aircraft*). Os artigos 9º e 10º dispõem sobre a responsabilidade civil e do seguro de responsabilidade civil. O artigo 12º estabelece os regimes contraordenacionais aplicáveis consoante a conduta em causa em contraordenações muito graves, contraordenações graves e contraordenação leve.

16 Observar as regras dos artigos 483.º, 493.º/2, 499, 563, do Código Civil Português e do Decreto-Lei nº 383/89, de 06 de Novembro (Responsabilidade Decorrente de Produtos Defeituosos).

17 Sobre o uso dos drones nos Estados Unidos da América (EUA), o autor Edmund F. Byrne faz as seguintes considerações: "*From its onset at the beginning of this century, the drone industry was largely funded by and for the military. Its budget for drones is still over $500 million annually; but now both military and commercial uses are generating new companies and new products. Many of these are intended for military use (Benjamin 2013, pp. 31–54). Some remain unpurchased (Pasztor 2015). Yet, according to one oftencited forecast (conducted by aerospace research company Teal Group Corp., in 2013), sales of civilian and military drones around the world may grow from the current $5.2 billion a year to $89 billion by 2023. In this climate, the possibility of running an ethical drone business becomes more feasible (Loewenstein 2014). However, there remain many concerns about the envisioned uses of drones. These have to do especially with domestic safety and privacy, because drones do interfere with manned flights and with activities of individuals on the ground*". BYRNE, Edmund F. *Making Drones to Kill Civilians: Is it Ethical?*. In: Journal of Business Ethics, v. 147, 2018, 81-93. Disponível em: <https://link.springer.com/article/10.1007/s10551-015-2950-4>.

Ver também o artigo dos Michael Froomkin e P. Zak Colangelo sobre a legislação de drones nos EUA. FROOMKIN, Michael; COLANGELO, P. Zak. *Self-Defense Against Robots and Drones*. In: Connecticut Law Review, v. 48, n. 1, nov./2015. Disponível em: <http://robots.law.miami.edu/2014/wp-content/uploads/2013/06/Froomkin-Colangelo-Self-Defence-Against-Robots-March-2014.pdf >.

18 Disponível em: <https://www.bloomberg.com/news/features/2018-09-16/singapore-s-changi-airport-is-partly-run-by-robots>.

3. INICIATIVAS DO PARLAMENTO EUROPEU

O Relatório das Nações Unidas de 2005 propõe uma definição geral de robô como "*a reprogrammable machine operating in a semi- or fully autonomous way, so as to perform manufacturing operations (e.g., industrial robots), or provide "services useful to the well-being of humans" (e.g., service robots)*"[19].

Entre os anos de 2010 e 2014, o aumento médio nas vendas de robôs foi 17% ao ano e nas vendas de 2014 registrou uma subida de 29%, o maior aumento anual de sempre, com os fornecedores de componentes automóveis e a indústria da eletrônica/elétrica a serem os principais motores do crescimento. Os processos de registro de patentes em tecnologia robótica triplicaram na última década.

A Europa tem uma posição forte na robótica, com 32% dos mercados mundiais atuais. A robótica industrial tem cerca de um terço do mercado mundial, enquanto no mercado de robôs de serviço profissional, os fabricantes europeus produzem 63% dos robôs não militares. A posição europeia no mercado dos robôs domésticos e de serviço representa uma quota de mercado de 14% e, devido à sua dimensão atual, esta é também uma área muito menor da atividade econômica na Europa do que as outras duas áreas[20].

Em 31/05/2016, o Comitê de Assuntos Jurídicos do Parlamento Europeu publicou o Projeto do Relatório com recomendações à Comissão sobre as Regras de Direito Civil em Robótica (2015/2103 (INL))[21].

---

19 "UN World 2005 Robotics Report". É importante destacar a existência da Federação Internacional de Robôtica: "*The International Federation of Robotics connects the world of robotics around the globe. Our members come from the robotics industry, national or international industry associations and research & development institutes. Our federation represents over 50 members from more than 20 countries. The IFR statistical department is the primary global resource for data on robotics. The IFR was established as a non-profit organization in 1987*". Disponível em: <https://ifr.org/association>.

20 *Robotics in Europe - Why is Robotics important? (...) In terms of scientific standing in robotics, Europe also has a strong world position. European diversity in science supports multi-disciplinary domains such as robotics, which in turn relies on a variety of fundamental domains and is thus to a large extent the science of integrating a broad spectrum of technologies. Europe is particularly strong in technologies such as cooperating robots and ambient intelligence; speech and haptics-based human-machine interface; safety; actuation (without gears); grippers and dextrous hands; locomotion (without bipedal locomotion); materials science and engineering; navigation and collision avoidance; motion and task planning; control of arms and vehicles; learning; modelling for control (kinematics and dynamics), biomimetics, bionics, and cybernetics.In terms of social sciences, the use of robotics in society raises many ethical and societal issues as well as legal ones. Europe has managed to lead the worldwide debate in this area and it is important that ethical, legal, and social ("ELS") investigations should be at the forefront of considerations regarding the deployment and use of robotics in the wider European society. Disponível em:* <https://www.eu-robotics.net/sparc/about/robotics-in-europe/index.html>.

21 Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN>.

Em 27 de Janeiro de 2017, a Comissão dos Assuntos Jurídicos do Parlamento Europeu publicou o Relatório que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica[22]. No Relatório, os deputados do Parlamento Europeu instaram a Comissão Europeia a adotar legislação para clarificar as questões de responsabilidade jurídica, propuseram ainda um código de conduta ético voluntário sobre robótica para investigadores e criadores, para assegurar que o desempenho das suas atividades se faça no respeito das normas jurídicas e éticas e que a concepção e utilização de robôs devem respeitar a dignidade humana. O Parlamento convidou igualmente à Comissão Europeia a ponderar a criação de uma agência europeia para a robótica e a inteligência artificial[23].

Este Relatório faz recomendações aos meios de transporte autônomos, nomeadamente os Drones (RPAS), no Considerando 30, ao reconhecer os avanços positivos nas tecnologias relativas aos drones como no domínio de busca e salvamento[24]. Contudo, ressalta a relevância de um quadro da União para os drones, a fim de defender a segurança, a proteção e a privacidade dos cidadãos da União[25].

Os drones, também chamados de robôs voadores não tripulados, seguem uma rota pré-programada ou se locomovendo para um destino fixo guiado automaticamente por GPS. Em um drone autônomo, tudo que se fizer vai depender do sistema computacional embarcado, como sensores, controles e programas, que poderão ser dotados de inteligência artificial e outros recursos das áreas da ciência da computação, eletrônica, mecânica, telecomunicações etc.[26].

---

22 Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//PT#title1>.

23 CATEA, Roxana Mihaela. *Challenges of the Not-So-Far Future: Eu Robotics and AI Law in Business.* Disponível em: <http://cks.univnt.ro/uploads/cks_2018_articles/index.php?dir=2_private_law%2F&download=CKS_2018_private_law_005.pdf>.
Mais detalhes no sítio eletrônico do Parlamento Europeu. Disponível em: <http://www.europarl.europa.eu/cmsdata/130982/comissao-juri-resumo-consulta-robotica.pdf>.

24 Os drones podem ser usados em resgate de pessoas, sistemas de comunicação aérea, vigilância de fronteiras, para uso militar, combate ao terrorismo e fotos aéreas de eventos.

25 E (...) insta a Comissão a acompanhar as recomendações da resolução do Parlamento, de 29 de Outubro de 2015, sobre a utilização segura de sistemas de aeronaves telepilotadas (RPAS), vulgarmente conhecidos como veículos aéreos não tripulados (UAV), no campo da aviação civil; exorta a Comissão a disponibilizar avaliações sobre as questões de segurança relacionadas com a utilização generalizada de veículos aéreos não tripulados; insta a Comissão a estudar a necessidade de introduzir um sistema de rastreabilidade e identificação destinado aos RPAS que permita determinar a posição da aeronave em tempo real durante a sua utilização; recorda que a homogeneidade e a segurança das aeronaves não tripuladas devem ser asseguradas através das medidas previstas no Regulamento (CE) n.º 216/2008 do Parlamento Europeu e do Conselho.

26 Disponível em: <https://www.em.com.br/app/noticia/tecnologia/2014/09/23/interna_tecnologia,571765/inteligencia-artificial-dos-drones-pode-ajudar-cada-vez-mais-em-diferentes-areas.shtml>.

Sendo que em 16 de Fevereiro de 2017, o Parlamento Europeu adotou uma Resolução com recomendações à Comissão Europeia sobre regras de Direito Civil sobre Robótica[27]. O anexo desta Resolução contém a definição e classificação de "robôs inteligentes"[28]; Carta da Robótica[29]; do Código de Conduta Ética para Engenheiros de Robótica e Código para Comissões de Ética em Matéria de Investigação; Licenças para Criadores e Licenças para Utilizadores.

O aumento da utilização de robôs e de Inteligência Artificial (IA) requer uma normalização europeia, a fim de evitar discrepâncias entre os Estados-Membros e a fragmentação do mercado interno da União Europeia. Além disso, os receios dos consumidores em matéria de segurança e proteção no que respeita à utilização de robôs e de IA têm de ser abordados[30]. A Resolução sublinha especificamente que o teste de robôs em cenários da vida real é essencial para identificar e avaliar os riscos que estes podem implicar[31].

---

27 Disponível em: <http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2015/2103(INL)#documentGateway> ; <http://www.europarl.europa.eu/oeil/popups/summary.do?id=1477231&t=e&l=en> e <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2017-0051>.

28 Definição e classificação de «robôs inteligentes»:
Deve ser criada uma definição comum europeia para robôs autônomos «inteligentes», incluindo, se for caso disso, definições das respectivas subcategorias, tendo em consideração as seguintes características:
– a capacidade de adquirir autonomia através de sensores e/ou através da troca de dados com o seu ambiente (interconectividade) e a análise destes dados;
– a capacidade de aprender com a experiência e com a interação;
– a forma do suporte físico do robô;
– a capacidade de adaptar o seu comportamento e as suas ações ao ambiente.
Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN>.

29 Considerando AA "Considerando que a autonomia de um robô pode ser definida como a capacidade de tomar decisões e de as aplicar no mundo exterior, independentemente do controlo ou da influência externa; considerando que esta autonomia é de natureza puramente tecnológica e que o seu grau depende do modo como o nível de sofisticação da interação do robô com o seu ambiente foi concebido". Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém Recomendações à Comissão sobre disposições de Direito Civil sobre Robótica. Disponível em: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0//PT>.

30 A robótica não é o mesmo do que Inteligência Artificial. A robótica é um ramo da tecnologia que lida com robôs e que envolve o projeto, a construção e a programação de robôs físicos, sendo que apenas uma parte deles envolve inteligência artificial. Os robôs são máquinas programáveis que são capazes de realizar uma série de ações de forma autônoma ou semiautônoma. Em termos gerais, um robô é definido por interagir com o mundo físico através de sensores e atuadores; ser programável; ser autônomo ou semiautônomo. No entanto, não há consenso absoluto em relação à definição de robô. Para controlar o sistema de robôs, é utilizada IA, inclui sensores, atuadores e outras programações além (ou não) de IA. Concluindo, os robôs artificialmente inteligentes são a ponte entre a robótica e a IA, mas existem muitos robôs que não requerem inteligência artificial, como aqueles que realizam movimentos repetitivos e que existem, há muito, nas fábricas. Disponível em: <https://observador.pt/explicadores/inteligencia-artificial/03-robotica-e-o-mesmo-do-que-inteligencia-artificial/>.

31 O autor M. Ryan Calo menciona que há uma sinergia entre inteligência artifical e robótica: "*There is a synergy between artificial intelligence and robotics: smarter programs increase the capacity of robots to engage in surveillance. An interesting example is software that permits cooperation among robots, permitting them to monitor a location from multiple angles. Another is software that promotes stealth: researchers at Seoul National University in South Korea, for instance, are developing an algorithm that would assist a robot in hiding from,*

No dia 10 de Abril de 2018, Portugal tornou-se signatário de várias iniciativas e declarações para o desenvolvimento do Mercado Único Digital na União Europeia. O país assumiu compromissos de cooperação nas áreas de Inteligência Artificial, *blockchain*, saúde, inovação e condução automóvel suportada por 5G, no âmbito da Jornada Digital 2018. Um dos compromissos foi o reforço dos centros europeus na investigação em IA com a assinatura de Portugal da Declaração de Cooperação em Inteligência Artificial, assumindo a vontade de unir recursos para uma abordagem europeia na referida área, com objetivos de garantir o aproveitamento de oportunidades para a Europa, assim como a resolução coletiva de problemas ao centrar-se no reforço dos centros europeus de investigação em IA, na criação de sinergias em regimes de financiamento para I&D em toda a Europa e na troca de opiniões sobre o impacto da IA na sociedade e na economia. Entre os desafios, estão os laborais, sociais, econômicos, éticos, jurídicos e educacionais[32].

A Comissão Europeia anunciou no dia 25 de Abril de 2018[33] que quer estar na linha da frente da IA através de três eixos-chave: aumentar o investimento público e privado em IA; preparar as mudanças socioeconômicas e garantir um quadro ético e jurídico adequado[34]. A União Europeia deverá investir pelo menos 20 mil milhões de euros até 2020 para se adaptar à era dos robôs, que já leva grande avanço nos Estados Unidos e no Japão, por exemplo[35]. Como parte desta iniciativa, serão elaboradas orientações éticas sobre IA até ao final de 2018, com base na Carta dos Direitos Fundamentais da União Europeia, tendo em consideração princípios

and sneaking up upon, a potential intruder". CALO, Ryan M. *Peeping Hals*. In: Artificial Intelligence, Elsevier, nº 175, Ano 2011, 940-941.

32 Disponível em: <https://www.computerworld.com.pt/2018/04/10/portugal-adere-a-5-iniciativas-para-o-mercado-unico-digital/>.

33 *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe*. Brussels, 25.4.2018 COM(2018) 237 final. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe >.
Sobre o Mercado Único Digital e a Inteligência Artificial: <https://ec.europa.eu/digital-single-market/en/artificial-intelligence>.

34 A Comissão Europeia (CE) apresentou uma série de medidas para o desenvolvimento da Inteligência Artificial (IA), para que esta seja colocada ao serviço dos cidadãos europeus e para estimular a competitividade da União Europeia (UE). A iniciativa sobre a inteligência artificial vem na sequência do pedido dos dirigentes europeus para que fosse tomada a nível europeu. Disponível em: <https://www.tveuropa.pt/noticias/uniao-europeia-vai-investir-em-inteligencia-artificial/>; <https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe> e <https://ec.europa.eu/digital-single-market/en/european-ai-alliance>.

35 Questionado pelos jornalistas sobre se um robô poderia ter direitos humanos ou, um dia, vir a ser comissário europeu, Andrus Ansip, que tem a pasta do Mercado Único Digital, respondeu: "Tenho muitos desses robôs, por exemplo, um deles está a limpar o meu apartamento enquanto estou nesta sala de imprensa. Estou a falar do aspirador de pó e penso que esse aspirador não deve ter direitos como os humanos. Talvez pensem que o meu aspirador de pó faria melhor o meu trabalho de comissário, mas não acho que isso vá acontecer". Disponível em: <https://pt.euronews.com/2018/04/25/uniao-europeia-vai-investir-milhoes-em-inteligencia-artificial>.

como a proteção dos dados e a transparência, e como base o trabalho do Grupo Europeu de Ética para as Ciências e as Novas Tecnologias[36].

4. O DIREITO DE PROPRIEDADE INTELECTUAL E ROBÓTICA

A Propriedade Intelectual está no cerne da inovação e da competitividade em todo o mundo, assim como na União Europeia (UE), e os Direitos de Propriedade Intelectual são protegidos por meio de patentes, marcas registradas e Direitos de Autor e são previstos também por um quadro de Diretivas e Regulamento. Os Direitos de Propriedade Intelectual permitem que indivíduos e empresas obtenham reconhecimento e/ou benefício financeiro do que inventam ou criam. Ao atingir o equilíbrio certo entre inovadores e interesse público, a Propriedade Intelectual visa fomentar um ambiente no qual a criatividade e a inovação possam florescer. A UE moldou o quadro que define e protege inovações e criações através da Propriedade Intelectual[37].

Não existem disposições legais especificamente aplicáveis à robótica na legislação de Propriedade Intelectual[38]. A Comissão Europeia insta a apoiar uma abordagem horizontal e neutra do ponto de vista tecnológico da Propriedade Intelectual aplicável aos diversos setores onde a robótica poderá ser aplicada, como nas normas de *hardware* e de *software* e códigos que protejam e promovam a inovação. Além disso, é exigida a elaboração de critérios para uma "criação intelectual própria" relativamente às obras passíveis de ser objeto de Direitos de Autor produzidas por computadores ou robôs.

O quadro de proteção da Propriedade Intelectual na UE permitiu à criação de um mercado interno apropriado para alcançar economias de escala para produtos e serviços caracterizados pelo uso intensivo dos Direitos de Propriedade Intelectual, que representa mais de 39% do produto interno bruto (PIB) da EU cujo valor é de aproximadamente 4,7 trilhões de euros. Cerca de metade das indústrias da UE usam intensivamente os Direitos de Propriedade

36 Disponível em: <http://europa.eu/rapid/press-release_IP-18-4160_pt.htm> e <http://europa.eu/rapid/press-release_IP-18-3362_pt.htm>.

37 Disponível em: <http://www.europarl.europa.eu/RegData/etudes/BRIE/2018/615662/EPRS_BRI(2018)615662_EN.pdf>.

38 Um drone é dotado de patente e de *softwares*. A problemática que pode recair é que um produtor copie a patente e/ou *software* do concorrente, daí recaem-se em problemas de uso sem autorização dos Direito de Propriedade Intelectual.

Intelectual, representando diretamente 26% de todos os empregos na UE e cerca de 56 milhões de empregos diretos. Além disso, a indústria intensiva em DPI paga uma remuneração mais elevada, com um prêmio superior a 40% e representa 90% do comércio da UE com o resto do mundo. As indústrias intensivas em Direitos de Propriedade Intelectual demonstraram ter lidado melhor com a grave crise econômica do que a economia como um todo, contribuindo para a prosperidade e competitividade da Europa.

Ao se ler este panorama dos resultados econômicos da produção de Propriedade Intelectual, percebemos que podem e devem estar alinhados a exploração dos Direitos de Propriedade Intelectual e da Robótica (marcas, patentes, desenho industrial e s*oftwares*) ao nível do Mercado Único da União Europeia.

5. CONCLUSÕES

Os robôs e a inteligência artificial estão cada vez mais sofisticados e trazem algumas implicações[39]. A tendência para a automatização pode e deve ser concebida de tal forma que preserve a dignidade, a autonomia e a autodeterminação dos indivíduos. Os produtores e criadores devem assumir a responsabilidade jurídica pela qualidade da tecnologia que produzem.

Nosso objetivo em mostrar esta problemática é mostrar que a produção dos drones ou robôs voadores, dotados de Direitos de Propriedade Intelectual, foram desenvolvidos sem colocar entraves à inovação. Contudo, as condutas dos usuários destas tecnologias podem prejudicar a segurança e privacidade da sociedade. Neste sentido, em Portugal encontram-se vigentes regulamentações sobre o tema.

Em nenhum momento, tentou-se impedir a evolução da inovação, da tecnologia e da automação[40]. Mas, a partir do momento que a evolução das ferramentas tecnológicas pode prejudicar a segurança da sociedade, pela conduta dos usuários de drones, é preciso sensibilidade jurídica para promover estudos e estimular a inovação com segurança. Salientamos que é necessário consagrar recursos suficientes à procura de soluções para os problemas sociais, éticos, jurídicos e econômicos suscitados pelo desenvolvimento tecnológico e pelas suas aplicações no escopo da robótica e da Inteligência Artificial[41].

39 "*The potential benefit of robotics and artificial intelligence are enormous. Deployed with care, robotics and artificial intelligence will continue to raise our collective standard of living the world over*". Calo, Ryan M. *Peeping Hals*. In: Artificial Intelligence, Elsevier, nº 175, Ano 2011, 940-941.

40 "*At the same time, we recognize that these technologies seem to jump out of the pages of science fiction, and the ethical dilemmas they raise also seem too distant to consider, if not altogether unreal. But as Isaac Asimov foretold: "It is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be . . . This, in turn, means that our statesmen, our businessmen, our everyman must take on a science fictional way of thinking" [7]. With human ingenuity, what was once fiction is becoming fact, and the new challenges it brings are all too real*". ABNEYB, Keith; BEKEY, George e LIN, Patrik. *Robot ethics: Mapping the issues for a mechanized world*. In: Artificial Intelligence, Elsevier, nº 175, Ano 2011, 942-949.

41 Para tanto, compreendemos como essencial o estímulo à investigação e inovação; o cumprimento dos princípios éticos; normalização, segurança e proteção, circulação dos dados e respeito aos Direitos de Propriedade Intelectual.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNEYB, Keith; BEKEY, George e LIN, Patrik. *Robot ethics: Mapping the issues for a mechanized world*. In: Artificial Intelligence, Elsevier, n. 175, ano 2011, 942-949.

BODEN, Margaret; BRYSON, Joanna; CALDWELL, Darwin; DAUTENHAHN, Kerstin; EDWARDS, Lilian; KEMBER, Sarah; NEWMAN, Paul; PARRY, Vivienne; PEGMAN, Geoff; RODDEN,Tom; SORRELL, Tom; WALLIS, Mick; WHITBY, Blay; WINFIELD, Alan. *Principles of robotics: regulating robots in the real world*. In: Connection Science, v. 2, n. 29, ano 2017, 24-129. Disponível em: <https://doi.org/10.1080/09540091.2016.1271400>.

BYRNE, Edmund F. *Making Drones to Kill Civilians: Is it Ethical?*. In: Journal of Business Ethics, v. 147, ano 2018, 81-93. Disponível em: <https://link.springer.com/article/10.1007/s10551-015-2950-4>.

CALO, Ryan M. *Peeping Hals*. In: Artificial Intelligence, Elsevier, n. 175, ano 2011, 940-941.

CATEA, Roxana Mihaela. *Challenges of the Not-So-Far Future: Eu Robotics and AI Law in Business*. Disponível em: <http://cks.univnt.ro/uploads/cks_2018_articles/index.php?dir=2_private_law%2F&download=CKS_2018_private_law_005.pdf>.

FISCHER, Amy Sherry; CARTMELL, Jordyn Eckert e FRANK, Liam. Drones: *A New Front in the Fight Between Government Interests and Privacy Concerns*. In: Defense Counsel Journal, v. 84, n. 4. Disponível em: https://www.iadclaw.org/publications-news/defensecounseljournal/drones-a-new-front-in-the-fight-between-government-interests-and-privacy-concerns/>.

FROOMKIN, Michael; COLANGELO, P. Zak. *Self-Defense Against Robots and Drones*. In: Connecticut Law Review, v. 48, n. 1, nov./2015. Disponível em: <http://robots.law.miami.edu/2014/wp-content/uploads/2013/06/Froomkin-Colangelo-Self-Defence-Against-Robots-March-2014.pdf >.

LEENES, Ronald; LUCIVERO, Federica. *Laws on Robots, Laws by Robots, Laws in Robots: Regulating Robot Behaviour by Design*. In: Law, Innovation and Technology, v. 6, n. 2, ano 2014, 193-220. Disponível em: <http://dx.doi.org/10.5235/17579961.6.2.193>.

LEENES, Ronald; et.al. *Regulatory challenges of robotics: some guidelines for addressing legal and ethical issues*. In: Law, Innovation and Technology, v. 9, n. 9, ano 2017, 1-44.

SILVA, Nuno Sousa. *Direito e Robótica: uma primeira aproximação*. In: Revista da Ordem dos Advogados. Lisboa: Ordem dos Advogados, v. 1, n. 77, jan./jun. 2017, 485-551.

CYBERLAW by CIJIC

THE ORGANIZATIONAL STRUCTURE OF AN INTERNATIONAL TRIBUNAL FOR THE INTERNET

DANIEL FREIRE E ALMEIDA *

* Ph.D. Professor of International Law, Internet Law and International Relations at Catholic University of Santos – PhD and Master´s Program. Postdoctoral researcher at Georgetown University (Washington-DC).
Contacto: da616@georgetown.edu , danielfreire@unisantos.br

RESUMO

Este artigo tem como principal objetivo apresentar a estrutura organizacional formulada pelo autor para criar um Tribunal Internacional para a Internet.

O texto de trabalho é dividido seis secções, que proporcionam o conhecimento de relevantes e inovadores argumentos da organização interna do Tribunal Internacional para a Internet, incluindo sua Assembleia Geral, a Secretaria-Geral, a Câmara dos Juízes, a Câmara de Procuradores, a Associação Internacional de Advogados e os Diplomatas do Tribunal. Tudo, pois, a ser estabelecido devido aos desafios que as jurisdições nacionais e regionais enfrentam para aplicar suas decisões judiciais e legislações no ambiente internacional da Internet.

Palavras-chave: Direito Internacional – Tribunal da Internet – Ambiente Digital - Direito na Internet – Tribunais Internacionais – Governança Global.

ABSTRACT

This article has as its main objective to present the organizational structure formulated by the author to create an International Tribunal for the Internet. The working paper is divided into six sections that provide the relevant knowledge and innovative arguments of the internal organization of the International Tribunal for the Internet, including on the General Assembly, the General Secretariat, the Judge's Chamber, the Chamber of Prosecutors, the International Association of Lawyers, and the Diplomats of the Tribunal. All therefore to be established due to the challenges that the jurisdictions of the national and regional spaces confront to apply their judicial decisions and laws in the international environment of the Internet.

Keywords: International Law – Internet Tribunal – Digital Environment - Internet Law – International Courts – International Tribunals – Global Governance.

1. GENERAL INTRODUCTION

Getting back to this distinguished Cyberlaw review, and facing innovative challenges in the Internet world, we come across the need of one International Internet Tribunal and global legislation on the Internet.

In fact, recently, the European Union have adopted the new REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[1], in effect since May 25th, 2018 (General Data Protection Regulation-GDPR).

There is no doubt about the necessity and importance of this *new* European regulation[2]. But, what about the rest of the World? Is the Internet "online" just only inside the European Union? Since when the Internet should be divided by territories? And, what about the Internet companies and stakeholders, worldwide dispersed? Only a few questions arising after this European legal concretion.

Furthermore, we know that the European Court of Justice (ECJ) ruled that search engines, like Google, Bing or Baidu, need to remove the link between search results and a website if it contains material that the individual deems should be "*forgotten*"[3].

In this sense, according to the decision, the Article 4(1)(a) of Directive 95/46 (now repealed by the GDPR) is to be interpreted as "*meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell*

1 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PT .

2 Vide DIXON, Helen. *Regulate to Liberate. Can Europe Save the Internet?* New York: Foreign Affairs. September 19, 2018. Accessed September 19, 2018. Available at https://www.foreignaffairs.com/articles/europe/2018-08-13/regulate-liberate .

3 See Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=153853&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=380763 .

advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State."[4].

In other words, Google, in case, is considered a controller of personal data, and the national data protection law (from Spain) is applicable, even if indexing happens in the United States of America or somewhere else.

In turn, the new GDPR is following and enforcing that the "Territorial scope" of the Regulation (2016/679) applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the European Union or not. Likewise, the Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or the monitoring of their behavior as far as their behavior takes place within the Union. Besides, the new GDPR applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

This new context has resulted in the emergence of a growing complexity of new laws and decisions, both at the domestic and/or international dimension levels, that can easily start an international conflict of decisions and laws, like the one provided by the European Court of Justice in this recent case.

Like I wrote before in my previous book[5], the fact that the European Union is trying to "speak" the same language in regulatory terms and decisions is, indeed, an excellent start. At last, it should be emphasized that the European Union, aware of the need for cooperation and international dialogue - because of the transnational aspects of the Internet and international e-commerce - stipulated as key priority issues the regulation and legalization of the Internet.

---

4 *Cfr*. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=153853&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=380763 .

5 See FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

However, the Internet is Global, international, worldwide. We will need to give a step forward. In fact, we need to do it now.

The international aspects of the Internet requires new forms of global governance to deal with these global issues. The global nature of the Internet and its global reach, provided by a worldwide architecture, presents a series of jurisdictional complexities to any country wishing to exercise its sovereign power ordinarily.

With the EU doing this, legislating on the world of the internet, without recognized global legitimacy but with manifest repercussions all over the world,, we will face conflicts of jurisdiction and laws (in fact that is what happening now!)[6].

More, within EU, take Germany, for example. According to the Interior Minister Horst Seehofer, Germany is considering a legal framework for cyberwar, enacting laws that would let it respond actively to foreign cyber-attacks, regardless of latitude, be it China, Iran, Russia, others... The Internet world demands a solution like an International Tribunal for the Internet, with international treaties.

The present working paper has as its principal goal to show the proposal to establish an International Tribunal for the Internet[7]. More specifically, we will address the organizational composition of the Tribunal, with some its basic tasks[8].

The Internet constitutes a topic that concerns all peoples, and it is used across the globe, where different computer systems are interconnected and the various languages find their universal terminology.

To the users, companies, States and other internet stakeholders, the benefits of one global judicialization of international disputes on the Internet, with proper organization, would allow for greater efficiency in the search for justice and legal security. On the other

6 See, for example, the case of China: SEGAL, Adam. *When China Rules the Web*. New York: Foreign Affairs. September 19, 2018. Accessed September 19, 2018. Available at https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web .

7 This working paper is based on our PHD Thesis defended at Coimbra University in 2012 (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

8 For a complete version of our proposal, please see our book: FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

hand, the arguments seeking to overturn the additional possibility of a world Law, Global or a *Universelles Völkerrecht* at no time mention the growing and dependent phenomenon of the Internet.

The paradigms have changed, we need to understand them, formulate new international routes, and address them. Because of this goal, and in order to resolve the issues raised, we are to propose the unprecedented International Tribunal for the Internet, presenting it in its essential organizational aspects.

Essentially, it is emphasized that its scope should be global, encompassing natural persons, companies, States and International Organizations, and to deal with **international** cases of the Internet. That is, the jurisdiction of the International Tribunal for the Internet should then be of a complementary range to the national jurisdictions. In fact, there would be no reason to move the adjudicative task at international level if the resolution materializes in the area of national scope of the disputed legal question.

The current paper is divided into six parts, raising some relevant topics to internal Organization of the International Tribunal for the Internet, namely: the General Assembly, the General Secretariat, the Judge's Chamber, the Chamber of Prosecutors, the International Bar Association, and diplomats of the Tribunal, to be established in order to overcome the challenges that national and international jurisdictions face in enforcing their respective judicial decisions and laws.

II. INTERNAL ORGANIZATION AND STRUCTURE OF THE INTERNATIONAL TRIBUNAL FOR THE INTERNET

It is appropriate to address, at this point, some relevant topics to internal organization of the International Tribunal for the Internet, including on the General Assembly, the General Secretariat, the Judge's Chamber, the Chamber of Prosecutors, the International Association of Lawyers, and diplomats of the Tribunal.

This approach will allow us to visualize the structure necessary to carry out the specific functions of prosecution of international cases involving the Internet and International Electronic Commerce, and duly justified by the challenges presented in the present Internet World[9].

1. General Assembly

It is initially necessary to the Tribunal to be provided with a legislative competence center set up by a **General Assembly**. Likewise, it is critical to the future goals of the international adjudicative body, to have their own place of reserved seat to the representatives of the Member States and Internet stakeholders.

Thus, regular and special meetings may be scheduled depending on the circumstances and needs, which certainly exist for these occasions. Within the assembly, all Member States should have a voice and vote, and to be represented by diplomats, Internet stakeholders, Global companies and technical-professionals (Law, Internet, E-Commerce, Computers).

At this point, be noted that the performance of this negotiator and representative role, by States, should be carried out by highly qualified personnel in international affairs and the Internet. This is because, it is desired that the future material that also serve as an international source for the Tribunal's trials is the result of various debates in this Assembly.

9 This working paper is based on our PHD Thesis defended at Coimbra University in 2012 (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

In this context, as a way to avoid merely delaying postures or goals hinder the continuity of actions, decisions about amendments or revisions of the founder Treaty, or supervening texts that should be part of this should be taken by a majority of two-thirds Member States present and voting, along the lines of the Vienna Convention (1969), article 9, paragraph 2[10].

One important final touch, subsequent Treaties that further define questions of international Law on the Internet and Electronic Commerce, should be part of the Tribunal Founder Treaty[11].

The aim with such means is the following: start a codification of international Law on the Internet and Electronic Commerce, and that the future Member States, when carrying out accession to the Tribunal, may, at the same time, consent with the sources to be used in trials.

In that context, it is worth mentioning here the hypothesis of negative international ratification, that is, it would be adopted a faster mechanism for subsequent Treaties originated in the General Assembly of the Tribunal, be considered as adopted by the Member States, without the need of internal procedures of each country[12].

Consequently, certainty as to the rules of international Law established by those Treaties, facilitate understanding by all stakeholders, as well as the resolution of cases before the Tribunal. In addition, the development of these rules can be reported by member countries.

Therefore, the General Assembly should be put on that body where all States and International Organizations members have voice and vote at the same level.

10 Article 9, paragraph 2. reads as follows: "2. The adoption of the text of a treaty at an international conference is effected by two-thirds majority of States present and voting, unless these states by the same majority, decide to apply a different rule. " *Cfr*. VIENNA CONVENTION ON THE LAW OF TREATIES, Vienna, 1969. On the matter of merely delaying postures or goals hinder the continuity of actions, *Vide* CASSESE, Sabino. *Regulation, Adjudication and Dispute Resolution Beyond the State.* Heidelberg: Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht, Fall, 2008, p. 09.

11 To check out our complete Treaty proposal ("THE FOUNDER TREATY OF AN INTERNATIONAL TRIBUNAL FOR INTERNET"), please see our book: See FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

12 This assumption would not only be set if the country expressly declared its untying to the dictates of the Treaty.

Everything, thus, compatible with the egalitarian principles among countries in the Public International Law. But, the configuration of the General Assembly will guarantee the presence and voice to the Internet stakeholders, to the Global companies and experts.

Additionally, in general terms, the General Assembly of the Tribunal would examine and promote the guidelines regarding the administration of the Tribunal, determine the budget and its guidelines, and seek to improve the Tribunal's efficiency through its decisions.

2. General Secretariat – Servers

Continuing, the Tribunal must host a General Secretariat. Referred body, managed by the General Manager, must focus on management, on a permanent basis, of all the Organization's internal structure and functioning, communication and negotiation of future interests.

It should consist of neutral servers in any way representing the desires or the policy of their own countries of origin or nationality. This quality, neutrality, should be very well represented, also, and above all, by the figure of Director General of the International Tribunal for the Internet.

The latter, head of international relations of the Tribunal, must seek to establish relations with the countries, International Organizations, Internet stakeholders and companies, as well as enter into treaties and cooperative systems on behalf of the Tribunal.

Continuing, in our view, the servers must be appointed by the Secretary, through global selection process in order to meet the qualified staff necessary to technical services and of support of the Tribunal, on the advice of Judges, Prosecutors, the International Bar Association, the diplomats and the Director General.

Yet, regarding the recruitment of staff, the Director General should seek to ensure the highest rules of efficiency, competence, impartiality, neutrality and integrity, taking into account the objectives of the body.

In no event could be any indication on the part of judges, prosecutors, diplomats or lawyers in world selection processes.

The only direct election would be the own Director General, open ballot, by a majority, considering the recommendations of the countries in the Assembly of the Member States.

The Director General should be elected for a period of five years, to perform duties on an exclusive basis, with no right to reelection. Due to the nature of the position, after the mandate would receive a reform to the same rules it had during the period of his term, ceasing in the moment that assumes any other gainful activity.

In addition, even with regard to the category of servers, the Tribunal should hire expert consultants. This is to assist the different organs of the Tribunal in its international and digital activities.

Therefore, the said category, in their specialized areas, would transit between the various organs, according to the need of the Tribunal.

They should, therefore, be of different areas of knowledge, with primacy for professionals in the Internet field, Informatics, software, applications, Information Systems, and Electronic Commerce.

3. Judge's Chamber

As a result, then, of their own goals already posted before the Tribunal, we found that the novel organization must have its adjudicative sector**.**

In primacy, the Judge´s Chamber gather Judges. These, in essence, should be guided by determinations that do not emphasize any State or private interest in their judgments, decisions and advisory opinions.

The Judges would be properly divided into sub-chambers of Instruction, Specialized Chambers (divisions in international legal areas of the internet, and a general division), and Boards of Appeal. In addition, any Judge of the Tribunal could, for distributive draw, draw up international advisory opinions.

Thus, initially, the sub-chambers of Instruction would examine, preliminarily, that the proposed action would fit between the Admissibility conditions. It should, for example, come across clearly unfounded actions. On the other hand, others may be irrelevant. Still, some may only want to establish conflicts in order to disturb

international personalities, companies or States, without having concerned any legal relationship with the person concerned.

Continuing, the Judge's Chamber would be divided into specialized chambers, that would dedicate their efforts to the trial of disputes involving the International Law on the Internet, with the knowledge of various fields of Law, including the Criminal Law, the Tax Law, the Electronic Commerce, the Civil Law, the Business Law, and others to raise the formation of a specialized Chamber. Those matters that do not concern a specialized division would be allocated to a Judge's Chamber General. In this regard, we can anticipate that the division into specialized Chambers does not withdraw, but objectives, an interdisciplinary adjudicative analysis.

In fact, the multiplicity of ways in which the phenomenon of Internet manifests and incorporates justified, largely, an interdisciplinary international adjudicative approach[13]. Under these angles, the purpose of the Tribunal is to go further and seek to overcome the natural demarcation of areas of Law. In other words, integrate, and then separate the areas of Law in its international dimension on the Internet.

In addition to the practical interest, the division into specialized Chambers is to ensure qualitatively that trials be supported by qualified judges in areas justifying deep meritorious knowledge. However, where the international and the Internet present to serve as an integration reference.

In summary about the own intricacies and details of the above disciplines must be guided by an international and Internet perspective in the evaluation of their cases[14].

Next, it is necessary for the body will house a Chamber of Resources, guaranteed up a double and ultimate degree to the demands of the Tribunal.

The judges dedicated to this section would be exclusive and should not participate in trials in Specialized Chambers. *The exception would give only the advisory tasks, where the resource judges could also contribute.*

13 *Vide* UERPMANN-WITTZACK, Robert. *Internetvölkerrecht.* Archiv des Völkerrechts, Volume 47, Number 3, September 2009 , p. 261/283.
14 *Vide* UERPMANN-WITTZACK, Robert. *Internetvölkerrecht.* Archiv des Völkerrechts, Volume 47, Number 3, September 2009 , p. 261/283.

Again, the Appeals Division would be divided into specialized segments, meeting the same criteria reserved for Specialized Chambers. Note that for each demand, upon appeal, where three participating judges.

Finally, the Tribunal should set aside additional task to each of the judges, including those of the Appeals Chamber, in order to participate in sweepstakes relating to consultations to the International Tribunal for the Internet.

Great international repercussion of questions requiring the interpretation of Applicable Law in the International Tribunal for the Internet could be submitted to the Advisory assessment of the Tribunal.

The Tribunal would fulfill its task in this area. Logically, an important collation, the Judge's Chamber shall have a large number and qualified judges. In the opposite direction, at this Tribunal the number should also mean quality. First, quantity determination must be guided by sufficiency to avoid up accumulations of cases, slow, and dissatisfaction of international (and National!) jurisdictional. Also, it cannot be the privilege of a few judges.

The aim, in fact, is hiring (by Global selection process) an unprecedented number of judges to the international scope of the Tribunal[15]. In other words, at least 2 per nationality, of the member countries[16]. In this case, it would be at a later stage, therefore, represented the main legal systems of the world, and would have, likewise, equitable geographical representation.

These criteria are not equivalent to saying that the judges would be appointed by the countries. Not even participate in the trials as representatives of their countries. Therefore, they cannot be political or ideologically, directly nominated by their countries of origin.

Even with regard to nationality criteria, the national of any member country can apply to be a Judge, ensuring at least 2 places per country, which should be increased by the need of the Tribunal, and in proportion to the number of direct connections to

15 The International Criminal Court meets in its "Judicial Divisions" 18 judges, while the International Court of Justice is composed of 15 judges and a "Register". However, we should be aware that the International Criminal Court held only 26 cases to date, while the International Court of Justice held only a little bit more of 150 cases. *Cfr*. *International Court of Justice*, Available at: https://www.icj-cij.org/en/list-of-all-cases . *Cfr*. *International Criminal Court*, Available at: https://www.icc-cpi.int/Pages/cases.aspx , Accesses in 09.18.2018.
16 Only member countries could have nationals in the internal composition of the Tribunal as a means of pressure to accession.

the Internet that the country has. That is, the country that has the most Internet users now has more judge positions in the Tribunal.

The intention here is that digital inclusion efforts of each country result in proportional guarantee vacancies for the Tribunal's office. In this line, for hiring a judge, they should, on its own initiative, apply to the Tribunal, through global selection process, with criteria that seek to represent what is desired from a Judge of the International Tribunal for the Internet.

It should be noted, fundamentally, that this procedure contradicts, on purpose, the criteria adopted for filling positions in other international legal bodies. This is because the Tribunal for the Internet is not intended to be a political instrument, used to embellish the partisanship of personalities, comrades, an intentional ideology or house of favor of certain counterparts.

After all, it should be noted that the merit criteria, based on legal knowledge, should guide the conduct of completing the Tribunal's office. Note, that it is not the case here to exacerbate the role of the lawyer in the case of judges Chamber. The desire is that the diplomatic or political criteria remain assigned to the negotiations in the General Assembly of the Tribunal, suitable location for the governments of each country and stakeholders to indicate their representatives and negotiators.

Still on the judges, as of now, some criteria can be tacked, and for now, then, as we talk about the quality of judges. They must have solid academic training; recognized legal competence; have specific knowledge of the operation of the qualities and details of International Law, the Internet and Electronic Commerce; they should devote themselves on an exclusive basis; gather specific knowledge of the complementary legal area, to which will dedicate in Tribunal: Criminal Law, Tax Law, the Electronic Commerce, the Civil Law, the Business Law; they should be guided by the independence in all functions; and shall have an excellent knowledge of one of the languages of the Tribunal[17].

17 To find out our complete Treaty proposal ("THE FOUNDER TREATY OF AN INTERNATIONAL TRIBUNAL FOR INTERNET"), please see our book: See FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

Due to the above criteria, the Secretary General must then be a remarkable Commission to prepare, conduct and decide to take the global selection process, ensuring that the fairs meet the parameters linked to the objectives and the material in the Statute, including its Applicable Law, and is made new selection every year, in order not to occur cases of vacancy, due to vacation or retirement of judges.

The position should be exercised until the date of retirement of the Magistrate, never before eight years of exclusive exercise in Tribunal[18], and with a minimum of age.

Judges should receive annual salaries, and tax-exempt, under the Vienna Convention on Diplomatic Relations (1961) and in alignment, with what was established in the Convention on the Privileges and Immunities of the United Nations in 1946, and in the Convention on the Privileges and Immunities of the Specialized Agencies (1947)[19].

4. Chamber of Prosecutors

Prosecutors must instruct the international investigations, submit and track complaints based on information about the Tribunal's jurisdiction practices. That way, you can link the Prosecutor to offices to investigate and report practices that would fall in the jurisdiction of the International Tribunal for the Internet.

First, an important point: he must conduct investigations, either on his own initiative or at the instigation of interested parties (persons, companies or States), along the lines arranged on Admissibility and Conditions Criteria[20]. Consequently,

18 The minimum number of years should be a candidate compromise in order to avoid those who would use the position before the Tribunal only as a way to spend a certain time in a new country or relevant position.

19 These conventions have been used as a model whenever a new International Organization prepares and negotiates its founder Treaties and the Headquarters Agreements concluded accordingly. *Vide* UNITED NATIONS. Convention on the Privileges and Immunities of the United Nations, 1946. *Vide* UNITED NATIONS. Convention on the Privileges and Immunities of the Specialized Agencies, 1947. Vide *Vienna Convention on Diplomatic Relations*, 1969. *Vide* REINISCH, August. *The Immunity of International Organizations and the Jurisdiction of Their Administrative Tribunals*. New York: International Law and Justice Working Paper 2007/11, p. 2 et seq.

20 Please see our complete Treaty proposal ("THE FOUNDER TREATY OF AN INTERNATIONAL TRIBUNAL FOR INTERNET"), in our book: See FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

they should report activities that may be subject to trial by the Tribunal, within those criteria, and that have not been made by interested parties.

For this, they could collect additional information from States, companies, people and other International Organizations as well as seek to receive written, digital or oral testimony at the Tribunal headquarters or regional headquarters located in the participating countries.

On the other hand, when the events are triggered by persons, companies and/or States, as subjects of certain actions, Prosecutors should only participate in a complementary way in assisting the judges' decisions. All activities should be guided by prudence and neutrality. However, in the shortest possible time. For more than once, we refer to extremely quickly and relocation of the content on the Internet qualities. All the Tribunal's activities should take this into consideration.

Prosecutors should seek, therefore, innovative actions and modern research methods. The request for information offices should be scanned and sent by digital means, in order of the modern Rules of Procedure.

An important collation, Prosecutors should be engaged in the same manner and criteria that we referred to the Judges. In fact, the only distinction will be a function of the position desired by the candidate, each of whom must apply for one career during a worldwide selection process: either Judge or Prosecutor, International Lawyer, or server, or Diplomat of the Tribunal.

5. International Bar Association

Another organization, as member of the Tribunal's structure, should be an International Bar Association.

The claimants should, in cases where they have no financial means to hire a lawyer in their country of origin, have free legal representation.

The criteria to be used to verify the situation will be interested to family income, which should not exceed €1,000 or $1000, in principle. The service should be as broad as possible. Therefore, the lawyers must reside in the country of the plaintiff, given the need for criteria to be reviewed by the Tribunal, through the Director General, and also on the recommendation of the Member States. The difference here, compared to

other positions, is that the lawyer must be entered on the national advocacy organ with a valid license to practice the law.

The costs of their activities, as well as their salaries shall be paid by the Tribunal. However, its work registration will be held in the country of the Tribunal. Here again, it would be proposed by the immunities provided by the Vienna Convention on Diplomatic Relations of 1961, including its headquarters and office work, the Convention on the Privileges and Immunities of the United Nations (1946), and the Convention on the Privileges and Immunities of Specialized Institutions (1947)[21]. The reason for this will be to ensure the independence and necessary security for their activities in relation to the country of residence.

The lawyer at the Tribunal should also work on an exclusive basis. He should follow audiences *online* to be made to the Tribunal, from the country of location of the branch of the International Tribunal for the Internet. In addition, he shall issue opinions on matters involving the country's Law on which it is situated, and defend the legal interests of the Tribunal with the assistance of the International Organization diplomats.

At the point above, namely of opinions, the intention, too, is to lend input to the Judges in their advisory role.

6. Diplomats of the Tribunal

The Tribunal should form a body of negotiating diplomats to the external interests of the Tribunal. This group, headed by the Director General, represent the purposes of the Tribunal, organizing inclusive conferences, meetings focused on multilateral negotiations, actively participate in regular and special meetings to promote the Law Applicable to the Tribunal and which international diplomatic positions the Tribunal should adopt. In other words, which are their goals, proposals, strategies, and

21 These conventions have been used as a model whenever a new International Organization prepares and negotiates its founder Treaties and the Headquarters Agreements concluded accordingly. *Vide* UNITED NATIONS. Convention on the Privileges and Immunities of the United Nations, 1946. *Vide* UNITED NATIONS. Convention on the Privileges and Immunities of the Specialized Agencies, 1947. Vide *Vienna Convention on Diplomatic Relations*, 1969. *Vide* REINISCH, August. *The Immunity of International Organizations and the Jurisdiction of Their Administrative Tribunals.* New York: International Law and Justice Working Paper 2007/11, p. 2 et seq.

subsequent negotiations (headquarters, regional offices, diplomatic representation, guarantees, and immunities).

This body shall act in accordance with the guidance of the Director General, through representation, information gathering, negotiation and promotion of interests of the International Tribunal.

Timely, again mention here that all servers, attorneys, diplomats, international lawyers should be hired in the same manner and criteria that we referred to the Judges.

The only difference is due to the position wanted by the candidate, each of whom, as noted, apply for one job during a worldwide selection process: either Judge or Prosecutor, International Lawyer, or server, or Diplomat of the Tribunal[22].

22 The positions in question receive such salaries, cost of cover, benefits and possible reform established by a Meeting of States Parties. These salaries and allowances cannot be reduced.

III. CONCLUSIONS

For all as proposed above, both with regard to Internet potentialities, and about new problems and conflicts introduced by it, it is justified that the direction for an International Tribunal for the Internet should be suitable for the new world of Internet.

In other words, if we repeat everything that had been done regarding some national court procedures, *and possibly international*, to design a new Tribunal, may fall in the same slow errors, excess delaying resources, few cases, inefficiency of decisions, among other challenges already historically investigated by scholars around the world.

Indeed, the resolution of international Internet disputes, requires a new paradigm of international justice. Therefore, the best results, for the Internet World, are very important [23] .**That what we want by addressing an International Tribunal for the Internet[24]**.

Essentially, what is desired, in addition to the identification and analysis of relevant problems which presents itself, is to idealize an effective solution. In fact, the view of the problems arising in the prosecution of international Internet issues and Electronic Commerce, opened, thereby, exciting ways to call for a solution.

The idealization of an International Tribunal for the Internet is a solution that, for us, is the best technique for legal and international conflict resolution of international Law on the Internet. Moreover, fundamentally, we must emphasize that the freedom that both attracts people to the Internet at the same time, and paradoxically, to be properly maintained need some sort, either by new regulatory means, whether by new judicial means.

Nevertheless, the establishment of an International Tribunal for the Internet, which we propose in this working-paper, can be improved in the course of future times, by those

---

23 *Vide* WHITING, Alex. *In International Criminal Prosecutions, Justice Delayed Can Be Justice Delivered.* Harvard International Law Journal, Volume 50, Number 2, Summer 2009, p. 323/364.

24 A complete list of arguments, reasons and details can to be found in our PHD Thesis defended at Coimbra University (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

.

wishing to also devote to the acquisition of true international Internet issues, and reflect on the best alternatives.

But everything should be done without neglecting the practice cases, the international reality of the Internet and E-Commerce, and without, fundamentally, despising academic and professional studies that are presented worldwide. Furthermore, although several statements or idealizations may find diverging forces and information on other precedents, we can say after borderless readings, and long critical meditations, that the present moment of international relations provided by the Internet offers scenarios and justifications to more modern and humbly bold positions. As a matter of fact, as evidenced by the digital world, the Internet has been a virtual space of convergence and concentration, unprecedented, of the most varied forms of information, communication, commerce, services, entertainment and crime.

We shall not respond to this new world with old regulatory and national judicial tools. In fact, the Internet meets certain characteristics and natural conditions that challenge old judicial experiences and regulatory requirements of resolution of legal disputes, locally and internationally. Indeed, digital networks operated by the companies are global, and the social structure in which they are based, digital networks, is by definition global. As we can see, the new patterns of choice for communication and social interaction online replaced territorially limited ways of human relationships.

Important here to be noted are the consequences of these changes and implications, huge for the future of our societies, increasingly digital. These digital communication tools pose a different set of legal problems, ranging from child pornography, passing through cybercrimes, conflicts between e-commerce companies and States or persons, cyberespionage, system intrusions, cybersecurity, the use of cryptocurrencies and blockchain for financial crime, money laundering and tax evasion, cyberattacks, among many and many others. Such cases are proliferating in Tribunals worldwide, involving a growing number of people, with an international dimension. In fact, in all areas where the Internet "manifests itself" we find significant legal repercussions reaching the Tribunals more constantly.

Disputes arising from new Internet activities put traditional judicial powers under uncomfortable situations, much because of the speed of arguments, instantaneity, internationality, exterritoriality, and hosting of the Internet data abroad (which can be used as an evidence in courts around the world).

The legal techniques of the past have not been able to respond to all new challenges. Likewise, are the legislative challenges, given the difficulty in achieving to subject the behavior of a citizen linked to multiple sovereignties, when in any trials.

Multiple activities conducted through the Internet are inherently transnational, presenting complexities on the implementation of national or regionally specific regulations. Technological advances have, through the numerous activities offered by the Internet, significant interactions with endless interferences on distant individuals physically, but more and more virtually connected.

It is in this line of reasoning then, that by taking legislative initiatives of a country that can slide wherein the Internet area, we can check a state interest in enforcing such rules for the acts and persons located in its national space, like the GDPR. But we find, on the other hand, that many (millions) other acts and people would be outside of the effective context of these laws, even relating with people and domestic companies through the Internet.

In other words, we can conclude that the limits on the scope of the regulations, in the affairs of the Internet, are faced by any country, similarly, no matter the content of the Law that arises. More specifically, we can address that some basic qualities of the Internet have offered resistance to the application of national legislation in the activities developed by the World Wide Web, as the globalization of the Internet, International electronic communications and data, and the multinational Electronic Commerce, exercised by the global digital companies.

Therefore, growing needs require new forms of global governance to deal with all these digital issues, but also global ones. Indeed, people and companies look for "*global greater certainty and justice*" in international affairs involving the Internet.

That is why we present the International Tribunal for the Internet, originally since 2008[25].

25 A complete list of arguments, reasons, the history, and details can to be found in our PHD Thesis defended at Coimbra University in 2012 (Portugal, European Union). See FREIRE E ALMEIDA, Daniel. An International Tribunal for the Internet. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

IV. BIBLIOGRAPHY

CASSESE, Sabino. *Regulation, Adjudication and Dispute Resolution Beyond the State*. Heidelberg: Max-Planck-Institut für ausländisches öffentliches Recht und Völkerrecht, Fall, 2008, p. 09.

DIXON, Helen. *Regulate to Liberate. Can Europe Save the Internet?*. New York: Foreign Affairs. September 19, 2018. Accessed September 19, 2018. Available at https://www.foreignaffairs.com/articles/europe/2018-08-13/regulate-liberate .

EINISCH, August. *The Immunity of International Organizations and the Jurisdiction of Their Administrative Tribunals*. New York: International Law and Justice Working Paper 2007/11, p. 2 et seq.

FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

GOOGLE SPAIN SL AND GOOGLE INC. V AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ, Available at http://curia.europa.eu/juris/document/document.jsf?text=&docid=153853&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=380763 .

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=PT .

SEGAL, Adam. *When China Rules the Web*. New York: Foreign Affairs. September 19, 2018. Accessed September 19, 2018. Available at https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web .

THE FOUNDER TREATY OF AN INTERNATIONAL TRIBUNAL FOR INTERNET, in FREIRE E ALMEIDA, Daniel. *An International Tribunal for the Internet*. São Paulo: Almedina, 2016, available at: https://www.almedina.net/ebook_info.php?ebooks_id=97885849301426 or https://www.amazon.co.uk/International-Tribunal-Internet-Daniel-Almeida-

ebook/dp/B018HHLO70/ref=sr_1_2/262-5128826-5206617?s=books&ie=UTF8&qid=1537272381&sr=1-2&refinements=p_27%3ADaniel+Freire+e+Almeida .

UERPMANN-WITTZACK, Robert. *Internetvölkerrecht.* Archiv des Völkerrechts, Volume 47, Number 3, September 2009 , p. 261/283.

UERPMANN-WITTZACK, Robert. *Principles of International Internet Law*. German Law Journal, Volume 11, nº 11, 2010.

UNITED NATIONS. *Convention on the Privileges and Immunities of the United Nations*, 1946.

UNITED NATIONS. *Convention on the Privileges and Immunities of the Specialized Agencies*, 1947.

VIENNA CONVENTION ON THE LAW OF TREATIES, Vienna, 1969.

WHITING, Alex. *In International Criminal Prosecutions, Justice Delayed Can Be Justice Delivered*. Harvard International Law Journal, Volume 50, Number 2, Summer 2009, p. 323/364.