
CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDIÇÃO N.º VIII – SETEMBRO DE 2019

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


CYBERLAW
by CIJIC

CYBERLAW by CIJIC

EDITOR: NUNO TEIXEIRA CASTRO

SUPORTE EDITORIAL: EUGÉNIO ALVES DA SILVA

PRESIDENTE DO CIJIC: EDUARDO VERA-CRUZ PINTO

COMISSÃO CIENTIFICA:

- ALFONSO GALAN MUÑOZ

- ANGELO VIGLIANISI FERRARO

- ANTÓNIO R. MOREIRA

- DANIEL FREIRE E ALMEIDA

- ELLEN WESSELINGH

- FRANCISCO MUÑOZ CONDE

- MANUEL DAVID MASSENO

- MARCO ANTÓNIO MARQUES DA SILVA

- MARCOS WACHOWICZ

- ÓSCAR R. PUCCINELLI

- RAQUEL A. BRÍZIDA CASTRO

CIJIC: CENTRO DE INVESTIGAÇÃO JURÍDICA DO CIBERESPAÇO

ISSN 2183-729

NOTAS DO EDITOR:

Nesta nova edição da revista do Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa, dada a pertença do CIJIC ao grupo do Network of Centers (https://networkofcenters.net/center/cyberlaw-research-centre-university-lisbon-school-law-cijic), a obrigação identitária desta comunidade, persuade-nos a publicar artigos em inglês. Traremos, portanto, duas investigações em anglo-saxónico.

Na oportunidade presente da publicação desta VIII Edição e dos actos legislativos nacionais em curso, foi nossa opção trazer uma visão jurídica sobre o poder, eventualmente, manipulativo da democracia através das redes sociais.

O contexto é o da eleição presidencial de 2018, no Brasil, mas o modo como se desenvolve, desde uma engenharia social mais dissimulada a uma difusão de *fake news* ou *deep fakes*, permitem utilizar tais distorção de forma globalizada. Sendo certo que carece de maior investigação o real efeito da *realidade* das redes sociais *versus* o do "*quotidiano não digitalizado*" e o resultado concreto disto em sede de apuramento final dos resultados de eleições livres e universais, parece já possível concluir que, mesmo ante esta condicionante ainda não determinada, a realidade democrática pode, efectivamente, ser *hackeavel*.

Não obstante, por princípio, a clarificação dos conceitos de *fake news* e *deep fakes*, deveria afastar-se do radical "notícia" que lhe dá a alma. Porque uma notícia corresponde a um acto jornalístico, exercício com tutela constitucional, que conclui um dado conteúdo factual, relatando acontecimentos de interesse geral da comunidade com

o maior grau de objectividade possível. Uma notícia identifica-se pela clareza, simplicidade, exatidão, e pelo bom uso da língua em que é escrita. Compreende contraditório, ou a possibilidade deste, suporta-se em fontes credíveis. Há todo um ónus ético e deontológico que sopesa uma notícia assinada por um jornalista. Toda esta súmula é uma notícia. Comentário, mesmo televisivo, liberdade de opinião, todos os outros "*fenómenos*", não se identificam com este radical conceptual. Logo, porque continuamos a insistir em querer colar uma qualquer liberdade opinativa ao conceito de "notícia"?

Não vos soa ridículo o exercício de contínuo *fact-check* a exercícios de liberdade de opinião? Desde quando é que mentira foi legalmente proibida? Mas, pelo contrário, uma notícia que veicule um facto falacioso, de cariz subjectivo, não é fortemente sancionável? Desde logo pelos poderes de regulação, pela sindicância da própria classe, pelo público?

Será assim tão difícil perceber as diferenças?

Noutro plano, em efeméride do décimo aniversário da Lei do Cibercrime portuguesa, a Lei n.º 109/2009, de 15 de Setembro, olhamos para a perspectiva da aptidão do enquadramento legal, num contexto nada fácil, de obtenção de resultados eficazes em tempos, da acção *contra-legem versus* investigação, demasiado assíncronos. Qual a razão que explica a falta de enquadramento legal nacional para o agente (digital) encoberto, quando dezenas de outras polícias de investigação, congéneres, já o fazem?

Se há disciplina onde a soberania das fronteiras físicas acabou é no digital. Outrossim, pela fragilidade dos "muros" digitais e das deficiências do enquadramento jurídico-penal nacional, abordaremos ainda o fenómeno do *Ransomware*. Dez anos volvidos da Lei do Cibercrime, e em apologia à vanguarda em que já estivemos nos idos do início da década de 90 do século passado, impõe-se no presente, em 2019, o revisitar a especialidade da lei do cibercrime. O contexto presente de *leaks* de índole variada e processos mais ou menos mediáticos, reclamam prudência. A digitalização do Estado, por outro lado, impõem mudanças assertivas. Ademais, quer a falta da criminalização do roubo de identidade digital[1], quer a complexidade jurídico-penal do

1 Atente-se por exemplo no Considerando (14) da Directiva: "(…) *A adoção de medidas eficazes contra a usurpação de identidade e outras infrações relacionadas com a identidade constitui outro elemento importante de uma abordagem integrada contra a cibercriminalidade. A necessidade de intervenção da*

Ransomware, quer a própria transposição da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013 (esgotado o prazo de transposição no ano de 2015), quer a protecção do Estado digital (e não só) reivindicam melhores ferramentas, desde logo legais, que bem que poderiam servir de impulso necessário ao dormente legislador nacional.

Por fim, tema que não sai das agendas, o Regulamento geral de protecção de dados. Desta vez, as fricções que a ferramenta *blockchain*, cada vez mais usada no contexto das relações entre particulares e organizações, compreende face ao RGPD mas, e também, a melhor consecução dos objectivos proclamados pelo RGPD que esta ferramenta pode ajudar a alcançar.

Por fim, mas antecipando o futuro, atendendo ao propósito identitário da revista, passaremos nas próximas edições a publicar artigos de investigação dos alunos do Mestrado em Segurança da Informação e Direito do Ciberespaço, trabalhos estes desenvolvidos nas cadeiras que frequentarem.

Resta-me, neste final, agradecer a todos quantos contribuíram para mais uma edição da Revista, pelo esforço e pelo trabalho, enereçando, em nome do Centro de Investigação Jurídica do Ciberespaço – CIJIC – da Faculdade de Direito da Universidade de Lisboa, um reconhecido:

- Muito Obrigado.

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

Boas leituras.

Lisboa, FDUL, 29 de Setembro de 2019

Nuno Teixeira Castro

União contra este tipo de comportamento criminoso poderá também ser ponderada no contexto da avaliação da necessidade de um instrumento transversal e abrangente da União."

CYBERLAW

by CIJIC

DOUTRINA

CYBERLAW
by CIJIC

A INVESTIGAÇÃO DO CIBERCRIME - NÓTULAS SOBRE O PARADIGMA LEGISLATIVO ATUAL E A REALIDADE TECNOLÓGICA

ARMANDO DIAS RAMOS [1]

1 Doutor em Direito – Ciências Jurídicas, pela Universidade Autónoma de Lisboa; Inspetor chefe na Polícia Judiciária, colocado na Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T); Professor Adjunto convidado no ISCAL-IPL; Editor assistente na Revista Brasileira de Direito Processual Penal. O presente artigo vincula apenas o seu autor e de nenhum modo as instituições anteriormente mencionadas.

ABSTRACT

In the 10th anniversary of the Portuguese cybercrime law we focused on legislative and technological developments in order to ascertain whether the legal norms we have are sufficient for effective criminal combat.

Among the many issues we identified, we look at the issue of using email and the undercover agent.

Indeed, the lack of modern instruments already used by several foreign counterparts in cybercrime investigation leads us to the conclusion that we need harmonized and more concrete legal instrument for a fast, fruitful and efficient investigation.

There is a need to change the current paradigm by imposing a change in the Portuguese cybercrime law.

Keywords: Portuguese Cybercrime law; Criminal investigation; judicial cooperation; cybercrime; e-mail; undercover agent.

RESUMO

Nos 10 anos da lei do cibercrime debruçamo-nos sobre a evolução legislativa e tecnológica com o intuito de apurar se as normas legais que temos são suficientes para um efetivo combate ao crime.

De entre diversos problemas que identificamos, analisamos a questão relacionada com a utilização do correio eletrónico e o agente encoberto.

Efetivamente a falta de instrumentos modernos, já utilizados por diversas congéneres estrangeiras na investigação de cibercrimes conduzem-nos à conclusão de que necessitamos de leis harmonizadoras e mais concretas, para uma investigação célere, profícua e eficiente.

Urge mudar o atual paradigma e impõe-se uma alteração da lei do cibercrime.

Palavras-chave: Lei do Cibercrime; Investigação criminal; cooperação judiciária; cibercriminalidade; correio eletrónico; agente encoberto.

1. INTRODUÇÃO

A 15 de setembro de 2019 faz 10 anos que a atual lei do cibercrime, Lei 109/2009, foi publicada. Passado um mês, a 15 de outubro de 2009, entrou em vigor e veio revogar, desta forma, a anterior lei da criminalidade informática[1].

Se, efetivamente, a lei da criminalidade informática esteve em vigor 18 anos, sofrendo apenas uma ligeira alteração, pelo decreto-lei n.º 323/2001, de 17 de dezembro, por força da introdução do euro como moeda em curso no nosso país, a atual lei, 10 anos depois, não sofreu qualquer alteração legislativa[2]. Contudo, se atentarmos à evolução da informática nos idos anos 90, do século passado, com os últimos 10 anos constatamos, indubitavelmente, que se passou de uma evolução de "passo de tartaruga" para "uma corrida de lebre", na breve alusão à fábula da corrida entre a tartaruga e a lebre.

Eis, pois, que se impõe refletir sobre estes 10 anos da lei do cibercrime, da evolução tecnológica operada nesta década e, principalmente, da evolução da cibercriminalidade e meios efetivos de combate. Não podemos olvidar os problemas associados à investigação do cibercrime, muitos deles já identificados, onde se destacam a desterritorialidade e a anonimização como matrizes para propalar a atividade delituosa.

Estará a lei do cibercrime devidamente atual face aos novos e cada vez mais complexos artefactos utilizados no cometimento de delitos informáticos ou por via informática? Deverá a investigação criminal, para ser mais célere, recorrer a vias informais, tanto a nível nacional como com as congéneres estrangeiras, para lograr o êxito de identificação dos criminosos e os entregar à Justiça?

Estas são algumas perguntas (problemas) que levantamos e que tentaremos dar resposta. Desde já fica o alerta que as instâncias europeias se têm preocupado com estes fenómenos criminológicos e definindo uma "agenda digital" para o combate à cibercriminalidade. Contudo, face à globalização da internet, bastarão as medidas europeias para um eficaz combate? Não restam dúvidas que atenuam os efeitos do cibercrime e ajudam a minimizar o problema. Ainda assim não poderemos olvidar que grandes empresas, presentes na Europa, são norte americanas, onde se destacam a Google e o Facebook, ou chinesas, tais como a Amazon e a Alibaba.

Os problemas agudizam-se fora da Europa uma vez que se torna mais difícil obter elementos conducentes à identificação dos suspeitos ou à recolha de prova digital. Efetivamente os mecanismos adotados, por diversas empresas estrangeiras, já permitem uma

1 Lei n.º 109/91, de 17 de agosto.
2 Encontrando-se Portugal em incumprimento uma vez que já deveria ter adaptado para o direito interno a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013.

celeridade na obtenção de elementos de provas. Desde logo deixou de ser necessário a emissão de cartas rogatórias bastando que o pedido seja efetuado por *e-mail*, emanado da autoridade judiciária competente, certificado pela respetiva assinatura digital. Também foram criados mecanismos protocolares entre essas empresas e as autoridades judiciárias portuguesas, no sentido de acelerarem os pedidos de informações e obtenção de elementos que, a ser obtidos por carta rogatória, poderiam tornar-se demasiado demorados.

A investigação do cibercrime não assenta somente em elementos técnicos e informáticos, mas estes são o cerne da questão por diversos fatores. Enquanto que num crime de cenário é possível a recolha de elementos que nos levam quase indubitavelmente ao que ali sucedeu e, eventualmente, de quem foram os seus agentes – veja-se a título de exemplo um crime de homicídio ou de roubo. Nos crimes informáticos é, na maioria das vezes, difícil percecionarmos quais as provas que necessitamos recolher em função do tipo de crime em investigação. O avanço tecnológico traz consigo a mudança de paradigma de *modus operandi*, apanhando desprevenidos não só os investigadores, mas essencialmente as vítimas.

Acompanhamos as palavras de JOSÉ BRAZ quando nos diz que "*a investigação criminal se desenvolve, basicamente, em duas estratégias (...) num quadro de permanente interatividade e integração (...) – o conjunto de procedimentos tendentes à obtenção da prova pessoal (interrogação) e, - o conjunto de procedimentos tendentes à obtenção da prova material (instrumentação)*"[3].

Se a investigação criminal na área do cibercrime necessita de evoluir, por força das novas tecnologias, a lei terá que acompanhar este progresso, dando mais ferramentas aos investigadores e aos julgadores para que a justiça seja feita.

3 JOSÉ BRAZ, *Investigação Criminal, a organização, o método e a prova, Os desafios da nova criminalidade*, Almedina, 2009, p. 20.

2. A ATUAL LEI DO CIBERCRIME

A atual lei do cibercrime teve a sua génese na transposição para a ordem jurídica interna da Decisão Quadro n.º 2005/222/JAI[4], do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa[5]. Nesta Decisão Quadro ficou estabelecido que os Estados-Membros deveriam tomar as medidas necessárias para dar cumprimento às suas disposições até 16 de Março de 2007. Ora, volvidos mais de dois anos a Decisão Quadro foi finalmente transposta para o nosso ordenamento jurídico. Por outro lado, com a ratificação da Convenção de Budapeste, criaram-se novos tipos legais de crime, usando a terminologia ali adotada.

A lei do cibercrime comporta diversos tipos legais de crime. Nela se encontram os crimes de falsidade informática (art. 3.º), dano relativo a programas ou outros dados informáticos (art. 4.º), sabotagem informática (art. 5.º), acesso ilegítimo (art. 6.º), interceção ilegítima (art. 7.º) e reprodução ilegítima de programa protegido (art. 8.º).

A inovação da lei do cibercrime verifica-se, para além dos tipos legais de crime, pela possibilidade da admissão de recolha de elementos de prova que não se encontravam previstos no código de processo penal. Admissibilidade esta que vai mais além da existente e se aplica, nos termos do art. 11.º, a todos os tipos de crime, não só a esta lei, mas a todos os ilícitos penais que sejam cometidos por via informática ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

Criou-se, deste modo, a possibilidade de efetuar a preservação e a revelação expedita de dados (art. 12.º e 13.º, respetivamente), injunção para apresentação ou concessão do acesso a dados (14.º), pesquisa e apreensão de dados informáticos (art. 15.º e 16.º, respetivamente), apreensão de correio eletrónico e registo de comunicações de natureza semelhante (art. 17.º), interceção de comunicações (art. 18.º) e ações encobertas (art. 19.º).

Destarte, também saiu reforçada a cooperação internacional com o principal mecanismo previsto na Convenção de Budapeste, isto é, a criação de um ponto de contacto permanente[6]. Este *focal point* tem em vista a assistência imediata para que as autoridades nacionais competentes cooperem com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, bem como para efeitos de recolha de prova, em suporte eletrónico.

---

4 Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32005F0222 [acedido em 23 de junho de 2019]. Esta Decisão Quadro foi substituída pela Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação.

5 Também designada por Convenção de Budapeste, por ter sido assinada naquela cidade em 23 de novembro de 2001.

6 Também conhecido por 24/7. Este ponto de contacto ficou sob a égide da Polícia Judiciária, por ser o Órgão de Polícia Criminal com competência, nos termos da LOIC, para a investigação dos crimes informáticos.

Se atentarmos nas normas europeias verificamos que a diretiva que deu origem à nossa lei do cibercrime foi substituída pela Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, foi publicada no Jornal Oficial da União Europeia em 12 de agosto de 2013.

O imperativo de transposição, para o ordenamento jurídico interno, surge na Diretiva 2013/40/UE que expressamente refere no seu art. 16.º, n.º 1, que "*os Estados-Membros põem em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva até 4 de setembro de 2015*." Efetivamente, como já mencionamos anteriormente, há muito que foi ultrapassado o prazo para a transposição, não se compreendendo este lapso temporal para tal. Como é referido no Relatório do Ministério dos Negócios Estrangeiros – "Portugal na União Europeia Ano 2013" "*[Q]uanto à diretiva relativa aos ataques contra os sistemas de informação, a sua transposição também não deverá exigir grande esforço legislativo, atendendo à disciplina já contida na Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime)*[7]."

Esta Diretiva tem como objeto aproximar as infrações penais no domínio de ataques contra sistemas de informação dos Estados-Membros e estabelecer regras mínimas relativas às sanções aplicáveis e respetivas infrações. Visa também, segundo o seu art. 1.º, a introdução de disposições comuns para prevenir tais ataques e melhorar a cooperação entre as autoridades judiciais e outras autoridades competentes europeias neste domínio[8].

Centrando-nos na atual lei do cibercrime, verificou-se que a sua interpretação, quando entrou em vigor e durante os primeiros anos, não foi fácil de efetuar. Desde logo a confusão operada por dados de base, dados de tráfego, dados de conteúdo, etc. Que autoridade judiciária poderia efetuar, por exemplo, junto das operadoras de comunicações determinado pedido? O Ministério Público ou obrigatoriamente o Juiz de Instrução Criminal? Tal celeuma deu origem a acórdãos dos tribunais superiores em sentido diverso, bem como a interpretações doutrinais diferentes[9].

Outros problemas surgiram por via da interpretação doutrinária. O art. 11.º, n.º 2 refere que "as disposições processuais previstas no presente capítulo não prejudicam o regime da Lei n.º 32/2008, de 17 de julho". Gerou-se a dúvida se a Lei de Retenção de dados se aplicava a todos os tipos legais existentes na Lei do Cibercrime ou apenas aos crimes graves[10].

---

7 Disponível em http://app.parlamento.pt [acedido em 12 de julho de 2019]. Relatório não datado mas pela sua leitura e análise que faz do ano de 2013 é de prever que tenha sido elaborado no decurso de 2014.

8 Para um estudo mais aprofundado sobre esta Diretiva, remetemos para o nosso artigo "A novíssima Diretiva relativa ao cibercrime", In SOUSA, CONSTANÇA URBANO DE (Coord.), *O Espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, EDIUAL, Lisboa, maio de 2014, pp. 176 a 192.

9 DUARTE RODRIGUES NUNES, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal, 2018, pp. 32 e ss; PEDRO VERDELHO, "Cibercrime", in *Dicionário da Sociedade de Informação*, IV, p. 376, e também em "A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa", in *Direito da Sociedade da Informação*, VI, pp. 270-271; DAVID SILVA RAMALHO, "A investigação criminal na Dark Web", in *Revista da Concorrência e Regulação*, n.º 14/15, pp. 398-399.

10 Definindo esta lei, art. 2.º, n.º 1, alínea g), que por crime grave se entende os crimes de terrorismo, criminalidade violenta, criminalidade altamente organizada, sequestro, rapto e tomada de reféns, crimes contra a

Efetivamente esta amálgama de legislação confusa, deixando ao intérprete uma ampla margem de defesa das suas posições aquando da interpretação da norma jurídica, leva o a que a certeza do Direito, *maximus*, princípio da certeza jurídica, ínsito no art. 2.º da Constituição da República, deixe de o ser tão certo. Contudo, temos constatado a falta de invocação, em sede própria, da validade da Lei n.º 32/2008[11]. É certo que se trata de uma lei gerada no seio da Assembleia da República e que cumpre todos os requisitos de aplicabilidade interna, mas tratando-se da transposição de uma Diretiva europeia, como mencionamos supra, que recentemente foi considerada inválida pelo Tribunal de Justiça da União Europeia, manterá esta validade sem mácula[12]? Poderá existir algum recurso que afaste a sua aplicabilidade legal?

Acresce, sendo de extrema importância, que a salvaguarda de dados de tráfego é condição *si ne quo non* para a identificação dos presumíveis autores de qualquer ilícito informático ou praticado através de meios informáticos. Manter-se-á válida a definição legislativa de "dados de tráfego" inserida na Lei do cibercrime ou estará a mesma desadequada face à realidade tecnológica?

Analisaremos de seguida o acórdão do TJUE uma vez que sem dados informáticos a investigação criminal, a nível do cibercrime, não poderá atingir os seus objetivos e consequentemente lograr-se uma profícua investigação, ou seja, a identificação dos autores da prática dos crimes.

---

identidade cultural e integridade pessoal, contra a segurança do Estado, falsificação de moeda ou títulos equiparados a moeda e crimes abrangidos por convenção sobre segurança da navegação aérea ou marítima.

11 A Provedora de Justiça, em 29/01/2019, endereçou uma recomendação à Ministra da Justiça no sentido de alterar a Lei n.º 32/2008, de 17 de julho, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações. Vide https://www.provedor-jus.pt/?idc=35&idi=17775 [*acedido em 27 de agosto de 2019*]. Mais recentemente, a 27 de agosto de 2019 a Provedora de Justiça solicitou ao Tribunal Constitucional a fiscalização abstrata da constitucionalidade dos art.s 4.º, 6.º e 9.º, da Lei n.º 32/2008.

12 No sentido do que acabamos de referir veja-se Ac. TRL, Proc. 8617/17.8T9LSB-A.L1-3, de 28-11-2018, Relator: Conceição Gonçalves, in www.dgsi.pt [acedido a 26 de agosto de 2019].

3. ANÁLISE DO ACÓRDÃO DO TRIBUNAL DE JUSTIÇA, DE 8 DE ABRIL DE 2014.

O Tribunal de Justiça da União Europeia (TJUE) foi chamado a pronunciar-se, em 12 de junho de 2012, em virtude do *High Court of Ireland* ter suscitado uma questão prejudicial sobre a validade da Diretiva 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março, em face dos Tratados (Processo C-293/12). Da mesma forma, em 19 de dezembro de 2012 e com uma argumentação algo distinta, o *Verfassungsgerichtshof* (Áustria) suscitou também, junto do TJUE, uma questão prejudicial sobre a validade da Diretiva 2006/24/CE em face dos Tratados (Processo C-594/12). Este processo por ser semelhante ao pedido da Irlanda ficou apenso ao mesmo.

O pedido apresentado pela High Court é relativo a um litígio que opõe a Digital Rights Ireland Ltd. (a seguir «Digital Rights») ao Minister for Communications, Marine and Natural Resources, ao Minister for Justice, Equality and Law Reform, ao Commissioner of the Garda Síochána, à Irlanda e ao Attorney General acerca da legalidade de medidas legislativas e administrativas nacionais respeitantes à conservação de dados relativos a comunicações eletrónicas. Ou seja, tratava-se de determinar se uma vigilância em massa é compatível com a salvaguarda dos Direitos Fundamentais, tal como constam da Carta e da Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais.

Concretamente:

1) A Diretiva 2006/24/CE é compatível com o direito dos cidadãos de circularem e permanecerem livremente no território dos Estados-Membros, consagrado no artigo 21.° TFUE?;

2) A Diretiva 2006/24/CE é compatível com o direito ao respeito pela vida privada, consagrado no artigo 7.° da Carta [dos Direitos Fundamentais da União Europeia (a seguir 'Carta')] e no artigo 8.° da [CEDH]? [13];

---

13 CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA (2010/C 83/02), publicada no Jornal Oficial da União Europeia, em 30/03/2010, estabelecendo:
Artigo 7.º-**Respeito pela vida privada e familiar:**
Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.
Artigo 8.º - **Proteção de dados pessoais:**
1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.
Artigo 11.º -**Liberdade de expressão e de informação:**
1. Qualquer pessoa tem direito à liberdade de expressão. Este direito compreende a liberdade de opinião e a liberdade de receber e de transmitir informações ou ideias, sem que possa haver ingerência de quaisquer poderes públicos e sem consideração de fronteiras.
2. São respeitados a liberdade e o pluralismo dos meios de comunicação social.

3) A Diretiva 2006/24/CE é compatível com o direito à proteção dos dados pessoais, consagrado no artigo 8.° da Carta?;

4) A Diretiva 2006/24/CE é compatível com o direito à liberdade de expressão, consagrado no artigo 11.° da Carta e no artigo 10.° da CEDH?;

5) A Diretiva 2006/24/CE é compatível com o direito a uma boa administração, consagrado no artigo 41.° da Carta?;

6) Em que medida os Tratados e, em concreto, o princípio da cooperação leal previsto no artigo 4.°, n.° 3, TUE, exigem que os tribunais investiguem e apreciem a compatibilidade das medidas nacionais de transposição da Diretiva 2006/24/CE com as garantias conferidas pela Carta, incluindo o seu artigo 7.° (cujo conteúdo é inspirado no artigo 8.° da CEDH)?

O pedido apresentado pelo *Verfassungsgerichtshof* é relativo a recursos em matéria constitucional interpostos perante este órgão jurisdicional respetivamente pelo Kärntner Landesregierung (Governo do Land de Caríntia), bem como por M. Seitlinger, C. Tschohl e 11 128 outros recorrentes, acerca da compatibilidade da lei que transpõe a Diretiva 2006/24 para o direito interno austríaco com a lei constitucional federal (*Bundes-Verfassungsgesetz*). Essencialmente, trata-se de determinar se os art.ºs 3.º a 9.º da Diretiva são compatíveis com os art.ºs 7.º, 8.º e 11.º[14] da Carta dos Direitos Fundamentais da EU, assim como, qual a relevância, *in casu*, *"[…] do Princípio da salvaguarda de um nível de proteção mais elevado, consagrado no artigo 53.º da Carta?"*; e, ainda, se *"[…] é possível deduzir da jurisprudência do Tribunal Europeu dos Direitos Humanos em relação ao artigo 8.º da CEDH a existência de elementos de interpretação do artigo 8.º da Carta que possam influenciar a interpretação deste último artigo?"*

Numa sociedade cada vez mais informatizada coloca-se em causa a proteção de dados pessoais, a liberdade de cada indivíduo e o respeito pela sua privacidade.

A decisão tomada pela Grande Secção do TJUE vem debruçar-se sobre este assunto e em particular à Diretiva 2006/24, que deu origem à nossa Lei n.º 32/2008. Neste aspeto referem os doutos magistrados daquela instância europeia que "*limitando-se a dispor que cada Estado-Membro define os procedimentos que devem ser seguidos e as condições que devem ser respeitadas para se ter acesso a dados conservados de acordo com os requisitos da necessidade e da proporcionalidade. Em particular, a Diretiva 2006/24 não estabelece um critério objetivo que permita limitar o número de pessoas com autorização de acesso e de utilização posterior dos dados conservados ao estritamente necessário à luz do objetivo prosseguido. O acesso aos dados conservados pelas autoridades nacionais competentes não está sobretudo sujeito a um controlo prévio efetuado por um órgão jurisdicional ou por uma entidade administrativa independente cuja decisão vise limitar o acesso aos dados e a utilização dos mesmos ao estritamente necessário para alcançar o objetivo prosseguido e*

14 A UE não só está vinculada pela sua Carta dos Direitos Fundamentais, mas também pela CEDH e pelas tradições constitucionais comuns aos Estados membros (Art.º 6.º do TUE).

ocorra na sequência de um pedido fundamentado destas autoridades apresentado no âmbito de procedimentos de prevenção, deteção ou ação penal. Também não foi prevista uma obrigação precisa de os Estados-Membros estabelecerem tais limitações."

Destarte tal não configurar uma obrigação dos Estados-Membros previsto na Diretiva, certo é que em Portugal o art. 8.º da Lei n.º 32/2008 estipula que a Comissão Nacional de Proteção de Dados (CNPD) deve manter um registo eletrónico permanentemente atualizado das pessoas especialmente autorizadas a aceder aos dados, nos termos da alínea d) do n.º 1 do artigo anterior. Desconhece-se até que ponto tal obrigação, por parte dos operadores nacionais, está a ser cumprida e devidamente fiscalizada pela CNPD. A este respeito recordamos que o art. 10.º da Lei n.º 32/2008 estabelece que a transmissão dos dados referentes às categorias previstas no artigo 4.º processa-se mediante comunicação eletrónica, nos termos das condições técnicas e de segurança previstas no n.º 3 do artigo 7.º. Esta transmissão veio posteriormente a ser regulamentada através da Portaria n.º 469/2009, de 6 de maio[15], que estabelece as regras sobre a transmissão de dados de forma eletrónica entre magistrados e os ISP's. Na prática tal sistema não se encontra em funcionamento[16] e levou inclusive a que a Procuradoria Geral da República firmasse um acordo com as operadoras que prestam serviços de Internet (ISP)[17]. Pelo que será de duvidar da eficácia deste artigo e nesse sentido damos razão aos magistrados do TJUE quando afirmam neste acórdão que "*a Diretiva 2006/24 não estabelece regras claras e precisas que regulem o alcance da ingerência nos direitos fundamentais consagrados nos artigos 7.° e 8.° da Carta. Impõe-se pois concluir que esta diretiva comporta uma ingerência*

15 Estabelece os termos das condições técnicas e de segurança em que se processa a comunicação eletrónica para efeitos da transmissão de dados de tráfego e de localização relativos a pessoas singulares e a pessoas colectivas, bem como dos dados conexos necessários para identificar o assinante ou o utilizador registado, nos termos previstos na Lei n.º 32/2008, de 17 de julho.

16 Esta Portaria estabelece, no n.º 1, do Art. 2.º, que o juiz que tenha ordenado ou autorizado a transmissão de dados nos termos previstos no artigo 9.º da Lei n.º 32/2008, de 17 de Julho, comunica a decisão através da aplicação informática denominada '**sistema de acesso ou pedido de dados às operadoras de comunicações**' **(SAPDOC)** especificamente disponibilizada para o efeito (*negrito nosso*).

17 Este protocolo foi assinado em 9 de julho de 2012 e estabeleceu um formulário tipo para o pedido de identificação de um titular de um IP, encontra-se acessível no *site* da PGR em http://www.pgr.pt/Protocolos/PROTOCOLO-comunicacoes.pdf. Posteriormente a PGR, através da Circular 12/2012, de 25/09/2012 esclarece os magistrados do Ministério Público que foi criado no SIMP (Sistema de Informação do Ministério Público) uma plataforma eletrónica para solicitar os pedidos às operadoras. Acrescenta-se, por isso, que enquanto não se mostrar possível a utilização da nova plataforma eletrónica do SIMP, os formulários serão impressos em papel e remetidos pelas vias habituais. Procedimento este que ainda hoje em dia é utilizado pelo Ministério Público para solicitar dados às operadoras de comunicações. Referida circular encontra-se disponível ao público no *site* da PGR, no endereço http://www.pgr.pt/Circulares/textos/2012/circular_12-2012.pdf [*acessos efetuados em 20 de agosto de 2019*].
Uma nótula relativa a este Protocolo que, em nossa modesta opinião, inverte os papéis da Justiça em Portugal, ao permitir que sejam os operadores, que acabam por ter acesso a informações que não necessitam, a decidir que dados fornecem ou não às autoridades judiciárias. O Ministério Público ou o JIC não deveriam informar os ISP's ao abrigo de que legislação requerem os dados de identificação de determinado cliente, num grupo data/hora e fuso horário. As interpretações da lei são da competência dos Tribunais e não de juristas de empresas de comunicações, cabendo aos Tribunais a aplicação da Lei, no estrito dever de legalidade, necessidade e proporcionalidade. Caso dúvidas subsistam, seja pela defesa, seja pelo MP, existem, para o efeito, os Tribunais de recurso. Discordamos totalmente da forma como foi construído este formulário bem como o objetivo final do protocolo: a cedência de informação por parte dos operadores que a Lei determina que seja fornecida obrigatoriamente no âmbito de um inquérito crime, cominando a desobediência com obstrução á justiça e a não salvaguarda de dados de tráfego com a aplicação de uma contraordenação.

nestes direitos fundamentais de grande amplitude e particular gravidade na ordem jurídica da União, sem que essa ingerência seja enquadrada com precisão por disposições que permitam garantir que a mesma se limita efetivamente ao estritamente necessário" e "*a Diretiva 2006/24 não estabelece regras específicas e adaptadas à grande quantidade de dados cuja conservação é imposta por esta diretiva, ao caráter sensível destes dados e ao risco de acesso ilícito aos mesmos, regras que se destinariam designadamente a regular de maneira clara e estrita a proteção e a segurança dos dados em causa, a fim de garantir a sua plena integridade e confidencialidade.*"

Mas o cerne da questão aflorado no arresto em análise refere-se que a Diretiva não impõe, quanto aos dados salvaguardados, que os mesmos sejam conservados no território da União, inviabilizando, deste modo, qualquer fiscalização, por entidade independente, expressamente exigida na Carta, pelo art. 8.º, n.º 3, do cumprimento das exigências de proteção e de segurança.

Face a todos os argumentos esgrimidos concluíram que "*há que considerar que, ao adotar a Diretiva 2006/24, o legislador da União excedeu os limites impostos pelo respeito do princípio da proporcionalidade à luz dos artigos 7.°, 8.° e 52.°, n.° 1, da Carta*". E declararam que "***[A] Diretiva 2006/24/CE do Parlamento Europeu e do Conselho, de 15 de março de 2006, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, e que altera a Diretiva 2002/58/CE, é inválida.***"

Por força da declaração de invalidade da Diretiva que originou a Lei n.º 32/2008 esta mantém-se em vigor mas poderá ser alvo de fiscalização da constitucionalidade em face do Primado do Direito da UE sobre os direitos nacionais.[18] Efetivamente a decisão do TJUE que considera inválido um ato de Direito secundário (neste caso a Diretiva de retenção de dados) porque viola o Direito primário tem um efeito *erga omnes*, traduzindo-se em consequências para todos: para todos os tribunais e demais aplicadores do direito que não podem mais aplicar um ato que viola direito superior; para o legislador que fica obrigado a eliminá-lo da ordem jurídica.[19] Donde, a decisão do TJUE constitui fundamento suficiente para que os tribunais

18 Tal já sucedeu em diversos países da UE, tendo as leis de transposição desta Diretiva sido consideradas inconstitucionais. Nomeadamente: Tribunal Constitucional da Roménia (Decisão n.º 1258, de 8 de outubro de 2009); Tribunal Constitucional da Alemanha (Sentença n.º 10/2010, de 2 de março); Tribunal Constitucional da República Checa (Sentença Pl. ÚS 24/10, de 31 de março de 2011).

19 Tende aqui a aceitar-se a primazia do direito da UE originário e derivado sobre o direito constitucional nacional, embora não deixe de se chamar a atenção para o facto de que se trata de um fenómeno material e funcionalmente limitado. (...) Na verdade, nas Declarações Relativas a Disposições dos Tratados, aprovadas quando da entrada em vigor do Tratado de Lisboa, encontra-se a Declaração 17, sobre o primado do direito comunitário, em que se lembra expressamente que, em conformidade com a jurisprudência do TJUE, os Tratados e o direito adotado pela União com base nos Tratados primam sobre o direito dos Estados membros, nas condições estabelecidas pela referida jurisprudência, tendo juntado inclusivamente um Parecer do Serviço Jurídico do Conselho afirmando que se trata aí de salvaguardar um princípio do direito comunitário. *Loc. cit.* pp. 67 a 69 *in* JÓNATAS E. M. MACHADO, *Direito da União Europeia*, 2.ª Edição, Coimbra Editora, 2012. Neste sentido, também, MARIA ROSA OLIVEIRA TCHING, "Juiz Natural – Um juiz cada vez mais europeu", *Revista Julgar*, n.º 14, Coimbra Editora, 2011, pp. 135-155.

nacionais dos Estados membros se abstenham de aplicar o ato considerado nulo e de reenviar a questão da respetiva validade para o TJUE.[20]

Sem este precioso e indispensável instrumento de identificação a prova digital fica seriamente comprometida e por mais que exista legislação, os crimes cometidos através da Internet deixarão de ser imputados a um determinado autor, por falta de elementos que conduzam até este e, consequentemente, ficará incólume à ação da justiça.[21]

20 *Loc. cit.* JÓNATAS MACHADO, *Ob. Cit.*. pp. 647-648

21 A este respeito remetemos para a nossa monografia *A Prova Digital em Processo Penal: o correio eletrónico*, Chiado Editora, 2.ª Edição, 2017, em especial para as páginas 93 a 99.

4. A CONEXÃO ENTRE A LEGISLAÇÃO ATUAL E A INVESTIGAÇÃO DA CIBERCRIMINALIDADE

Do que temos vindo a discorrer não restam dúvidas que a investigação criminal sai fragilizada face às normas legais que possuímos. Efetivamente a obtenção de prova é fulcral para que num processo-crime se possa imputar a responsabilidade penal ao agente. Caso contrário a prova sucumbe, por ter sido ilícita ou obtida tardiamente, e o arguido não ser condenado, por inexistência de provas.

Dos diversos problemas já enumerados iremos aflorar dois, para os quais ainda não dedicamos a atenção devida e por serem fulcrais na investigação da cibercriminalidade.

Primus, a equiparação da apreensão do correio eletrónico ao regime da correspondência do Código de Processo Penal. É sabido que nos dias que correm o uso regular do correio eletrónico é uma banalização. Eventualmente já o era há 10 anos, aquando da criação da lei do cibercrime, mas atualmente, e com a facilidade com que se pode efetuar um registo de correio eletrónico, é um dos problemas que afetam a investigação criminal a referida equiparação. Já o defendemos no passado[22] e continuamos a advogar que esta equiparação é inimiga de uma célere investigação. Proceder formalmente à equiparação do regime da correspondência, levando ao conhecimento do JIC os *e-mail's* apreendidos para que seja o primeiro a tomar conhecimento, leva a o JIC não leia todos os *e-mail* e não determine quais os que são de interesse para juntar aos autos. Antes leva o juiz a efetuar um despacho genérico delegando na Polícia a faculdade de ver os *e-mail's* e posterior junção dos que tenham interesse com a investigação. O espírito do legislador aquando da criação da norma do art. 179.º do CPP foi a da proteção da reserva da vida privada e familiar em observância da norma constitucional do art. 26.º, n.º 1 da CRP. Procedendo como se tem vindo a assistir, ou seja o JIC tomar conhecimento dos *e-mail*, mas não visualizando o seu conteúdo e delegando no OPC a faculdade de em primeira instância ver e juntar aos autos as mensagens de correio eletrónico, não só está a ser violado o regime processual penal como se está a permitir a divulgação de e-mail's com conteúdo da vida íntima dos visados por outras pessoas. PAULO PINTO DE ALBUQUERQUE afirma categoricamente que "*a omissão do exame da correspondência pelo juiz constitui uma nulidade do art. 120.º, n.º 2, alínea d), porque se trata de um acto processual legalmente obrigatório*"[23].

Concordamos com Rui Cardoso quando afirma que "*o legislador deveria então ter criado um regime autónomo e auto-suficiente, com repartição equilibrada de competências entre o Ministério Público e o juiz de instrução, a este reservando o estritamente necessário à*

22 ARMANDO DIAS RAMOS, *A prova digital em processo penal: o correio eletrónico*, 2.ª Edição, Chiado Editora, 2017.

23 In comentário ao art. 179, nota 12, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção dos Direitos do Homem*, 2.ª Edição, Universidade Católica Editora, 2008, p. 495.

garantia de direitos dos visados, adequado às especificidades técnicas das comunicações eletrónicas, muito diferentes da correspondência corpórea"[24].

Em nosso modesto entendimento o Ministério Público deveria delegar no investigador a faculdade de visualizar o conteúdo e selecionar os *e-mail's* de interesse, sendo este o único a visualizar o conteúdo dos mesmos e submetendo ao seu escrutínio a junção dos relevantes ao processo. Posteriormente, tal como sucede no regime das interceções telefónicas, o MP remeteria ao JIC para validação formal.

Secundus, o uso das ações encobertas na investigação da cibercriminalidade. O legislador previu, no n.º 2 do art. 19.º da Lei do Cibercrime, o recurso a meios e dispositivos informáticos, nas ações encobertas, observando-se a utilização das regras previstas no CPP relativas à interceção das comunicações. Analisando as regras do CPP que dizem respeito às escutas telefónicas, ínsitas nos artigos 187.º a 189.º, verificamos que não obtemos respostas a certas perguntas, as quais fazem parte do nosso problema. Desde logo porque a função do agente encoberto não se reconduz a uma mera interceção. Como bem já referimos noutras instâncias[25], intercetar significar intrometer de permeio, ou seja, entre o emissor e o recetor alguém consegue captar todo o conteúdo das comunicações eletrónicas. Ora, salvo melhor opinião em contrário, não nos encontramos perante a figura do agente encoberto. Define a Lei das Ações Encobertas, no n.º 2, do art. 1.º, que se consideram ações encobertas aquelas que sejam desenvolvidas por funcionários de investigação criminal ou por terceiros, atuando sob controlo da Polícia Judiciária, para prevenção ou repressão dos crimes (...), com ocultação da sua qualidade e identidade (negrito nosso). É certo que quando se efetua uma interceção telefónica, regime previsto no CPP, para onde somos levados obrigatoriamente pelo legislador na Lei do Cibercrime, não existe qualquer ocultação da qualidade do agente ou da sua identidade, apenas se trata de um procedimento técnico em que se consegue "escutar" a comunicação, seja ela telefónica ou de dados informáticos. Subjazem, pois, muitas dúvidas como se poderá efetivamente aplicar o art. 19.º da Lei do Cibercrime às regras enunciadas no CPP. Recorrendo a DÁ MESQUITA "*consagra-se uma norma espúria no ordenamento jurídico português ao prever, sem qualquer outro enquadramento, o "recurso a meios e dispositivos informáticos" em ações encobertas*"[26].

Os problemas, para além destes que já enunciamos, são mais diversos e complexos, os quais a legislação não dá resposta, por nos encontrarmos num estado avançado da tecnologia e do direito continuar estagnado. O legislador continua ainda a olhar para a criminalidade informática, que pode ser muito grave, inclusive com atos terroristas, com olhos de equiparação entre duas realidades que são bem distintas.

---

24 RUI CARDOSO, "Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei 109/2009, de 15.IX", In *Revista do Ministério Público*, n.º 153.º, Janeiro-Março de 2018, Almedina, p. 178.

25 Ver nosso *A prova digital em processo penal...*, p. 52.

26 PAULO DÁ MESQUITA, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010, p. 127.

Um dos problemas que desde já se coloca é se será lícito a um investigador ou terceiro, na qualidade de agente infiltrado, enviar *benware*[27], sob a forma de disfarce de atualização de um *software* ou por intermédio de qualquer outro subterfúgio, para poder aceder a todo o conteúdo do disco rígido do computador do suspeito? Constata-se que efetivamente numa ação encoberta relativa a tráfico de estupefacientes, por exemplo, o agente que se infiltra numa determinada zona e convive com os suspeitos detém uma perceção visual do espaço que o rodeia. Poderá assim confirmar a existência de balanças de precisão, de panfletos prontos a serem utilizados, etc., ou de outros elementos tidos por pertinentes para os fins da investigação em curso. E estes elementos, ainda que o agente não visualize diretamente o produto estupefaciente, são tidos em linha de conta para a investigação e poderão concatenar as provas de modo a que existam fundadas suspeitas ou indícios suficientes dos crimes que ali se praticam. E quem se refere a crimes de narcotráfico também se reconduz a crimes de terrorismo, com a perceção de elementos que possam originar um ataque em massa ou de grandes proporções. A nível informático tal situação não é assim tão linear. Quanto muito o suspeito, após ter ganho a confiança do seu interlocutor, poderá permitir apenas o acesso a uma pasta partilhada do seu computador ou servidor, ficando o agente maniatado de obter outros elementos que poderão conduzir a provas irrefutáveis da prática de crimes cibernéticos tais como de (ciber)terrorismo ou de financiamento dos mesmos, entre outros.

Assim, coloca-se novo problema, será lícito a um agente infiltrado criar artefactos virtuais, sem entrar na esfera da provocação, de forma a "atrair" e identificar criminosos? A este respeito não poderemos esquecer a criação da menina virtual, apelidada de *Sweetie*, de origem filipina e com 10 anos de idade, pela ONG holandesa *Terre des Hommes*[28], onde foram identificados em 2013, durante 10 semanas em que colocaram a imagem virtual da menina em salas de conversação (denominados *chats*) de pornografia infantil, mais de 1.000 homens interessados em ter sexo com menores de 16 anos. Onde efetivamente termina a ação encoberta e começa a ação provocadora no ciberespaço?

Será lícito criar perfis falsos nas redes sociais, sem conhecimento das autoridades judiciárias e consequentemente à margem do regime de agente infiltrado, para obter mais informações do suspeito, incluindo-se aqui a interação virtual com os suspeitos?

O mesmo se reconduz aos crimes de terrorismo, sejam estes praticados de forma tradicional, sejam praticados através da Internet. O agente encoberto poderá com a utilização de técnicas informáticas entrar na esfera privada do suspeito e obter informações que não conseguiria de outro modo?

---

27 Por opisição a *Malware* , i.é, nome abreviado para "software malicioso". *Malware* é qualquer tipo de software indesejado, instalado sem o seu devido consentimento. Vírus, *worms* e *cavalos de tróia* são exemplos de *software* mal-intencionado que com frequência são agrupados e chamados, coletivamente, de *malware*. In http://www.microsoft.com/pt-br/security/resources/malware-whatis.aspx [*acedido em 5 de julho de 2019*].
28 http://www.terredeshommes.nl/languages/en [*acedido em 5 de julho de 2019*].

Não almejamos responder a todas estas perguntas, face à complexidade que as mesmas abarcam e por nos conduzirem a outro campo de outra importância, que se relaciona com Direitos, Liberdades e Garantias dos cidadãos.

É na Constituição da República que encontramos o expoente máximo da garantia dos cidadãos no que aos seus Direitos e Liberdades dizem respeito, podendo existir uma contração destes em situações previstas na Lei e sempre em obediência aos princípios da necessidade, subsidiariedade e proporcionalidade (art. 18.º CRP).

As ações intrusivas, na vida pessoal e familiar, provocadas pela figura do agente encoberto digital, ao conseguir aceder aos conteúdos do computador do visado, a conseguir localizar de forma imediata a sua localização, através do sistema GPS, revelam-se menores face aos atos que poderão a vir ser cometidos, salvaguardando-se, através da prevenção, a vida de muitas pessoas, entre outros bens jurídicos.

Urge mudar este paradigma para que, dentro da legalidade, seja possível realizar investigações criminais que salvaguardem os direitos e as liberdades dos suspeitos. Por outro lado, muitas das investigações ficam inquinadas porque adotado o regime das interceções das comunicações a dados encriptados os investigadores não lograram obter quaisquer informações por força da codificação destas.

5. EM JEITO DE CONCLUSÃO

Do decurso do tempo, nestes 10 anos, de aplicação da lei do cibercrime verifica-se um fosso abismal entre a legislação em vigor e a tecnologia existente.

Como discorremos as tecnologias informáticas estão evoluídas e surgem novos ilícitos criminais que não poderão ser investigados por falta de norma legal. A título de exemplo a criação de perfis falsos nas redes sociais, usando fotografias e criando a ilusão que se trata de uma pessoa conhecida de terceiros, com intuitos ilícitos. De igual modo a criação de endereços de correio eletrónico[29] usurpando a identidade de terceiros é outro dos problemas que urge tipificar. Se é certo que o art. 3.º da lei do cibercrime poderá acolher esta situação, quando utilizados para finalidades juridicamente relevantes tal não sucede quanto à criação do próprio endereço de *e-mail* pois não se está, com intenção, a introduzir, modificar, apagar ou suprimir dados informáticos, nem a interferir num tratamento de dados informáticos. De igual modo não se produzem dados ou documentos não genuínos.

A lei do cibercrime necessita de uma adaptação a esta realidade mormente no âmbito da recolha de prova. O uso corriqueiro do correio eletrónico e a implementação de sistemas encriptados conduz-nos a outra era dos crimes informáticos.

Urge adaptar ao direito interno a Diretiva 2013/40/UE, pois a mesma encerra medidas de investigação mais célere com as congéneres europeias, nomeadamente:

1.º - Aproximando o direito penal dos Estados-Membros no domínio dos ataques contra os sistemas de informação, estabelecendo um conjunto de regras mínimas relativamente às infrações penais e às suas sanções;

2.º - A utilização de *botnets*[30] para fins criminosos, que coloca em causa sistemas de informações de infraestruturas críticas da União, comprometendo a realização de uma sociedade de informação mais segura e de um espaço de liberdade, segurança e justiça; e,

---

29 Se considerarmos os endereços dos servidores de webmail verifica-se a panóplia de possibilidade de criação de endereços de e-mail semelhantes.

30 Na própria exposição de motivos encontramos a definição de *botnet*. Assim, "*o termo «botnet» designa uma rede de computadores que foram infectados por software maligno (vírus informáticos). Esta rede de computadores «sequestrados» («zombies») pode ser ativada para executar ações específicas, como atacar sistemas de informação (ciberataques). Estes «zombies» podem ser controlados – frequentemente sem o conhecimento dos utilizadores dos computadores «sequestrados» – por outro computador, igualmente conhecido como «centro de comando e de controlo». As pessoas que controlam este centro fazem parte dos infractores, já que utilizam os computadores «sequestrados» para lançar ataques contra os sistemas de informação. É muito difícil localizar os autores da infracção, dado que os computadores que formam o «botnet» e realizam o ataque podem encontrar-se num local diferente daquele em que se encontra o infractor.*" Disponível *online* em http://new.eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX%3A32013L0040&qid=1377248567337 [*acedido em 14 de agosto de 2019*].

3.º - Aumenta a eficácia dos pontos de contato 24/7, responsáveis pela aplicação da lei nos Estados-Membros, com respostas urgentes a terem que ser obtidas no prazo de 8 horas.

Não será necessário aos órgãos de investigação o recurso a meios informais para obtenção de informação se se tivesse uma cooperação internacional mais eficaz. A nível interno a obtenção de elementos de prova poderia também ser mais célere se o titular da ação penal (Ministério Público) detivesse mais poder e apenas a intervenção do JIC fosse requerida aquando da hipotética violação de direitos fundamentais, no seu núcleo (ou o conteúdo) essenciais[31].

Só desta forma, a par de um reforço na justiça com a dotação de magistrados com mais conhecimentos informáticos e mais recursos humanos e técnicos nas polícias, se logrará a eficácia do combate ao cibercrime. Na verdade, assistimos a uma deslocação do mundo criminal para o mundo virtual, no qual os meliantes trocaram a insegurança pela segurança, a possibilidade de ser identificado com a certeza da quase anonimização, a punição pelo sentimento de impunidade.

31 GOMES CANOTILHO/VITAL MOREIRA, *Constituição da República Portuguesa Anotada*, I, 4.ª ed., Coimbra, 2007, p. 153

6.BIBLIOGRAFIA

ALBUQUERQUE, PAULO PINTO DE, *Comentário do Código de Processo Penal à luz da Constituição da República e da Convenção dos Direitos do Homem*, 2.ª Edição, Universidade Católica Editora, 2008.

BRAZ, JOSÉ, *Investigação Criminal, a organização, o método e a prova, Os desafios da nova criminalidade*, Almedina, 2009.

CANOTILHO, J. J. GOMES; MOREIRA, VITAL, *Constituição da República Portuguesa Anotada*, I, 4.ª ed., Coimbra, 2007.

CARDOSO, RUI, "Apreensão de correio electrónico e registos de comunicações de natureza semelhante – artigo 17.º da Lei 109/2009, de 15.IX", In *Revista do Ministério Público*, n.º 153.º, Janeiro-Março de 2018, Almedina.

MACHADO, JÓNATAS E. M., *Direito da União Europeia*, 2.ª Edição, Coimbra Editora, 2012

MESQUITA, PAULO DÁ, *Processo Penal, Prova e Sistema Judiciário*, Coimbra Editora, 2010.

NUNES, DUARTE RODRIGUES, *Os meios de obtenção de prova previstos na Lei do Cibercrime*, Gestlegal, 2018.

RAMALHO, DAVID SILVA, "A investigação criminal na Dark Web", in *Revista da Concorrência e Regulação*, n.º 14/15, Almedina, 2013.

RAMOS, ARMANDO DIAS, "A novíssima Diretiva relativa ao cibercrime", In SOUSA, CONSTANÇA URBANO DE (Coord.), *O Espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, EDIUAL, Lisboa, maio de 2014.

RAMOS, ARMANDO DIAS, *A prova digital em processo penal: o correio eletrónico*, 2.ª Edição, Chiado Editora, 2017.

TCHING, MARIA ROSA OLIVEIRA, "Juiz Natural – Um juiz cada vez mais europeu", *Revista Julgar*, n.º 14, Coimbra Editora, 2011

VERDELHO, PEDRO, "Cibercrime", in *Dicionário da Sociedade de Informação*, IV, Coimbra Editora, 2003.

VERDELHO, PEDRO, "A Convenção sobre o Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa", in *Direito da Sociedade da Informação*, VI, Coimbra Editora, 2006