Segurança e Defesa

COORDENAÇÃO

JOSÉ MANUEL ANES

ADÉLIO NEIVA DA CRUZ
ADRIANO MOREIRA
AGOSTINHO COSTA
ANTÓNIO FIGUEIREDO LOPES
ANTÓNIO SILVA RIBEIRO
ANTÓNIO VILAR
JOÃO PAULO FERNANDES
JORGE MANUEL DIAS SEQUEIRA
JOSÉ MANUEL SIMÕES
NELSON LOURENÇO
PEDRO LEDO

DIÁRIO DE BORDO

Coordenação
José Manuel Anes

Autores
Adélio Neiva da Cruz
Adriano Moreira
Agostinho Costa
António Figueiredo Lopes
António Silva Ribeiro
António Vilar
João Paulo Fernandes
Jorge Manuel Dias Sequeira
José Manuel Simões
Nelson Lourenço
Pedro Lêdo

Editor
Paulo Noguês

Design Gráfico e Paginação
TotalForce

Impressão
Procer, S.A.

1.ª Edição
Janeiro de 2020

ISBN: 978-989-54463-2-2

Depósito Legal: 467042/20

Diário de Bordo
Apartado 25
EC ERICEIRA
2659-909 ERICEIRA

O CIBERCRIME

O FENÓMENO
MEIOS DE OBTENÇÃO DE PROVA

PEDRO LÊDO
Licenciado em Direito
Pós Graduado em Cibercrime e Análise Digital Forense

Antes de mais conviria referir que o cibercrime tornou-se um crime emergente à escala mundial e com um desenvolvimento futuro sem precedentes.Temendo-se fortes ramificações para o Ciberterrorismo, aliás já é uma evidência, o que ainda agravará mais este crime emergente.

Em Portugal, são enviadas 30 milhões de mensagens de forma diária;

Cerca de 78% dos Internautas estão mal informados de como se protegerem do cibercrime;

No Mundo 400 milhões de pessoas são vítimas de cibercrime.

Convém pois ao legislador português rapidamente alterar o ´estado da coisa' e ´fundir´ rapidamente um conjunto de diplomas portugueses dispersos em Diário da República, e criar uma só lei que tenha como espectro

O presente texto não foi redigido ao abrigo do Novo Acordo Ortográfico.

também aquilo que se vai legislando nos estados membros europeus e no Mundo em geral (Convenções Mundiais e fundamentalmente Europeias). Não basta na minha opinião a Lei nº 109/91, de 17 de Agosto - Lei da Criminalidade Informática. É manifestamente insuficiente.

Elenco alguns dos principais cibercrimes (ou crimes digitais) e como numa primeira análise nos devemos proteger deles:

Cibercrime é o nome dados aos crimes cibernéticos que envolvam qualquer atividade ou prática ilícita na internet. Essas práticas podem envolver invasões de sistema, disseminação de vírus, roubo de dados pessoais, falsidade ideológica, acesso a informações confidenciais e tantos outros. O cibercrime compreende também os crimes convencionais realizados por meio de dispositivos eletrônicos ou que incluam a utilização de alguma ação digital como instrumento para a prática do crime.

O termo "cibercrime" (ou "cybercrime", em inglês) foi iniciado ou atribuído numa reunião do G-8 (grupo composto pelos sete países mais ricos do Mundo) próximo do final dos anos 90 onde estavam a ser abordadas as maneiras e os métodos utilizados para se combater as práticas ilícitas na internet.

Uma das fortes características do cibercrime é a predominância transnacional, o que dificulta as investigações e a apuração de provas contra os criminosos.

Outra característica também está na relação do aumento significativo do aumento de uso dos computadores pessoais, tablets e smartphones, que permitem que qualquer pessoa no mundo possa realizar práticas criminosas contra indivíduos de qualquer lugar do planeta sem necessidade de sair do seu domicílio.

A prática do cibercrime é tão comum que, segundo dados divulgados pela Norton, empresa especializada em segurança digital nomeadamente antivirus, cerca de 65% dos internautas já foram vítimas de cibercrime.

A maior dificuldade no combate a esses crimes é a falta de leis específicas e punições eficazes em diversos países na luta contra os hakers.

Abaixo discrimino alguns dos principais crimes cibernéticos:

- Ameaça: por escrito ou por imagem, ainda que em tom de brincadeira ou anônima.

- Difamação: acusar alguém de um ato à honra;

- Injúria: é ofender a dignidade de alguém;

- Calúnia: é acusar alguém publicamente de um crime;

- Discriminação: qualquer comentário ou imagem preconceituoso em relação a raça, cor, etnia, religião ou origem de uma pessoa;

- Falsidade ideológica (falsificar identidade): passar-se por outra pessoa para obter algum tipo de vantagem;

- Phising: roubo e utilização de dados sigilosos como passwords, dados bancários, documentos utilizando de artifícios digitais;

- Pirataria: é do que a reprodução não autorizada de algo protegido pelo direito com pertença de alguém.

- Pornografia Infantil: maliciosos utilizam a internet e dispositivos de acesso para criar e distribuir materiais com conteúdo pornográfico de crianças e menores de idade;

- Lavagem de dinheiro: tipo de crime é bastante comum. Os criminosos realizam transferências de dinheiro de maneira ilegal com o objetivo de esconder a sua fonte e também o seu destino;

CIBERTERRORISMO:

Todos estão familiarizados com o que "terrorismo" significa, mas quando colocamos a palavra "cyber" na frente, as coisas ficam delicadas e porque não dizer até nebulosas por muitos de nós, ainda.

Considerando que os efeitos do terrorismo do mundo real são óbvios e destrutivos, os do terrorismo cibernético são muitas vezes escondidos para aqueles que não são diretamente afetados.

Além disso, esses efeitos são mais propensos a causar danos do que destrutivos, embora isso nem sempre seja o caso.

Um dos primeiros exemplos de terrorismo cibernético foi um ataque em 1996 contra um ISP em Massachusetts, sendo que um hacker associado ao movimento de supremacia branca nos Estados Unidos invadiu o seu ISP, com base na mesma cidade, após impedi-lo de enviar uma mensagem racista mundial sob o seu nome. O indivíduo apagou alguns registos e desativou temporariamente os serviços do provedor, deixando a ameaça "Vocês não viram ainda o que é o terrorismo electrónico, garanto-vos que isto é apenas o princípio.

Embora este seja um exemplo claro de um incidente ciberterrorista realizado por um indivíduo mal-intencionado e politicamente motivado que causou tanto perturbações quanto danos, outros exemplos frequentemente listados encaixam-se menos claramente na categoria de "terrorismo".

Por exemplo, enquanto os ataques que removeram os call centers de serviços de emergência ou o controle de tráfego aéreo podem ser considerados terrorismo cibernético, a motivação dos indivíduos geralmente não é clara. Se uma pessoa causasse uma perturbação da vida real a esses sistemas, mas não tivesse outra motivação específica além do prejuízo, seriam classificados como terroristas?

Da mesma forma, os protestos cibernéticos, como os que ocorreram em 1999 durante o Kosovo contra a campanha de bombardeio da OTAN/NATO no país ou as invasões de sites e *ataques DDoS, são versões online de protestos tradicionais, mas na minha opinião classificados e tipificados como actos terroristas electrónicos.*

Além disso, no caso de guerra civil, se um lado cometer um ataque cibernético contra o outro, então pode-se dizer que é mais um ato de guerra - ou guerra cibernética - do que um de terror cibernético.

De fato, o FBI define ciberterrorismo como "qualquer ataque premeditado e politicamente motivado contra informações, sistemas de computação ou programas de computador, e dados que resultem em violência contra alvos não combatentes por parte de grupos subnacionais ou agentes clandestinos".

Segundo essa definição, muito poucas das dezenas de milhares de ataques cibernéticos realizados todos os anos contam como terrorismo cibernético.

À medida que o número de dispositivos conectados à internet aumenta, a probabilidade de um incidente terrorista cibernético mais destrutivo é cada vez maior.

Este é o crime que mais preocupa os países desenvolvidos, mas também pode ser visto em larga escala em outros lugares no mundo.

Esta tipologia de crime o Ciberterrorismo deve ser objecto de forte vigilância e análise que por parte dos serviços secretos de Países, como depois de seguida serem os OPC's a aplicar o seu papel a que estão cometidos pela Lei.

O Ciberterrorismo - Consiste em ações premeditadas com motivações políticas cometidas, geralmente, contra governos, partidos e instituições governamentais. Também podem ser cometido amplamente contra civis;

Ciberativismo: crime praticado contra organizações que defendem determinadas causas. Esse cibercrime envolve roubo de informações e manipulações nos materiais que são divulgados ao público e à imprensa;

Roubo: envolve a utilização de computadores ou outros dispositivos para desviar fundos ilegalmente, roubar dados de outros indivíduos, empresas ou instituições, para realizar espionagem, roubo de identidade, fraude, plágio e pirataria.

Para nos prevenirmos contra cibercrimes, especialistas orientam que os internautas tomem o máximo de cuidado ao navegar na internet. Também alertam sobre emails suspeitos e anexos maliciosos, especialmente em

formato .exe, que são enviados por remetentes desconhecidos, que nunca devem de ser abertos.

É importante procurar evitar sites pouco conhecidos e banners, links e ofertas que ofereçam benefícios muito especiais e duvidosos.

Manter o antivírus e o firewall sempre atualizados, além de outras ferramentas de segurança do computador, bem como o próprio sistema operacional, também é de suma importância para evitar ser vítima desses ataques cibernéticos.

Dr. Rogério Bravo, Inspector-Chefe da Unidade Nacional de Combate ao Cibercrime e a Criminalidade Tecnológica (UNC3T) defende num artigo de opinião que passo a citar:

«…Existe a percepção de que existe mais um espaço de vivência humana, a par dos tradicionais e naturais espaços (terra, mar e ar), e onde o Homem vive há conflito, e, dentro das formas de conflito (sentido amplo), o crime; donde, não sendo este espaço ciber um espaço marginal, mas sim um espaço em mutação acelerada, de grande aceitação social e baseado no apetite do utilizador pela novidade tecnológica, torna-se, pela sua interdependência com os outros espaços de vivência humana, imprevisível quanto à sua evolução tecnológica, tendências de uso e consequências sociais resultantes da adesão a essas tecnologias, a par da ausência de percepção de "ciberrisco". O mercado regula o utilizador.

Daí que o crime no espaço ciber seja "cibercrime" (crimes "tradicionais" cometidos por novas formas), mas deste cibercrime só algum é crime informático (crime em que as tecnologias de informação, processamento e comunicação são meio e fim para o crime acontecer e em que esse crime atinge sempre uma ou mais das condições de operacionalidade da segurança da informação: a confidencialidade, a integridade, a disponibilidade e o não repúdio da informação).

São alguns destes tipos de crimes que vêm tipificados na Lei do Cibercrime. Três exemplos: se é sabotagem informática, ataca-se a disponibilidade dos dados; se há um acesso ilegítimo, cai a confidencialidade; se são eliminados

dados ou corrompidos dados, atacou-se a integridade. Quando isto acontece, afecta-se a "informação contida" nos dados. E na justa medida em que se verifica maior adesão social a este espaço ciber, verificam-se mais crimes "contra" a segurança da informação, designadamente os que mencionei e que são apenas três dos crimes "puros e duros" do conjunto de crimes informáticos.»

Defendo integralmente a tese do Dr. Rogério Bravo, sendo que o mais difícil é a aceitação pelo legislador e por grande parte dos utilizadores destas tecnologias em rede de que o ciberespaço, é formatado através de transmissão electrónica de dados, que posteriormente vão ser ou até já foram transmitidos.

O ciberespaço "é feito" das estruturas físicas e dos dados informáticos num dos três estados possíveis.

Torna-se assim impossível fazer a proteção ao tráfego, mas também mitigar os incidentes de segurança, prevenir o crime e investigar a autoria destes crimes, é uma impossibilidade prática.

Com esta realidade acima descrita, o equilíbrio aquando da decisão legislativa é um ponto extremamente difícil e quase impossível.

DESENVOLVIMENTO LEGISLATIVO E SEU ENQUADRAMENTO

Começa a vigorar em 1991, no ordenamento jurídico português a Lei nº 109/91, de 17 de Agosto - Lei da Criminalidade Informática.

Embora esta lei contemplasse um conjunto amplo de ilícitos criminais, ficaria de fora aquilo que se designa juridicamente com uma «lacuna» a recolha de prova em ambiente digital.

Ficou de fora a recolha de prova em ambiente digital nos termos que se encontram definidos no Código de Processo Penal, no seu artigo 187.º e seguintes.

A restrição do regime da intercepção e gravação de comunicações telefónicas, dificultava o curso das investigações, até a subsistência das próprias investigações.

Conclui-se que embora manifestamente insuficiente a Lei do Cibercrime, veio efectivamente colmatar uma lacuna que existia no sistema processual penal em Portugal.

Embora os órgãos de polícia criminal (OPC's), ficassem apetrechados dos meios necessários - para o combate dos crimes previstos nessa mesma lei, como também o combate estaria garantido contra o crime da criminalidade informática.

A cibercriminalidade, é um crime transfronteiriço, sem sombra para dúvidas, por isso haveria que legislar nesse sentido.

Devem ser criados instrumentos legais, de carácter universal e de cooperação internacional, de modo a poderem vir a ser implementados por todos os Estados Membros.

Existem alguns diplomas internacionais a respeito da cibercriminalidade e da prova digital, destacam-se três principais diplomas de forte empacto na entrada na legislação Portuguesa:

- Convenção sobre o Cibercrime do Conselho da Europa, de 23 de Novembro de 2001;

- Directiva nº 2006/24/CE, do Parlamento e do Conselho, de 15 de Julho.

- Convenção sobre o Cibercrime do Conselho da Europa, de 23 de Novembro de 2001

- Decisão-Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro;

Em Budapeste (23 de Novembro de 2001) foi aprovada, pelo Conselho da Europa a Convenção sobre o Cibercrime.

Esta Convenção como atrás se mencionada é assinada em em 23 de Novembro de 2001, em Budapeste, dando entrada em vigor na ordem jurídica internacional a 1 de Julho de 2004, ainda assim sofreu cinco ratificações exigidas.

Esta Convenção tem como objectivo harmonizar a lei penal material no que se refere às previsões relativas à área do cibercrime, zelando para que na lei processual penal as autoridades competentes sejam dotadas dos necessários poderes de investigação e de combate a esta nova área da criminalidade. Cria igualmente um mecanismo rápido e eficaz de cooperação internacional. A Convenção prevê como crimes, designadamente, o acesso e intercepção ilegal em redes informáticas, o dano e sabotagem informática, o uso de vírus, e a posse, produção e distribuição de material de pornografia infantil na Internet.

A Convenção sobre o Cibercrime contemplou:

1. Um conjunto de conceitos informático-jurídicos;

2. Um conjunto de ilícitos criminais;

3. Um conjunto de medidas processuais destinadas a regular a forma de obtenção de prova em ambiente digital e mecanismos destinados a promover a cooperação internacional.

Portugal subscreveu a Convenção sobre o Cibercrime em 2001.

A Lei nº 109/2009, de 15 de Setembro, adaptou ao direito interno a Convenção sobre o Cibercrime.

A LEI Nº 109/2009, DE 15 DE SETEMBRO – A "LEI DO CIBERCRIME"

Em 15 de Setembro de 2009, Portugal procedeu, igualmente, à ratificação da Convenção sobre o Cibercrime, e do Protocolo Adicional à Convenção sobre o Cibercrime, relativo à Incriminação de Actos de Natureza Racista, praticados através de Sistemas Informáticos.

A Convenção veio estabelecer um conjunto de disposições:

Em primeiro lugar estabeleceu um conjunto de disposições penais materiais, processuais e normas destinadas a promover a cooperação internacional, e assim abriu o conhecimento tão importante da realidade internacional, onde os fenómenos nesta matéria já iam bastante avançadas assim como os objectos de repressão dos mesmos em termos legais.

É normal pois que a Lei nº 109/2009, de 15 de Setembro, reveste-se de um carácter inovador.

A Lei do Cibercrime vem assim quase em definitivo colmatar uma lacuna que existia, há muito tempo, no sistema processual penal português, já atrás referida.

A lei veio introduzir um regime processual não aplicável somente a processos relativos a crimes previstos na respectiva lei, mas também a processos relativos a crimes cometidos através de um sistema informático ou em qualquer processo criminal em que seja necessário proceder a recolha da chamada prova digital. É o que dispõe o artigo 11.º da referida Lei.

Assim, como indica Pedro Verdelho, o aparecimento desta lei propiciou o aparecimento de "novas ferramentas processuais"

Pode assim ser afirmado que as medidas processuais de recolha da prova digital, previstas na Lei do Cibercrime, têm um campo "de aplicação geral", na medida em que estamos perante a possibilidade de recurso a estes "meios de obtenção de provas digitais para o combate da criminalidade, seja qual for a sua forma."

Assim, entramos num regime processo para obtenção de prova digital com um vasto campo de aplicação mais abrangente do que a própria lei em si.

Não fica de forma restringida a sua utilização a processos relativas aos crimes que nela se encontram tipificados, mas também:

A crimes praticados através de um sistema informático, ou

Em processos relativos a crimes em que, independentemente da natureza ou moldura penal do crime, seja necessário, no decurso da investigação criminal, proceder à recolha de prova digital.

Isto porque, o que se pretende efectivamente com a criação deste regime de recolha de prova digital é de providenciar às autoridades criminais, instrumentos que permitam o combate contra a criminalidade em geral e não apenas relativa aos crimes previstos na Lei do Cibercrime.

A Lei nº 32/2008, de 17 de Julho transpôs para a ordem jurídica portuguesa, a Directiva nº 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de Março, relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações.

Como refere Rita Castanheira Neves, "a Lei do Cibercrime tem um âmbito de aplicação delineado, não se podendo "perder de vista os requisitos da Lei nº 32/2008, de 17 de Julho.

Mais, para a Autora, face ao disposto no artigo 11.º número 2, "somos for-

çados a demarcar campos de aplicação distintos para a Lei do Cibercrime e para a Lei nº 32/2008, de 17 de Julho"38, aplicando-se esta última lei à investigação dos chamados "crimes graves" (terrorismo, criminalidade altamente organizada), definidos no artigo 2.º número 1 alínea g).

Por seu turno, os meios de obtenção de prova contemplados na Lei do Cibercrime, aplicam-se, com as devidas excepções, aos crimes previstos na mesma, aos crimes praticados através de sistema informático bem como em processos relativos a crimes em que seja necessário proceder à recolha de prova electrónica.

No entanto, tendo a Lei nº 32/2008, de 17 de Julho transposto para a ordem jurídica portuguesa a referida Directiva, a validade da mesma pode ser posta em causa, invocando-se a eventual violação do Direito da União Europeia.

Como alerta Pedro Venâncio, "relativamente às medidas previstas nos artigos 12.º a 15.º da Lei do Cibercrime, assume especial pertinência o disposto na Lei n.º 32/2008, de 17 de Julho."

Para Pedro Venâncio: «a consagração de disposições processuais relativas à preservação, revelação, apresentação, pesquisa e apreensão de dados informáticos (previstas nos artigos 12.º a 17.º da LC) impunha-se não só como um imperativo de direito internacional, face à ratificação da Convenção sobre Cibercrime, mas, acima de tudo, como uma inevitabilidade civilizacional»

Assim, a Lei do Cibercrime prevê um conjunto de mecanismos processuais relativos à obtenção da prova digital, de carácter geral:

1. Apreensão de dados informáticos (artigo 16.º);

2. Apreensão de correio elecrónico e registos de comunicações de natureza semelhante (artigo 17.º);

3. Preservação expedita de dados (artigo 12.º);

4. Revelação expedita de dados (artigo 13.º);

5. Injunção para apresentação ou acesso a dados (artigo 14.º);

6. Pesquisa informática (artigo 15.º);

E, meios de obtenção de prova digital restritos a um conjunto determinado de crimes:

Intercepção de comunicações (artigo 18.º).

Acções encobertas (artigo 19.º).

Com a Lei do Cibercrime, o Ministério Público e até os órgãos de polícia criminal ficam com a possibilidade de ordenarem a preservação de dados, revelação de dados e apresentação ou concessão de acesso a dados informáticos a entidades e cidadãos.

Ficam desde já munidos de poderem exigir a preservação e a concessão de acesso a dados informáticos não só a "entidades públicas ou privadas, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático ou outra entidade que trate ou armazene dados informáticos"

Estamos perante uma medida que, embora se denomine de "pesquisa" (o legislador optou por uma terminologia diversa da prevista na Convenção), acaba por consistir nas tradicionais buscas, adaptada, porém, ao ambiente digital.

A autoridade judiciária é a autoridade competente para autorizar ou ordenar, por despacho, a realização da referida diligência, tendo, sempre que possível, que presidir à mesma.

À apreensão de dados informáticos aplicam-se as mesmas regras processuais que se aplicam à pesquisa de dados informáticos.

Compete à autoridade judiciária ter a competência pra autorizar ou ordenar

a realização da apreensão, podendo esta apreensão ser levada a cabo sem a prévia autorização da autoridade judiciária quando se verifique "urgência ou perigo na demora", nos termos dos artigos 16.º número 1 e número 2.

Algumas notas importantes:

- Adaptando o regime das apreensões previstas no Código de Processo Penal à realidade digital, deve ter-se presente que são apreendidos os dados ou documentos informáticos de um determinado sistema informático que serviram ou foram destinados a servir a prática de um crime, bem assim como todos aqueles que tiverem sido deixados pelo agente no local do crime ou quaisquer outros susceptíveis de servir a prova.

- Tendo como base o artigo 16.º número 3, quando esteja em causa a apreensão de "dados pessoais ou íntimos, que possam pôr em causa a privacidade do respectivo titular", os mesmos têm que ser apresentados ao juiz, só podendo ser juntos aos autos após uma ponderação, que deverá ter em conta "os interesses do caso concreto".

Já, Rita Castanheira Neves segue uma posição diversa:

A ingerência nas mensagens de correio electrónico ou registos de natureza semelhante não deverá ser objecto de um triplo tratamento – como defende de Paulo Dá Mesquita e Pedro Verdelho – mas sim de um duplo tratamento: enquanto intercepção nas comunicações, em tempo real e, enquanto comunicações armazenadas em suporte digital.

De notar que o artigo 18.º regula a "intercepção de comunicações" electrónicas ficando assim com a incumbência de abarcar as medidas processuais contempladas na Convenção sobre o Cibercrime.

A maior parte da doutrina, é consensual e considera que a intercepção de comunicações electrónicas pode ser utilizada em processos relativos a crimes:

Praticados através de sistema informático em relação aos quais seja necessário proceder à recolha de prova electrónica, desde que os crimes

se encontrem previstos no artigo 187.º número 1 do Código de Processo Penal.

À semelhança do que sucede no ordenamento jurídico português – antes e depois da entrada em vigor da Lei do Cibecrime – no ordenamento jurídico alemão, o recurso à intercepção e gravação das comunicações, só é admissível em processos relativos a um conjunto específico de crimes.

A respectiva intercepção tem que ser autorizado ou ordenado por um juiz, embora em caso de "perigo na demora", o Ministério Público pode ordenar as mesmas. No entanto, terá que ser posteriormente validada por uma autoridade judicial.

Já Rita Castanheira Neves, defende que esta norma é indicadora de que a intercepção e gravação de comunicações não se cinge apenas às comunicações telefónicas, permitindo-se a intromissão em comunicações de outra natureza.

O artigo 19.º, polémico tem como título na sua epígrafe "acções encobertas", fica determinada a admissibilidade de "recurso às acções encobertas previstas na Lei nº 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes:

- Os previstos na presente lei; e os cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infracções económico- financeiras, bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos.

Parece assim estarmos perante uma medida processo algo inovadora, na medida em que, tal como o artigo 17.º, não encontra correspondência na referida Convenção.

O artigo 19.º número 1, vai ampliar a possibilidade de recurso à acção encoberta, prevendo um conjunto de crimes que não se encontram previstos na Lei nº 101/2001, de 25 de Agosto - Regime Jurídico sobre as Acções Encobertas.

Fica assim tipificado que existem duas fontes normativas, que regulam o modo de obtenção da prova digital: a Lei do Cibercrime e o Código de Processo Penal.

Assim, de acordo com o contemplado no Código de Processo Penal:

A intromissão nas comunicações já armazenadas em suporte digital deverá seguir o regime processual aplicável à intercepção e gravação de comunicações telefónicas (artigo 189.º número 1, segunda parte);

Assim, só é permitido o recurso a este tipo de diligência em processos relativos aos crimes elencados no artigo 187.º número 1 (deixando de fora um conjunto significativo de crimes informáticos);

O recurso a este tipo de diligência só é permitido durante a fase do inquérito e "se houver razões para crer que a diligência é indispensável para a descoberta da verdade, ou que a prova seria, de outra forma, impossível ou muito difícil de obter."

Já a Lei do Cibercrime estabelece:

A apreensão de correio electrónico ou registos de natureza semelhante pode ser levada a cabo em processos relativos aos crimes previstos na respectiva lei; aos crimes praticados através de sistema informático e aos crimes em que seja necessário proceder à recolha de prova em suporte electrónico (artigo 11.º número 1);

A referida diligência terá que se autorizada ou ordenada pelo juiz quando a referida apreensão seja "de grande interesse para a descoberta da verdade ou para a prova"; (artigo 17.º)

É aplicável "o regime de apreensão de correspondência previsto no Código

de Processo Penal" (artigo 17.º).

O regime da apreensão de correio electrónico e registos de comunicações de natureza semelhante passa a ser regulado directamente pelo artigo 17.º da Lei do Cibercrime e, subsidiariamente (por remissão expressa do mesmo), pelos pressupostos e requisitos legais relativos à apreensão de correspondência, previstos nos artigos 179.º e 252.º (nº 2 e 3) do Código de Processo Penal.

Com o artigo 17.º desta Lei:

"passa a ser admitido o acesso e obtenção de correio electrónico em todas as investigações criminais cujo crime em causa esteja previsto na Lei nº 109/2009, seja cometido por meio de um sistema informático ou em relação ao qual seja necessário proceder à recolha de prova em suporte electrónico.

Para Manuel Costa Andrade, o artigo 189.º número 1 do Código de Processo Penal contempla em si duas realidades distintas: por um lado, regula-as comunicações/conversações, em tempo real, realizadas através de um meio técnico diferente do telefone e, por outro lado, regula as conversações/comunicações armazenadas em suporte digital, ou seja, o produto do acto comunicacional.

Para este Autor,o direito fundamental à inviolabilidade das telecomunicações, constitucionalmente consagrado no artigo 34.º (da Constituição da República Portuguesa), assegura "o livre desenvolvimento da personalidade de cada cidadão, nomeadamente através da troca, à distância de informações, notícias, pensamentos, opiniões, à margem da devassa da publicidade.

Para Pedro Venâncio, quando existam mensagens de correio electrónico que, embora não tenham sido interceptadas em tempo real mas que se encontrem armazenadas na caixa do correio do destinatário, seja em servidor que preste serviço de armazenamento ou no próprio computador sejam relevantes para a descoberta da verdade, existem os meios específicos previstos nos artigos 12.º a 17.º da Lei do Cibercrime", destinados a garantir o seu acesso.

Deste modo, a doutrina - bem como a jurisprudência – reúne consenso quanto à desaplicação do artigo 189.º número 1 do Código de Processo Penal.

Para Pedro Verdelho, o regime de apreensão de correspondência previsto no Código de Processo Penal não é inteiramente aplicável ao regime estatuído no artigo 17.º da Lei do Cibercrime.

Nos termos do artigo 179.º do Código de Processo Penal:

A apreensão de correspondência só poderá ser ordenada ou autorizada quando existirem "fundadas razões para crer que: a) a correspondência foi expedida pelo suspeito ou lhes é dirigida, mesmo que sob nome diverso ou através de pessoa diversa; b) está em causa crime punível com pena de prisão superior, no seu máximo, a 3 anos e c) a diligência se revelará de grande interesse para a descoberta da verdade ou para a prova" (artigo 179.º número 1);

Pedro Verdelho defende a não aplicação do artigo 179.º número 1 do Código de Processo Penal, embora considere que "o artigo 17.º da Lei do Cibercrime não ignora os requisitos previstos no artigo (179.º número 1), tendo inclusive integrado um deles no regime do artigo 17.º (nomeadamente o requisito "quando a apreensão (…) se afigure ser de grande interesse para a descoberta da verdade ou para prova").

Quanto à intervenção judicial, Pedro Verdelho defende que o regime do artigo 17.º da Lei do Cibercrime tem que ser interpretado num sentido diverso do regime legal previsto nos artigos 179.º e 252.º do Código de Processo Penal.

Fica assim assente que as mensagens de correio electrónico (e os registos de comunicações de natureza semelhante) só podem ser juntas aos autos após intervenção judicial.

O que Pedro Verdelho defende é que essa intervenção judicial só pode acontecer após a apreensão – que neste caso será uma apreensão provisória – dado o objecto sobre que incide a referida diligência.

Assim, para Pedro Verdelho, o regime para a apreensão de correspondên-

cia previsto no Código de Processo Penal não deve ser totalmente aplicado ao regime previsto no art. 17.º da Lei do Cibercrime.

Assim, nos termos do Código de Processo Penal:

Só era permitido o uso desta diligência, em processos relativos aos crimes elencados no artigo 187.º número 1 (deixando de fora um conjunto significativo de crimes informáticos);

Só era permitida durante a fase do inquérito e se houvesse "razões para crer que a diligência é indispensável para a descoberta da verdade, ou que a prova seria, de outra forma, impossível ou muito difícil de obter."

ALGUMAS CONCLUSÕES PARA REFLEXÃO

O legislador português limitou-se, até à entrada em vigor da Lei do Cibercrime, a englobar a realidade digital num único regime processual:

O regime da intercepção e gravação de comunicações telefónicas, mas descurou as suas especificidades e componentes desta tão grande realidade.

Embora o combate contra a criminalidade informática seja uma preocupação constante do legislador português, na verdade é que o regime jurídico de obtenção da prova digital só veio a ser implementado em 2009, pecando por tardio.

A Lei do Cibercrime tenta reflectir uma linha de entendimento que regula de forma distintiva, tendo introduzido regimes assentes em princípios e linhas orientadoras distintas:

A intercepção e registo de comunicações electrónicas, entende-se por comunicações como comunicações levadas a cabo através de um meio técnico diferente do tradicional telefone e a intromissão nas comunicações armazenadas em formato/suporte digital.

Desta maneira, a Lei nº 109/2009, de 15 de Setembro – a "Lei do Ciber-

crime" – veio superar uma lacuna que existia em matéria de prova digital no ordenamento jurídico Português, ainda que na minha opinião manifestamente insuficiente.

Lei do Cibercrime estabeleceu um regime para a intercepção e registo de comunicações electrónicas, bem como um regime especificamente direcionado para a apreensão de correio electrónico ou seja, para a apreensão do daquilo que resulta do produto de um acto comunicacional.

Na minha opinião, o crescente número de casos de crimes cibernéticos é devido à crescente exposição à tecnologia em todo o mundo. Hoje em dia, mais pessoas estão a abusar da tecnologia nas suas vidas diárias, especialmente na internet. Como a Internet está amplamente ligada, algumas pessoas aproveitam esta tecnologia para a práctica de crimes. Além disso, as pessoas tendem a ser influenciadas pela curiosidade sobre novidades mas também lucros que estes ilícitos podem trazer, sem investigar as fontes, especialmente da internet. Assim, é muito mais fácil para os criminosos usarem essa tecnologia avançada que temos hoje para fazer alguns crimes.

As pessoas hoje em dia deveriam aumentar a consciencialização sobre a lei do crime cibernético para que os utilizadores pudessem evitar o abuso dessa tecnologia para este tipo de crime, especialmente na Internet e para a segurança deles mesmos e dos seus filhos!

Percebi que há vários efeitos deste crime cibernético em todas as expectativas, como a degradação moral entre as novas gerações, perda de receita, desperdício de tempo, reputação prejudicada e produtividade reduzida e privacidade dos utilizadores completamente exposta. Assim, todas as partes envolvidas devem levar este problema a sério.

Não basta pensar na solução para superar este problema, mas também pensar na solução para evitar os fatores que contribuem para os crimes cibernéticos. Não se julgue apenas o governo, mas os Pais também desempenham papéis importantes para educar seus filhos a usar as tecnologias;

A Consciência individual é a coisa mais considerável para superar este crime cibernético. A tecnologia está a funcionar para desenvolver o conhecimento

humano e facilitar as tarefas da vida diária, que podem ser simplificadas sem sobra de dúvida, mas com as devidas precauções.

BIBLIOGRAFIA

BRAVO ROGÉRIO; Entrevista *Revista Ordem dos Advogados*, 2017 - http://boletim.oa.pt/oa-02/entrevistas

ALBUQUERQUE, PAULO PINTO DE, *Comentário do Código de Processo Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, Universidade Católica Editora, 2008;

ANDRADE, MANUEL DA COSTA, "Bruscamente no verão passado", a Reforma do Código de Processo Penal-Observação críticas sobre uma lei que podia e devia ter sido diferente, Coimbra Editora, 2009;

CANOTILHO, J. J. GOMES; MOREIRA, VITAL, *Constituição da República Anotada*, Vol. I, 4ª Edição Revista, 2007

NEVES, RITA CASTANHEIRA NEVES, *Natureza e Respectivo Regime Jurídico do Correio Electrónico Enquanto Meio de Obtenção de Prova*, Coimbra Editora, 2011

MARQUES, MARIA XARA-BRASIL, *Dissertação Mestrado*, Universidade Católica, 2014

MIRANDA, JORGE; MEDEIROS, RUI, *Constituição Portuguesa Anotada*,Tomo I, Coimbra Editora, 2011

VENÂNCIO, PEDRO, *Lei do Cibercrime Anotada e Comentada*, Coimbra, Coimbra Editora, 2011;

VERDELHO, PEDRO, "A obtenção de prova no ambiente digital", *Revista do Ministério Público*, Ano 25.º, nº 99 Julho-Setembro 2004 pp. 117-136;

VERDELHO, PEDRO; BRAVO, ROGÉRIO; ROCHA, MANUEL LOPES, *Leis do Cibercrime*, Col. PAULA VEIGA, Vol. I., Centroatlantico.pt, Portugal 2003.