DIANA VIVEIROS DE SIMAS

O CIBERCRIME

Orientador: Prof. Doutor José Sousa Brito

Universidade Lusófona de Humanidades e Tecnologias

Departamento de Direito

Lisboa

2014

DIANA VIVEIROS DE SIMAS

O CIBERCRIME

Dissertação apresentada para a obtenção do Grau de Mestre em Direito, no Curso de Mestrado em Ciências Jurídico-Forenses,
conferido pela Universidade Lusófona de Humanidades e Tecnologias.
Orientador: Prof. Doutor José Sousa Brito

Universidade Lusófona de Humanidades e Tecnologias

Departamento de Direito

Lisboa

2014

Agradecimentos

Em primeiro lugar quero agradecer à minha família. Aos meus pais, Luísa Viveiros e Rui Simas, pelo incentivo e apoio incondicionais durante toda a minha vida, e claro, como não podia deixar de ser durante a minha licenciatura e mestrado. A insistência e persistência que demonstraram neste percurso fez-me crer e acreditar no que hoje estou a finalizar, uma das melhores etapas da minha vida. Sem vocês não estava aqui e mais que tudo sem vocês não seria o que sou.

Em segundo lugar quero agradecer, ao meu namorado Nuno Vieira, por tudo o que temos até agora vivido, pelo dia-a-dia repleto de cumplicidade, pelo tempo dedicado a aturar-me, seja nos momentos de mais certeza na elaboração deste trabalho, seja nos momentos de maior frustração. Sempre ouvi uma palavra de apoio, uma atitude de ajuda, uma presença constante que me fez ter força e vontade em terminar algo que parecia longe de se concretizar.

Quero, também, agradecer à minha madrasta, Cila Simas, aos meus irmãos, Hélder Simas, Carolina Simas e Matilde Simas, que tiveram sempre presentes e dedicados em ajudar-me a elaborar este trabalho, seja a descontrair através das suas conversas, brincadeiras, seja através de mimos e abraços que em muito ajudaram.

À Fátima Vieira e José Vieira obrigada por me aturarem na sua casa durante toda a elaboração da minha tese, por estarem sempre prontos a ajudar e me proporcionarem tudo o que precisei. Obrigada pelo apoio e confiança que depositaram em mim.

À Arminda Silveira, Tiago Ávila e Diogo Silveira, por todo o apoio e força, por todos os momentos que me proporcionaram num ambiente de amizade, por todas as conversas e risadas que me permitiram prosseguir com força o meu trabalho.

Aos meus amigos intemporais, Ricardo Leal, Nuno Coelho, Cátia Machado, Pedro Pereira, Guilherme Machado e Artur Silva, agradeço por todos os dias passados a discutir a sociedade em que vivemos, os problemas da actualidade, o desgoverno que sentimos, a revolta que transmitimos e com um contributo extremo para o meu trabalho, as opiniões que expressaram sobre o tema Cibercrime, o que ajudou e muito. Mas principalmente e acima de tudo, obrigada por ajudarem a esquecer tudo isto e me proporcionarem momentos inesquecíveis.

Aos meus amigos de faculdade que para sempre ficaram, Inês Costa, Filipa Francisco, Sancho Cazeiro, Sara Ribeiro, Isabel Teixeira, Sara Sousa, João Silva, Diogo

Brito, Luís Santos, longe ou perto senti o apoio e confiança que depositaram em mim. Um brinde aos nossos jantares que em todos os momentos me deram motivação e descontracção.

À Universidade Lusófona de Humanidades e Tecnologias, obrigada pela formação concedida, pelas condições oferecidas e por se ter transformado numa segunda casa.

A todos os meus professores, agradeço a confiança que demonstraram nas minhas competências e na minha pessoa que muito contribuiu para o meu desenvolvimento pessoal e profissional.

A todas as pessoas que de uma maneira ou de outra se atravessaram no meu caminho e que marcaram cada dia da minha vida.

Resumo

O Cibercrime, realidade cada vez mais presente na sociedade, impõe uma resposta eficaz por parte do Direito. A crescente evolução tecnológica permite o aparecimento de novos crimes e a modernização dos tradicionais, pelo que importa conhecer os tipos de cibercrimes existentes e desta forma combate-los com legislações adequadas.

A nível internacional existem instrumentos legislativos que, atendendo às necessidades sentidas no âmbito da tutela de determinados bens jurídicos, tratam o tema do Cibercrime e tipificam diversas condutas consideradas lesivas de direitos fundamentais. São, nomeadamente a Convenção sobre o Cibercrime adoptada em Budapeste de 23 de Novembro de 2001 e a Decisão-Quadro 2005/222/JAI do Conselho de 24 de Fevereiro de 2005.

A nível nacional verificamos que para adequar a sua legislação à evolução tecnológica e exigência imposta pela legislação internacional, surgiu a Lei do Cibercrime 109/2009, 15 de Setembro, que tipifica os comportamentos considerados como crime no âmbito do Cibercrime.

É de ter em consideração que as legislações que regulam esta matéria não podem ser estáticas, devendo sempre que se afigure necessário proceder-se a uma adaptação do direito penal à realidade informática, nomeadamente quando surjam figuras que possam ter uma influência neste meio, como por exemplo os prestadores de serviços de internet.

Palavras-chave: Cibercrime, Convenção sobre o Cibercrime, Lei do Cibercrime 109/2009

Abstract

The Cybercrime reality present in society requires an effective response by the law. The technological development allows the emergence of new crimes and the modernization of the traditional ones. So, it is important to know the types of cybercrimes and thus combat them with appropriate laws.

There are international legal instruments, that because of the felt needs, tutelage certain legal rights, by treating the theme of Cybercrime and qualifying several behaviours deemed detrimental to fundamental rights. Are, in particular, the Cybercrime Convention adopted in Budapest November 23th, 2001 and the Framework Decision 2005/222/JHA February 24th, 2005.

At national level, to adjust legislation to technological developments and requirements imposed by international law was created the Cybercrime Law 109/2009, September 15th, which typifies the behaviour regarded as a cybercrime.

It should be borne in mind that the cybercrime laws can not be static and should whenever it appears necessary proceed to an adaptation of criminal law to technological reality, especially when figures that may have an influence on this medium arise, such as the companies that provides internet services.

Key-words: Cybercrime, Cybercrime Convention, Cybercrime Law 109/2009

Abreviaturas

Acórdão – AC

Acórdão do Tribunal da Relação de Lisboa – ATRL

Acórdão do Tribunal da Relação do Porto – ATRP

Acórdão do Tribunal da Relação de Coimbra - ATRC

Artigo – Art.

Assembleia da República – AR

Código Civil - CC

Código dos Direitos de Autor e Direitos Conexos- CDADC

Código Penal – CP

Código de Processo Penal - CPP

Comité de Especialistas Sobre a Criminalidade no Ciberespaço – PC-CY

Comité Europeu para os Problemas Criminais – CDPC

Confirma – Cf.

Constituição da República Portuguesa – CRP

Convenção sobre o Cibercrime – Ccib

Decisão Quadro – DQ

Departamento de Investigação e acção penal – DIAP

Internet service providers /fornecedores de serviços - ISP

Lei da Criminalidade Informática – LCI

Lei de Organização da Investigação Criminal - LOIC

Lei do Cibercrime – LC

Lei do Comércio Electrónico – LCE

Lei de Protecção de dados pessoais - LPDP

Juiz de Instrução Criminal – JIC

Ministério Público – MP

Página – pág.

Polícia Judiciária - PJ

Presidente da República – PR

Procuradoria-geral da República – PGR

Regime Jurídico do Comércio Electrónico - RJCE

União Europeia – UE

Índice

Introdução

Nos dias de hoje a informática tornou-se um elemento essencial à actividade económica, cultural e social e ao seu desenvolvimento.

Com a evolução sentida nas tecnologias de informação, que facilitam a vida dos cidadãos, seja a nível de trabalho, pessoal ou mesmo social, notou-se que a liberdade de circulação na internet e de comunicação teria que ser aliada a direitos que pudessem garantir segurança às pessoas que usufruem desta tecnologia. Isto, porque, se a informática é munida de grandes vantagens, também o é de desvantagens.

Tornou-se um instrumento facilitador da prática de factos ilícitos, sejam eles os denominados crimes tradicionais, como também facilitou o surgimento de outros tipos de crime.

A União Europeia mostrou-se sensível a estas questões, fazendo um esforço nas orientações legislativas desde então. A aplicabilidade do direito à Sociedade de Informação sempre levantou alguns problemas, devido à extraterritorialidade da informática. Sentiu-se necessidade em harmonizar as legislações e trazer aos Estados novas medidas e instrumentos que pudessem combater eficazmente os novos problemas associados aos crimes cometidos por meio da informática, nomeadamente para fazer face à internacionalização da criminalidade informática.

A Convenção sobre o Cibercrime adoptada em Budapeste em 23 de Novembro de 2001 e a Decisão-Quadro 2005/222/JAI do Conselho 24 de Fevereiro de 2005, são os dois instrumentos internacionais mais importantes no que diz respeito ao tema cibercrime, que surgiram como resposta ao crimes cometidos pela tecnologia informática. Impõe-se fazer uma análise de ambos os instrumentos para que se perceba as condutas que à luz destes diplomas são consideradas crimes. Acresce que, ainda neste âmbito, surgiram diversas exigências para serem adoptadas a nível nacional, permitindo desta forma a consonância entre as legislações dos Estados assinantes.

A Lei 109/2009 de 15 de Setembro, Lei do Cibercrime, transpôs para a ordem jurídica interna aqueles instrumentos legislativos e revogou a até então vigente Lei da Criminalidade Informática. Criou tipos de crimes onde a informática aparece como meio para a prática de um crime.

Dada a sua natureza penal, e apesar de constar fora das normas do Código Penal, deve em todos os casos ser aplicável a parte geral deste Código.

Resta considerar se faz ou não sentido a inserção destes crimes fora do CP, pois como veremos na análise dos crimes da LC, muitas vezes impõe-se conjugar as normas constantes em ambos os diplomas legais, interpretando o seu sentido, atendendo à vontade do legislador, considerando a época histórica envolvida.

Alguns autores consideram a LC inapropriada e injustificada pelo facto de muitas vezes reproduzir crimes já revistos no CP, alegando que a sua existência deve-se a exigências comunitárias. Em outros países, como Itália e Alemanha, os tipos de crime previstos na LC, como por exemplo a falsidade informática, encontram-se tipificados nos Códigos Penais [1], encarando-os como forma qualificada do tipo, no caso italiano, ou como crime especifico com uma relação de especialidade à norma comum, como no caso Alemão.

Teremos sempre de considerar que o legislador pretendeu, ao criar a LC, tipificar crimes, com semelhanças existentes ou não no âmbito do CP, que sejam praticados por meio de sistema informático e suas componentes como prática e objecto do crime. Surgindo aqui o meio informático como elemento objectivo do tipo. Tratam-se de crimes próprios inseridos na criminalidade económica e/ou crimes contra a intimidade ou privacidade, merecendo uma disciplina por parte do direito penal, atendendo aos direitos, liberdades e garantias concedidos pela Constituição da República Portuguesa.

Em muitas ocasiões o que nos vai permitir distinguir os crimes previstos no CP dos crimes tipificados na LC é o bem jurídico tutelado, pois naquele encontramos bem jurídicos que são protegidos única e exclusivamente pela sua natureza iminentemente patrimonial, enquanto que na LC os bens jurídicos protegidos incidem, nomeadamente, na integridade dos sistemas informáticos. É exactamente a real gravidade dos crimes, em função da protecção de bens jurídicos, que justificam a intervenção penal da LC.

Outra consideração a ser feita é o papel que desempenham os prestadores de serviço de internet, seus direitos e deveres, pois com cada vez mais frequência estes envolvem-se em situações que se enquadram nos cibercrimes, devendo apurar-se a sua responsabilidade neste âmbito.

[1] Artigo 491bis do Código Penal Italiano e Secção 269 do StGB)

1. O conceito de Cibercrime

O conceito de criminalidade informática, ou cibercrime, como hoje conhecemos não é unânime, nem tão pouco exacto. Alguns entendem que é considerada como "todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é alvo simbólico desse acto ou em que o computador é objecto de crime"[2], outros inserem o crime informático em categorias diferentes – crime informático digital próprio/puro ou crime digital impróprio/impuro[3] – inserindo os crimes onde o bem jurídico protegido é a informática no conceito de criminalidade-digital em sentido próprio[4].

Podemos afirmar que associado a este fenómeno da criminalidade informática estão, sem dúvida, condutas violadoras de direitos fundamentais, seja através da utilização da informática para a prática de um crime, ou como um elemento do tipo legal de crime. Face a esta perspectiva, a criminalidade informática em sentido amplo, engloba toda a actividade criminosa que pode ser cometida através de meios informáticos. Em sentido estrito, são englobados os crimes quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital.

Como referido anteriormente a informática pode ser um instrumento para a prática de crimes ditos tradicionais, que não necessitam do suporte informático para serem realizados, nem fazendo este parte do seu tipo legal, veja-se a maioria dos crimes contra a honra, que podem muito bem ser cometidos com recurso ao meio informático para sua divulgação por exemplo (correio electrónico, redes sociais). Outros são os casos em que a informática surge como elemento integrador do tipo, podendo o bem jurídico protegido não ser unicamente relacionado com a informática, como por exemplo sucede no crime contra programas de computador em que o bem jurídico protegido é o direito de autor.

A prática de crimes na internet assume várias denominações, entre elas - crime digital, crime informático, crime informático-digital, «high technology crimes», «computer related crime». Não existe consenso quanto à expressão, quanto à definição, nem mesmo quanto à tipologia e classificação destes crimes, contudo, atendendo aos diversos instrumentos legislativos, consideramos ser de especial interesse utilizar a denominação de cibercrime.

[2] Garcia Marques e Lourenço Martins, Direito da Informática, 2ª Ed., Almedina, Coimbra, 2006

[3] O Crime é cometido por meio da informática e contra um sistema informático, enquanto que na categoria de impuro o crime cometido pode ser diversificado.

[4] Benjamim Silva Rodrigues, Direito Penal – Parte Especial, Tomo I – Direito Penal Informático-Digital,Coimbra Editora, 2009

A Comissão Europeia, inclui no cibercrime três tipos de actividade criminosa: os **crimes tradicionais** cometidos com o auxílio do computador e redes informáticas, os **crimes relacionados com o conteúdo**, nomeadamente a publicação de conteúdos ilícitos por via de meios de comunicação electrónicos, e os **crimes exclusivos das redes electrónicas**, que são cometidos exclusivamente por meio informático.

A doutrina portuguesa[5], diferentemente, engloba quatro tipos de actividade criminosa associada ao cibercrime: **- Os crimes que recorrem a meios informáticos**, não alterando o tipo penal comum, correspondem a uma especificação ou qualificação deste, são exemplo a "devassa por meio de informática" (art. 193º do Código Penal), o crime de burla informática e o crime de burla informática nas telecomunicações (art. 221º); **- Os crimes relativos à protecção de dados pessoais ou da privacidade** (Lei nº 67/98, de26 de Outubro, transposição da Directiva nº 95/46/CE e a Lei nº 69/98, de 28 de Outubro); **- Os crimes informáticos em sentido estrito**, sendo o bem ou meio informático oelemento próprio do tipo de crime. Neste grupo inserem-se os crimes previstos na Lei nº 109/2009 de 15 de Setembro; **- crimes relacionados com o conteúdo**, onde se destacam a violação do direito de autor, a difusão de pornografia infantil (art. 172º, nº 3, alínea d)) ou a discriminação racial ou religiosa (art. 240º, nº 1, alínea a)).

[5] Oliveira Ascensão, Pedro Dias Venâncio

1.1 A evolução da Internet aliada ao crescimento do cibercrime

A Internet foi criada, em 1969, pelo governo norte-americano, tendo como principal escopo objectivos militares. A primeira versão desse sistema ficou conhecida como ARPAnet (nome derivado de Advanced Research Projects Agency ou Agencia de Projectos de Pesquisa Avançada).

O nome "Internet" surgiu décadas mais tarde, quando a tecnologia desenvolvida passou a ser usada para ligar universidades americanas entre si e depois também institutos de pesquisa sediados em outros países.

A exploração comercial de serviço começou no inicio da década de 90 e desenvolveu-se devido à invenção da "World Wide Web", um enorme pacote de informações, em formato de texto ou «midia» (imagens e arquivos de áudio e vídeo), organizadas para que o usuário possa percorrer as paginas da rede, a partir de sequencias associativas (links) entre blocos vinculados por remissões.

Contudo, o seu objectivo principal foi "esquecido", tendo a internet chegado a toda a população mundial, tornando-se num espaço cibernético sem qualquer tipo de fronteiras, dando origem ao que hoje conhecemos por "Sociedade da Informação".

Podemos com toda a clareza afirmar que a internet desempenha um papel fundamental na sociedade, servindo de suporte às mais variadas infra-estruturas governamentais, militares, de segurança, económicas, de telecomunicações, de transportes, educacionais, energéticas, de saúde, estendendo-se a todo o tipo de relações, sejam elas comerciais, sociais e pessoais, nomeadamente neste último campo encontramos as conhecidas redes sociais, blogues e fóruns. A crescente dependência da sociedade de informação em relação aos sistemas informáticos, tornou o cibercrime um fenómeno frequente, internacional, perigoso e violador de direitos fundamentais.

A evolução operada nas novas tecnologias, projectou-se sobre o fenómeno criminal, pois se atendermos às suas duas vertentes, por um lado, a tecnologia pode ser, ela mesma, objecto de prática de crimes e por outro lado, suscita e potencia novas formas criminais ou novas formas de praticar antigos crimes. Podemos tomar como exemplo os casos de violação dos direitos de autor que cada vez mais, através do formato digital, se torna fácil a sua reprodução. A multiplicidade das redes de comunicação possibilitam a troca e partilha em rede de ficheiros, neste caso concreto, obras cujo autor não deu autorização para tal, como filmes, músicas, livros etc. Não podemos esquecer que a partilha de ficheiros nem sempre

implica uma actividade ilícita, como nos casos em que o trabalho, por exemplo de uma empresa, pode ser disponibilizado a uma pessoa que não se encontra no espaço físico daquela. Contudo, a par desta partilha de ficheiros lícita e legítima, encontramos cada vez mais sujeitos que se aproveitam desta possibilidade para o fazer de forma ilícita e partilhar ficheiros aos quais não se encontram autorizados pelo titular do direito a faze-lo.

Para fazer face a esta problemática impõe-se um nível de segurança, fiabilidade e eficiência no seio da internet, criando para tal uma segurança informática.

1.2 O Cibercrime no mundo

Uma sociedade é pautada por regras, costumes, pelo que a cultura que lhe está inerente influencia directamente o modo de relacionamento entre as pessoas, a forma como estas projectam as suas vontades e como se posicionam na vida social. Claro que estes aspectos são perceptíveis na forma como gerem os seus negócios, no modelo de empresa de escolhem, nas decisões que tomam e em tudo os que os rodeia no meio social. Claro que se entrarmos no campo dos ilícitos criminais, estes aspectos não deixam de ser marcantes, pelo que o cibercrime é directamente influenciado.

Raphael Labaca, especialista em educação e pesquisa do laboratório de segurança "Eset" na América Latina, em entrevista ao "IT WEB", explicou os aspectos regionais dos ataques ou ameaças cibernéticas. Sendo uma pessoa multicultural, vive bem de perto as realidades associadas ao cibercrime. Afirma que no caso da América Latina, uma das principais dificuldades é a punição dos sujeitos que praticam estes crimes, pois não existe no código penal a tipificação de cibercrime, como crime.

Através do estudo elaborado foi possível, em relação aos países alvo daquele, retirar as seguintes conclusões:

⇒ O crime mais comum na **Rússia** é a invasão em computador alheio. O sujeito invade o computador e apropria-se do seu domínio. Para que o proprietário do computador o possa voltar a usar e aceder aos seus arquivos, o infractor exige um pagamento em dinheiro para conceder à vítima uma senha que lhe permite aceder ao computador normalmente.

⇒ A **China** é uma grande fabricante de "malware", contudo os ataques originados no interior do país não são, normalmente, virados para os usuários chineses. Isto porque para tal acontecer é necessário entender a língua perfeitamente, o que não acontece na maioria dos casos. À parte disto basta conhecer o inglês para atingir qualquer usuário do mundo, independentemente da sua localização. Não quer isto dizer que não existem ataques na China, existem e muitos, mas em larga escala existe de dentro para fora do país.

⇒ O **Brasil** é constituído por uma vasta população, pelo que o número de ataques existente é superior ao de muitos outros países. É analisado a parte dos países inseridos na América Latina, por ser o único em que se fala Português. O sector bancário é dos mais afectados, o cibercrime incide fortemente na vertente financeira. Os ataques ocorrem de duas formas, via «phishing» onde o usuário recebe um e-mail, supostamente, do seu banco

para actualizar informações pessoais sob risco da conta ser cancelada. Outra forma, é através de um cavalo de Tróia, um "malware" instalado dentro do computador que redirecciona o URL quando o usuário digita no browser o "link" do banco. Em ambos os casos é criado um ambiente "fantasma" semelhante ao que usuário está acostumado a visualizar.

⇒ Na **Europa** o cibercrime está na sua maioria voltado para os falsos antivírus que são conhecidos como "Rogues", janelas que aparecem no browser durante uma navegação alertando o usuário que o seu computador está infectado. Este ao aceitar fazer uma verificação no seu computador é depois alertado que este está infectado, o sistema oferece ao usuário a possibilidade de corrigir este problema, mediante a compra do serviço. Contudo o serviço não existe e a pessoa paga por algo que não terá retorno.

⇒ A **América Latina** é também alvo de ataques ao sector bancário. Diferentemente do Brasil, que direcciona este problema para o elevado número de população, aqui a facilidade está no idioma. Muitos bancos usam a língua oficial espanhola nos seus sistemas, tornando mais fácil os ataques direccionados dentro deste perfil. Por outro lado a criação de "botnets" a partir de pendrives infectados são acções muito praticadas em países como o Peru, Chile e Argentina.

⇒ Os **E.U.A.** devido à sua extensa dimensão, elevado número de Estados e população e pelo imenso número de acessos à internet, são alvo de todos os tipos de ameaça cibernética, desde ataques ao sistema bancário, como "cavalos de Tróia", "botnets" etc.

Estes são os comportamentos mais comuns nestes países o que não quer dizer que não ocorram outro tipo de ameaças ou ataques cibernéticos nestes países, mas em menor número.

Em 2012, a empresa "Sperling's BestPlaces" elaborou um estudo que considera a cidade de Manchester, no Reino Unido, a mais arriscada para se navegar na Internet, com mais tentativas de "malware", mais precisamente 1977 (software destinado a entrar no sistema de computador alheio de forma ilícita, com o intuito de causar dano ou roubo de informações), seguida das cidades de Amesterdão, na Holanda, e Estocolmo, na Suécia, que ocupam o segundo e terceiros lugares da lista dos dez locais mais arriscados para utilizar a internet. O estudo revela, ainda, os factores de risco existentes online e que tornam os seus consumidores mais vulneráveis ao cibercrime, dados que resultam de uma combinação com informações fornecidas pela "Symantec", fabricante de software de segurança e que dispõe de informações relativas ao estilo de vida do consumidor na Internet. A cidade que se encontra

em sétimo lugar, Milão, em Itália, foi alvo de 555 ataques tentados na internet e 3768 nos "spams" contra endereços de IP. Por outro lado, Paris, em França, que é a quarta cidade mais arriscada domina os "bots", aplicação de software concebida para simular acções humanas repetidas vezes de maneira padrão.

Os dados revelados pelo estudo sobre o cibercrime "baseiam-se na contagem dos "bots" por cidade, no número de ataques na Web, no número de infecções tentadas por "malware" e no "spam" a endereços IP", afirma a empresa autora do estudo.

1.3 O Cibercrime e os ataques informáticos, a Banca Online e as Redes Sociais

- ### O Cibercrime

A comissão europeia afirma, que segundo diversos estudos, todos os dias são vítimas de crimes online cerca de um milhão de pessoas. De acordo com o já referido relatório da "Symantec", os danos resultantes dos ataques informáticos ascendem a 290 mil milhões de euros. Os dados do Eurobarómetro demonstram uma preocupação atendendo à realidade que se verifica, visto que 12% dos utilizadores de Internet admitem que já foram vítimas de ataques e 89% reconhecem que disponibilizam informação pessoal na rede.

A "Symantec", na sua edição de 2012 do estudo anual "*Norton Cibercrime Report* ", revela que em cada segundo dezoito adultos são vítimas de cibercrimes a nível mundial, o que se traduz em meio milhão de vítimas por dia. Este estudo baseado na informação transmitida por treze mil adultos distribuídos por 24 países calcula que cada vitima perca 197 dólares por ano devido a ataques informáticos, o que resulta num custo de 110 mil milhões de dólares para os consumidores, registando-se um valor inferior ao de 2011 (338 mil milhões de dólares).

O estudo aponta, em comparação com o ano anterior, novas formas de cibercrime, atendendo ao crescente aparecimento de redes sociais e dispositivos móveis que servem de plataforma para cometer diversos ataques, pois os utilizadores estão mais desprovidos dos riscos de segurança. Segundo o relatório, 21% dos utilizadores adultos afirmam ter sido vítimas de cibercrime em redes sociais ou a partir de dispositivos moveis e 39% alvo de "cibercrime social", com destaque para o roubo de identidades (15%) e para a recepção de mensagens de desconhecidos a sugerir a ligação a outros links (31%). A "Symantec" aconselha a que os utilizadores façam uso de palavras passe seguras e que as alterem constantemente, prevenindo desta forma possíveis ataques às contas dos utilizadores.

Os estudos da "Symantec" são fortemente criticados pelos números que divulgam, contudo continuam a ser uma forte base nas estatísticas relacionadas com a cibercriminalidade, sendo considerado um dos estudos mais completos realizados actualmente sobre este tema.

Um estudo do "Global Economic Crime Survey 2011", da PwC, revela que o cibercrime está entre os quatro primeiros crimes económicos mais frequentes[6], sendo que um terço das organizações mundiais sofreu no ano de 2010/2011 algum tipo de fraude económica e um quarto destas foram alvo de cibercrime.

O estudo incidiu sobre um total de 3.877 inquiridos no seio de 78 países que reconhecem que o cibercrime é uma realidade que está a afectar cada vez mais as empresas e que muitas ameaças derivam do interior daquela. Contudo, apesar de terem noção deste facto, muitas empresas confessam que não têm uma resposta eficaz para combater o cibercrime. Dos inquiridos inseridos neste estudo, 53% referem que o departamento de tecnologias de informação é onde o cibercrime predomina, seguindo-se as operações (39%), departamento de vendas e marketing (34%) e departamento financeiro (32%).

Através desta pesquisa da PwC, foi possível definir o "perfil típico" de um funcionário interno que pratica um cibercrime. As empresas revelam que 85% são colaboradores juniores ou gestores de nível médio, com menos de 40 anos (65%) e fazem parte da organização há menos de cinco anos (50%).

Os países com maior probabilidade de sofrer cibercrime são Hong Kong, China, Índia, Nigéria, Rússia e E.U.A..

Na sua maioria as empresas têm conhecimento quando são alvo de ameaças ou de prática de cibercrimes, contudo 11% dos inquiridos, executivos com cargos importantes, desconhecem se as suas empresas sofreram algum tipo de fraude.

O "2012 Global Security Report" da "Trustwave", aponta que as autoridades no mundo todo detectaram cinco vezes mais violações em 2011 do que em 2010, concluindo que 33% das empresas com violações de dados foram alertadas por órgãos legais, o que representa 7% a mais do que 2010.

Uma investigação levada a cabo por autoridades de vários países, durante cerca de dois anos, (Alemanha, Austrália, EUA, Holanda, Macedónia, Reino Unido, Roménia e Ucrânia) resultou no encerramento de 36 sites que tinham como objectivo a venda de dados pessoais e de cartões de crédito e na detenção de três pessoas, duas de nacionalidade britânica e outra macedónia. Durante esta investigação as autoridades recuperaram 2,5 milhões de dados de cartões de crédito, que se fossem utilizados pelos cibercriminosos poderiam ter gerado lucros de 611 milhões de euros. O responsável pela "Serious Organised Crime Agency" (Soca) - organização britânica envolvida na investigação - revelou que esta operação

[6] Sendo outros o furto ou a apropriação indevida de activos, fraude contabilística e suborno e corrupção

prova que os cibercriminosos "estão a industrializar os seus procedimentos e ao mesmo tempo nós também temos de industrializar os nossos processos para nos equipararmos a eles". Outra preocupação desta organização é a procura de hackers pelos criminosos, com o intuito daqueles escreverem códigos maliciosos para serem utilizados em fraudes online.

- ## Ataques informáticos

Desde o ano de 2012, mais de 400 sites sob o domínio ".pt" já sofreram ataques de "defacement", isto de acordo com o site de notícias de segurança "Zone-H". Entre as entidades alvo de ataques podemos enumerar - câmaras municipais (Vale de Cambra, Santa Comba Dão ou Loulé, por exemplo), juntas de freguesia e governos civis, várias federações (de patinagem ou pesca), o partido CDS, universidades (Aveiro, Lusófona, de Lisboa, Coimbra, Évora, Minho, Porto, ISCTE), várias áreas do site do Centenário da República, escolas na rede científica RCTS, várias organizações não lucrativas (incluindo o causas.sapo.pt), a Academia Militar, Instituto Nacional de Administração, FIL, Tribunal de Contas, UGT ou a embaixada da Argélia em Portugal[7].

No final do ano de 2011, um estudo do "Computerworld" revelou que mais de 1250 sites portugueses foram alvos de ataques, tendo sido os com servidores Linux os mais afectados.

Um estudo realizado em Coimbra, no ano de 2013, conclui que Portugal está bastante vulnerável a ataques informáticos, nomeadamente através de correio electrónico indesejado (SPAM). De acordo com o estudo "ao contrário do que se possa pensar, as mensagens electrónicas não desejadas conhecidas por SPAM podem ser muito perigosas porque são a porta de entrada para vírus e fraudes informáticas com possíveis consequências graves". Acrescente que "A lei, não só não protege os cidadãos e as instituições dos ataques "spam", como ainda pode eventualmente facilitar ataques informáticos de maior impacto, passíveis de gerar danos graves", refere Francisco Rente, investigador e especialista em segurança informática.

Segundo o responsável da empresa tecnológica Dognaedis, criada por especialistas em informática da Universidade de Coimbra, os autores do estudo simularam um ataque de "spam" legal "ultrapassando praticamente todas as barreiras de protecção e de alerta". Para

[7] Cf. Análise do "Zone-H"

que tal acontecesse foram enviadas 60 mil mensagens electrónicas, cujos endereços foram obtidos de fontes públicas legítimas, através de busca na Internet, divididas por três cenários: "dois credíveis - uma sondagem sobre as eleições autárquicas e o caso do norte-americano Edward Snowden, o antigo analista que revelou planos de vigilância da Agência Nacional de Segurança dos EUA - e um "mais inverosímil", relacionado com o aparecimento, no mercado, de um novo medicamento Viagra, contra a disfunção eréctil". O sucesso deste ataque simulado foi de 10%, o que se traduz em seis mil mensagens lidas, semelhante ao que acontece em ataques reais de "spam".

O "spam", só por si, não é o principal causador de danos, mas sim o veículo para que os ataques de maior impacto aconteçam. O "spam" é o "ladrão que fica à porta", sublinha o especialista. Os resultados do estudo foram apresentados, em Lisboa, na "InfosecWeek", iniciativa promovida no âmbito do Mês Europeu de Cibersegurança.

Um site usado por piratas informáticos que tem como principal objectivo expor longos textos com códigos de programação, divulgou um vídeo que demonstra o decorrer de um ataque informático a uma base de dados que gere informações pessoais e de créditos de vários portugueses que detêm um cartão de cliente de uma superfície comercial ("Continente"). Este ataque foi reivindicado pelo grupo "Team Noobz".

Rui Cruz, web designer e fundador do "Tugaleaks", revelou que "os ataques a sites e bases de dados duplicaram em Portugal". Relaciona este fenómeno com "o surgimento do LulzSec Portugal".

- **Grupos de hackers mais conhecidos**

⇒ "**Etical hackers**" – procuram falhas para serem corrigidas

⇒ **"Anonymous"** – Combate todas as manifestações de abuso de autoridade

⇒ **"LulzSec"**– Tem como objectivo encontrar falhas de segurança nos sistemas

- **Tipos de ataques**

⇒ "**DDoS**" - O acrónimo significa "Distributed Denial of Service". A ideia é inundar um sistema informático - o servidor onde se encontra alojado um site de internet - com uma enchente de tráfico de dados, vinda de centenas ou milhares de computadores. A descarga maciça de informação acaba por bloquear o sistema e o site fica offline;

⇒ "**SQL Injection**" - A sigla significa "Structure Query Language". Isto é: Linguagem de consulta estruturada, que é usada para comunicar com bases de dados. Uma

"injection" serve para encontrar vulnerabilidades num sistema e permitir roubar informação (incluindo palavras chaves e dados de cartões de credito) ou colocar conteúdos de forma intrusiva num site;

⇒ "**Brute Force Attack**" - É conhecida como a técnica de aceder a um sistema, tentando todas as palavras-chaves possíveis;

⇒ "**Defacements**" - ataque em que se modifica o conteúdo de um site;

⇒ **"XSS"** – "Cross site secripting" – ataque a dados de página juntamente com "defacement";

⇒ **"Social Engenering"** – "erro humano" – ex. envio de e-mails com um layout, redireccionando para outra página (igual à pagina oficial);

⇒ "**Vírus**" são "**malwares**" (softwares maliciosos) criados com o objectivo de danificar arquivos armazenados no disco rígido (especialmente arquivos críticos para o funcionamento do sistema), tornando o sistema inoperante. "**Worms**" são como os vírus, mas têm a capacidade de se propagar para outros computadores e normalmente, geram um aumento considerável no tráfego de dados, prejudicando o acesso aos serviços de rede, fazendo a sua propagação procurando vulnerabilidades nos sistemas e no correio electrónico;

⇒ "**Spywares**" são programas espiões, usados geralmente com fins comerciais, que permitem o acesso a informação sensível do computador.

⇒ "**Botnets**" é um programa de computador criado para infectar milhares de computadores de forma a realizar ataques informáticos e/ou obter informação dos mesmos. Uma pessoa recebe um e-mail falso, supostamente remetido por uma instituição conhecida, como um banco ou órgão governamental. Aqueles contêm, arquivos maliciosos anexados ou ligados quando o utilizador selecciona um determinado link inserido no texto da correspondência. Aberto o arquivo, um robô ("bot") é instalado no computador do utilizador. Através da Internet, o robô liga o computador a uma rede ("botnets") controlada por um "cracker". Este cibercriminoso consegue, remotamente, controlar os comuputadores dos utilizadores vinculados à rede, obtendo dados como palavras-chaves e números de cartões, furtando arquivos pessoais e dados internos do sistema

- **Ataques ao Estado**

⇒ O Ministério da Educação foi alvo de um ataque que divulgou algumas das suas "passwords".

⇒ Em Agosto de 2012, algumas embaixadas portuguesas - na Alemanha, em Espanha, na Republica Checa - foram vítimas de "defacements"

⇒ A "Parque Escolar" também viu a sua base de dados violada e divulgada pelo mesmo movimento.

⇒ O site do Governo Regional da Madeira, atacado pelo mesmo grupo, lançou um vídeo com o Presidente Regional, Alberto João Jardim, a dizer " Escondi 1113 milhões de euros em dívidas."

- **Ataques ao Patriarcado de Lisboa**

⇒ Em Outubro de 2012, o grupo SideKingdom12 atacou três sites ligados ao patriarcado de Lisboa

- **Ataques à ACAPOR** (Associação do Comercio Audiovisual de Obras Culturais e de Entretenimento de Portugal)

⇒ Em Outubro de 2012, um grupo denominado "Anontuga", invadiu a base de dados da ACAPOR e divulgou uma lista com 335 nomes e passwords internas desta organização.

- **Ataques aos Partidos Políticos**

⇒ O site do PSD de Lisboa foi alvo de ataques pelo menos meia dúzia de vezes entre o fim de 2011 e o verão de 2012. O ataque mais sério levou à divulgação de um ficheiro PDF com os dados de oito mil militantes.

⇒ O PS, em 2011, viu ser colocado no seu próprio site um extracto de uma conta nas ilhas Caimão alegadamente da família de José Sócrates.

- ## Banca Online

Outro dos problemas associados ao uso da internet é a banca ou compras online. Muitos Portugueses, de acordo com um estudo da Comissão Europeia de 2012 afirmam que continuam com receio em utilizar estes serviços, representando 56% dos residentes em Portugal. Apenas 42% se sentem com confiança para usufruir destes tipos de serviço. As razões apuradas para justificar este receio no uso da banca ou compras online, prendem-se

com a preferência na realização de transacções presenciais de serviços e produtos, permitindo um contacto pessoal com colocação de questões, revelam 40% dos entrevistados. Outra das preocupações, é o mau uso que se possa dar aos dados pessoais transmitidos pelos utilizadores destes serviços, afirmam 39%.Os casos de roubo de identidade, de acordo com 69% dos entrevistados, é a maior preocupação em matéria de ameaças quando se utilize a banca online, sendo que 82% receiam que a informação não seja mantida em segurança pelos respectivos sites. Muitos revelam ter sido vítimas de utilização indevida dos seus dados pessoais para realização de compras e também de fraudes online, quando por exemplo na compra de produtos, estes não são entregues ou são entregues outros totalmente diferentes, representando 10% dos entrevistados.

A falta de informação sobre os riscos decorrentes da utilização da internet ronda os 75% dos portugueses, sendo que 87% acreditam que estes aumentaram nos últimos anos, contudo mais de metade (61%) não alteraram as suas palavras passe no último ano e 91% afirma que tenta não fornecer informações online.

As entidades competentes em sede de investigação do cibercrime alertam para um novo tipo de "malware" especializado em roubo de contas bancárias, conhecido como vírus "SpyEye" e "Zeus" que facilita o trabalho aos cibercriminosos, permitindo a transferência de dinheiro de contas bancárias de forma automática, sem que haja qualquer intervenção destes. Esta informação foi dada pela agência Reuters.

O vice-presidente da "Trend Micro", Tom Kellerman, alerta que já foram identificados ataques desta dimensão em instituições financeiras do Reino Unido, Alemanha e Itália, acontecimentos alarmantes, pois os bancos europeus são dos mais cautelosos em matéria de segurança informática.

- ## As redes sociais

Relativamente ao ano de 2011, um estudo da empresa de segurança informática "Kasperskylab", durante uma apresentação de "Novas soluções para o mercado doméstico" revela que em Portugal o cibercrime cresceu 492% e que entre 2009 e 2010, no Mónaco cresceu 670%, países relativamente mais pequenos.

As redes sociais, com o seu "malware", foram referidas como "o novo spam", pois com o elevado fluxo de informação pessoal que aqui é inserido, nomeadamente através de

redes domésticas, onde a protecção é menor, tornam-se mais fácil os ataques e a possibilidade de enviar mensagens que pareçam legitimas.

As redes sociais nem sempre são um aspecto negativo na sociedade de informação, pela facilidade com que o cibercrime pode ser cometido por meio delas. Outras vezes podem até mesmo ajudar na prevenção do crime ou na localização de agentes criminosos. Foi o caso do "Facebook", uma das redes sociais mais conhecidas, que em 2012 ajudou o FBI a desmantelar uma rede internacional de cibercrime, através da identificação das vítimas e criminosos, alegadamente responsáveis por terem infectado onze mil computadores em todo o mundo e de terem extorquido 650 mil euros com a utilização de software malicioso que permitia aceder a informações pessoais, como o número de contas bancárias e cartões de crédito. A investigação resultou na detenção de dez pessoas naturais de diversos países, entre eles Bósnia e Herzegovina, da Croácia, da Macedónia, da Nova Zelândia, do Peru, do Reino Unido e dos EUA.

1.4 O Cibercrime organizado e a cooperação internacional

De acordo com o estudo "Organised Crime in the Digital Age" 80% dos cibercrimes estão ligados a grupos organizados, na sua maioria são formados por jovens (29% deles têm até 25 anos) e homens de uma faixa etária mais elevada (43% estão acima dos 35 anos), com competências técnicas. Não se consegue precisar, em termos geográficos, quais as origens do cibercrime, mas atendendo aos estudos realizados consegue-se identificar que grande parte do software malicioso é desenvolvido em países como a Rússia, ex-países soviéticos e na China.

Os avanços tecnológicos impedem as autoridades de fazerem um acompanhamento eficaz e de as normas jurídicas estarem constantemente actualizadas de acordo com as evoluções que se vão registando. Como tal, verifica-se, de igual modo, uma dificuldade na obtenção de prova destes comportamentos ilícitos.

Como já referido, a internet detém uma característica própria, a extraterritorialidade, que permite a uma pessoa, independentemente, do lugar onde se encontre, disponibilizar conteúdos que ficam acessíveis a qualquer outra pessoa de forma a os descarregar. Esta versatilidade dificulta e muito determinar com exactidão o local onde foram praticados os factos ilícitos, quem os praticou e qual a lei penal e processual aplicável ao caso.

As leis nacionais de cada Estado são de aplicação no seu próprio território, não acompanhando, por isso, a extraterritorialidade da internet, pelo que se impõe que recorram à cooperação internacional.Tomemos como exemplo o caso de alguém invadir o e-mail de uma pessoa, para provar que foi efectuado um acesso ilegítimo, a autoridade competente tem que solicitar os "logs" que comprovam tal acesso. Se por exemplo estiverem num servidor localizado noutro país, será necessário solicitar a esse Estado que obrigue o prestador de acesso a fornecer tal informação, caindo aqui no âmbito da cooperação internacional que nem sempre é de fácil aplicação.

Uma das principais prioridades do FBI é o combate ao terrorismo, contudo, face à evolução que se tem registado no âmbito do cibercrime organizado, "hacktivistas" e intrusões informáticas realizadas por outros países, as atenções desta entidade estão a desenvolver-se rapidamente neste âmbito, tendo já sido criadas "ciberbrigadas" em todas as delegações espalhadas pelo território de forma a monitorizarem os crimes realizados na internet.

Foi inaugurado no inicio deste ano o Centro Europeu da Cibercriminalidade como o intuito de reforçar e melhorar a capacidade da União Europeia na luta contra a

cibercriminalidade e para garantir, de igual forma, uma internet "livre, aberta e mais segura", referiu a Comissária europeia para os assuntos internos, Cecilia Malmstrom.

Este Centro, tem em vista unir conhecimentos e prevenir os crimes que se praticam nesta área. Desta forma as acções levadas a cabo no terreno podem ser mais céleres e eficazes, seja na troca de informação, mobilização de recursos ou peritagens forenses e técnicas quando se trate de uma investigação.

O Centro Europeu da Criminalidade, com o objectivo de combater o cibercrime no seio da União Europeia, é visto pela Comissão Europeia como "o ponto de convergência europeia na luta contra a cibercriminalidade online que incide nas actividades dos grupos criminosos organizados, especialmente os que geram grandes lucros ilegais, como a fraude online através do uso indevido de cartões de crédito e de dados de contas bancárias". Aliado a este objectivo primordial, o centro prevê a protecção dos perfis nas redes sociais, o combate ao roubo de identidades na Internet, o fim da partilha de conteúdos de pornografia infantil online e nos ataques contra infra-estruturas críticas e sistemas de informação comunitários. Por último inclui a emissão de alertas sobre ameaças e falhas nas defesas informáticas dos 27 Estados Membros, a identificação de redes organizadas especializadas neste tipo de criminalidade e a prestação de apoio operacional em investigações.

As instalações do Serviço Europeu da Policia (Europol), localizadas em Haia, vão servir em parte para o funcionamento do centro que vai estar focado, nomeadamente, em questões ligadas a ataques contra sistemas financeiros, infra-estruturas críticas e sistemas de informação da UE, assim como casos de pedofilia online.

A Europol está a liderar uma das maiores consultas internacionais sobre o cibercrime, de forma a ajudar os governos, autoridades e empresas a lidarem com o cibercrime - a consulta está a cargo da "International Cyber Security Protection Alliance". O Project 2020, um estudo daquela entidade tem como objectivo analisar as tendências actuais no cibercrime e como este pode evoluir nos próximos oito anos e junta a City of London Police, a European Network and Information Security Agency ou especialistas do International Information System Security Certification Consortium e da International Association of Public Prosecutors, bem como as empresas Visa Europe, Shop Direct Group, Transactis, Yodel, McAfee, CGI Canada, Atos, Cassidian, Digiware, Core Security Technologies e Trend Micro.

A Europol, preocupada com as tendências verificadas neste âmbito, antecipa três cenários de ameaças preocupantes: - serviços na cloud computing (nuvem); - entidades a

quem se fornece dados pessoais; e - os ataques a equipamentos médicos ou componentes de infra-estruturas de extrema importância.

Em termos de cooperação policial internacional, no âmbito do Gabinete Nacional da Europol, foram abertos 2.727 processos, sendo que 166 estavam relacionados com a criminalidade informática. Na cooperação judiciária, foram abertos 124 processos para este tipo de criminalidade.

A crescente preocupação com a cibercriminalidade tem sido notada a nível internacional, sendo considerada uma das ameaças globais à segurança, tendo sido integrada, no Novo Conceito Estratégico aprovado aquando a Cimeira de Lisboa.

2. Instrumentos Legislativos

2.1 Internacionais

O Pacto Internacional sobre os Direitos Civis e Políticos e a Convenção de Genebra, assim como a Convenção de Budapeste são essenciais em matéria de cibercriminalidade. O Pacto Internacional garante os direitos à privacidade, à liberdade de expressão e sanções contra o incitamento ao ódio, enquanto a Convenção de Genebra dá garantias de direitos em tempo de guerra, mas a Convenção de Budapeste é o instrumento legislativo com aplicação mais imediata. Como vai ser analisado, a Convenção tem como objectivo a harmonização das legislações nacionais, assim como da melhoria das suas técnicas de investigação e aumento da cooperação internacional.

A convenção trata de todas as formas de actividade criminosa online, incluindo violação de direitos autorais, fraude informática, pornografia infantil e violação de segurança das redes.

2.1.1. Convenção sobre o Cibercrime, adoptada em Budapeste a 23 de Novembro de 2001

- ***Objectivo***

Face ao desenvolvimento do Cibercrime, a UE tem vindo a demonstrar a sua preocupação neste domínio, nomeadamente através de instrumentos legislativos que possam adequar a realidade jurídica à realidade informática.

Foi criado o Comité Europeu para os problemas Criminais (CDPC) mediante deliberação CDPC/103/211196, datada de Novembro de 1996, reunindo especialistas para lidar com a questão da cibercriminalidade.

O Comité teve como objectivos analisar as Recomendações nº (89) 9 e (95) 13, no que diz respeito a crimes com computadores e problemas de direito processual, respectivamente; prevenir as infracções cometidas no ciberespaço e responsabilidade dos intervenientes, incluindo os fornecedores de serviços; aplicabilidade de poderes coercivos com carácter transfronteiriço e jurisdições sobre as infracções cometidas; assim como questões de cooperação internacional no âmbito das investigações criminais. Atendendo a

estas preocupações incumbiu ao comité a criação de um instrumento internacional vinculativo.

Na sequência da decisão tomada pelo CDPC, o Comité de Ministros decidiu criar um novo comité, designado por "Comité de Especialistas sobre a Criminalidade no Ciberespaço" (PC-CY) que iniciou os seus trabalhos em Abril de 1997, dedicando-se às negociações relativas a um projecto de convenção internacional sobre o cibercrime.

Desde logo os Ministros da Justiça Europeus demonstraram o seu apoio a estas negociações através da Resolução nº1 adoptada na sua 21º Conferência (Praga, Junho de 1997). Recomendavam a harmonização das legislações nacionais em matéria penal e a utilização de meios de investigação eficazes. Os Estados-Membros da UE expressaram o seu apoio aos trabalhos em desenvolvimento através de uma Posição Comum adoptada em Maio de 1999.

Entre 1997 e 2000 foram realizadas diversas reuniões para finalizar o Memorando Explicativo e revisão do projecto da Convenção, tendo por base o parecer emitido pela Assembleia Parlamentar.

Em Abril de 2000, foi publicada uma versão preliminar do projecto de Convenção, seguindo-se a divulgação das minutas de cada assembleia plenária realizada, a fim de permitir aos Estados participantes a sua consulta.

Em Junho de 2001, o projecto de Convenção e o seu Memorando Explicativo foram terminados e submetidos à aprovação do CDPC que foi posteriormente submetido ao Comité de Ministros a fim de ser adoptado e aberto para assinatura.

A Recomendação nº (89) 9 aproximou os conceitos nacionais, mas não se revelou suficiente. Apenas um instrumento internacional com carácter vinculativo pode garantir a eficácia no combate a estes novos fenómenos.

Surge, assim, a Convenção sobre o Cibercrime com o propósito de responder a estes desafios defendendo os direitos do Homem na Sociedade de Informação em que está inserido. Protegendo a confidencialidade, integridade e disponibilidade de sistemas informáticos, redes e dados, bem como a utilização fraudulenta destes sistemas, reprimindo tais comportamentos e integrando formas de investigação e acção penal.

Teve como objectivo intensificar a cooperação entre os Estados partes, prosseguindo com uma política criminal comum, protegendo a sociedade do cibercrime, adoptando

legislação adequada ao seu combate com o fomento da cooperação internacional[8], de forma rápida e eficaz.

A Convenção sobre o Cibercrime teve em conta outros instrumentos internacionais de grande relevo, que protegem o direito à liberdade de opinião, expressão e o respeito pela vida privada, como por exemplo:

- Convenção para a Protecção dos Direitos do Homem e das Liberdade Fundamentais do Conselho da Europa (1950);
- Pacto Internacional sobre os Direitos Civis e Politicos das Nações Unidas (1966);

Protegeu, igualmente, o direito à protecção de dados pessoais, com referência à:

- Convenção do Conselho da Europa para a Protecção de Pessoas – tratamento automatizado de dados de carácter pessoal (1981);

Atendeu à:

- Convenção das Nações Unidas sobre os Direitos da Criança (1989) e
- Convenção da Organização Internacional do Trabalho sobre as Piores Formas de Trabalho Infantil (1999)

A Convenção pretende ser um complemento a outros instrumentos legislativos em matéria penal, tornando, como se referiu, mais eficazes as investigações e acções penais no âmbito do Cibercrime, melhorando os aspectos da cooperação internacional e tendo em conta outras iniciativas das Nações Unidas, OCDE, União Europeia e G8:

- Recomendação do Comité de Ministros nº (85) 10 - aplicação prática da Convenção Europeia de Auxílio Judiciário Mútuo – cartas rogatórias para a intercepção de telecomunicações;
- Recomendação do Comité de Ministros nº (88) 2 – combate à pirataria no âmbito dos direitos de autor e direitos conexos;
- Recomendação do Comité de Ministros nº (87) 15 – regulamenta a utilização de dados pessoais no sector da polícia;
- Recomendação do Comité de Ministros nº (95) 4 – protecção de dados de carácter pessoal;
- Recomendação do Comité de Ministros nº (89) 9 – estabelece directrizes para os legisladores nacionais na definição dos crimes informáticos;

[8] Cf. Preâmbulo da Convenção sobre o cibercrime

- Recomendação do Comité de Ministros nº (95) 13 – questões processuais;
- Resolução nº1 adoptada pelos Ministros europeus da Justiça na sua 21º Conferência em Praga (1997) que recomenda ao Comité de Ministros o apoio ao trabalho desenvolvido pelo CDPC no domínio do Cibercrime com o intuito de aproximar as legislações nacionais;
- Resolução nº3 adoptada na 23º Conferência dos Ministros europeus da Justiça em Londres (2000) que reforça a necessidade de existir um elevado números de Estados Partes na Convenção do Cibercrime;
- Plano de Acção que foi adoptado pelos Chefes de Estado e de Governo do Conselho da Europa na Segunda Cimeira em Estrasburgo (1997).

- ***A Convenção***

Atendendo às evoluções das tecnologias de informação e as preocupações anteriormente referidas, a Convenção teve como principais objectivos a harmonização do direito penal substantivo e processual de âmbito nacional relativo às infracções cometidas no ciberespaço e poderes necessários para a investigação e propositura de acções penais, assim como de um regime eficaz de cooperação internacional.

A Convenção foi dividida em quatro capítulos:

I – Terminologias

II – Medidas a adoptar a nível nacional no direito penal substantivo e processual

III – Cooperação Internacional

IV – Disposições finais

É definido pela Convenção no seu **Artigo 1º**, em que consiste um sistema informático, dados informatizados, fornecedor de serviços e dados de tráfego, sendo que neste último caso a definição confere a cada parte uma margem no que toca à protecção jurídica a ser dada, consoante a realidade nacional. Contudo, impõe no seu **Artigo 15º**, que aquela seja adequada à protecção dos direitos do Homem.

Assim, considera-se:

- "«Sistema informático» um equipamento ou conjunto de equipamentos interligados ou relacionados entre si que asseguram, isoladamente ou em conjunto, pela execução de um programa, o tratamento automatizado de dados;
- «Dados informáticos» qualquer representação de factos, informações ou conceitos numa forma adequada para o processamento informático, incluindo um programa que permita a um sistema informático executar uma função;
- «Prestador de serviços»: i) Qualquer entidade pública ou privada que faculte aos utilizadores dos seus serviços a possibilidade de comunicarem por meio de um sistema informático; ii) Qualquer outra entidade que processe ou armazene dados informáticos em nome desse serviço de comunicações ou dos seus utilizadores;
- «Dados de tráfego», quaisquer dados informáticos relativos a uma comunicação efectuada por meio de um sistema informático, que foram gerados por um sistema informático enquanto elemento da cadeia de comunicação, e indicam a origem, o destino, o trajecto, a hora, a data, o tamanho e a duração da comunicação, ou o tipo de serviço subjacente."

Pretende-se com este capítulo adequar as legislações nacionais com a determinação de uma norma comum, de forma a possibilitar uma melhor prevenção do crime, assim como uma estatuição semelhante. Evita-se desta forma que ocorra, no caso de um crime aqui previsto, uma transferência para uma parte que possua uma norma menos rigorosa. Foi também considerado neste capítulo a importância de verificação dos requisitos da dupla criminalidade.

De referir que a Convenção teve como objectivo criar normas comuns, não excluindo a possibilidade de cada parte adequar à sua legislação nacional, podendo inclusive excluir as infracções menores do âmbito de aplicação dos **art. 2º a 10º** e até mesmo formular reservas atendendo a determinadas circunstancias (cf. **Art 40º e 42º**).

É de notar que nas infracções a conduta em causa seja seguida "sem que tal direito lhe assista", ou seja, não foi esquecida a exclusão da responsabilidade criminal, como sucede no direito interno como o consentimento ou a necessidade, relevando, aqui, também outros princípios, como por exemplo quando uma parte quer manter a ordem pública, ou mesmo no caso de actividades legítimas respeitantes à concepção de redes, exploração e comércio. Basta que cada parte adeqúe estes princípios à sua legislação.

Os crimes previstos na Convenção deverão ser cometidos com dolo para que seja imputada a responsabilidade criminal, sendo que em alguns casos é exigido um elemento intencional e adicional específico, como se verifica no art. 8º - *Fraude relacionada com computadores*.

- ***Direito penal material***

O capítulo referente ao **direito penal substantivo** (**Art. – 2º a 13º**) define nove tipos de crime agrupados em quatro categorias diferentes, abordando seguidamente a responsabilidade acessória e respectivas sanções.

São considerados crimes, pela Convenção, sendo que cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno:

- **Acesso ilícito – art. 2º** - "quando praticado intencionalmente o acesso ilícito a um sistema informático no seu todo ou a parte dele", seja por violação de medidas de segurança ou através de sistemas informáticos conectados;
- **Intercepção ilícita – art.3º** - "quando praticada intencionalmente, a intercepção não autorizada" elencando as diversas formas em que pode ser realizada a intercepção; seja, igualmente, por violação de medidas de segurança ou através de sistemas informáticos conectados;
- **Dano provocado nos dados – art.4º** - "quando praticados intencionalmente, a danificação, o apagamento, a deterioração, a alteração ou supressão não autorizados de dados informáticos";
- **Sabotagem informática – art. 5º** - "quando praticada intencionalmente, a perturbação grave, não autorizada, do funcionamento de um sistema informático mediante inserção, transmissão, danificação, eliminação, deterioração, alteração ou supressão de dados informáticos"
- **Utilização indevida de dispositivos – art.6º** - "quando praticadas intencional e ilicitamente: a)A produção, venda, aquisição para efeitos de utilização, importação, distribuição, ou outras formas de disponibilização" de um dispositivo ou uma palavra passe. B) A posse de um destes elementos com o objectivo de praticar um dos crimes previstos no art. 2º a 5º. Exceptua-se a criminalização nos testes autorizados ou a protecção de

um sistema informático. As partes podem formular reserva de não aplicação do nº1 do art. 6º, desde que não diga respeito à alínea a), ii).

- **Falsificação informática – art. 7º** - "quando praticadas intencional e ilicitamente, a introdução, a alteração, o apagamento ou a supressão de dados informáticos dos quais resultem dados não autênticos, com o intuito de que esses dados sejam considerados ou utilizados para fins legais como se fossem autênticos", podendo existir ou não intenção fraudulenta;
- **Burla informática – art. 8º** - "quando praticado intencional e ilicitamente, o prejuízo patrimonial causado a outra pessoa por meio de: a) Qualquer introdução, alteração, apagamento ou supressão de dados informáticos; b) Qualquer interferência no funcionamento de um sistema informático; com intenção de obter para si ou para outra pessoa um benefício económico ilegítimo"
- **Infracções relacionadas com pornografia infantil – art. 9** – "quando praticadas de forma intencional e ilegítima, as seguintes condutas", através de um sistema informático: a) Produção de pornografia infantil com o propósito de a divulgar; b) Oferta ou disponibilização de pornografia infantil; c) Difusão ou transmissão de pornografia infantil; d) Obtenção para si ou para outra pessoa de pornografia infantil; e) Posse de pornografia infantil; "a expressão «pornografia infantil» deverá abranger todo o material pornográfico que represente visualmente: a) Um menor envolvido em comportamentos sexualmente explícitos; b) Uma pessoa com aspecto de menor envolvida em comportamentos sexualmente explícitos; c) Imagens realistas de um menor envolvido em comportamentos sexualmente explícitos; a expressão «menor» deverá abranger qualquer pessoa com menos de 18 anos de idade. Qualquer uma das Partes pode impor um limite de idade inferior, não podendo, contudo, ser fixado abaixo dos 16 anos." Poderá existir reserva da Parte no todo ou em parte nas alíneas d) e e) do nº1 e b) e c) do nº2.
- **Infracções relacionadas com a violação dos direitos de autor e direitos conexos – art. 10º** - quando exista "as violações do direito de autor, tal como estas se encontram definidas na lei dessa Parte" ou "violações dos direitos conexos tal como estas se encontram definidas na lei dessa Parte" quando tais actos são praticados de forma intencional, para fins comerciais e por meio de um sistema informático. A Parte pode formular reserva ao nº1 e 2º desde que respeite os instrumentos internacionais a que se encontra vinculada.

O **art. 11º** da CCib - **Tentativa, auxílio ou instigação** - vem impor que os Estados partes adoptem medidas para "classificar como infracções penais, nos termos do seu direito interno, o auxílio ou a instigação à prática de qualquer uma das infracções previstas nos artigos 2.º a 10.º da presente Convenção, quando praticados intencionalmente tendo em vista a prática dessa infracção" (nº1) e ainda, " a tentativa deliberada de praticar qualquer uma das infracções previstas nos artigos 3.º a 5.º , 7.º, 8.º e nas alíneas a) e c) do n.º 1 do artigo 9.º da presente Convenção (nº2). Cada parte tem o direito a formular reserva quanto ao nº2.

A **responsabilidade das pessoas colectivas**, previstas no **art. 12º** da CCib, será abordada no capítulo referente à responsabilidade penal das pessoas colectivas, para onde é remetido este tema.

A parte dedicada às disposições materiais termina com o **art. 13º - sanções e medidas** - obrigando a cada parte a punir com "sanções eficazes, proporcionais e dissuasivas" os crimes cometidos ao abrigo dos ars. 2º a 11º, inclusive as pessoas colectivas, sejam as sanções de natureza penal ou não e pecuniárias.

A Convenção agrupou os tipos de crime em diferentes títulos, sendo que:

- **Titulo I** – crimes relacionados com computadores; crimes que atentam contra a confidencialidade, a integridade e disponibilidade dos sistemas informáticos e dos dados informatizados, ou seja, crimes de acesso não autorizado e manipulação ilícita de sistemas, programas ou dados – **Art. 2º a 6º**
- **Titulo II** – outros crimes relacionados com computadores - prevenir que os meios tradicionais ilegais se cometam através de computadores – **Art. 7º e 8º**
- **Titulo III** – crimes relacionados com o conteúdo – produção ou distribuição ilícita de pornografia infantil por meio da utilização de sistemas informáticos – **Art. 9º**
- **Titulo IV** – crimes relacionados com a violação dos direitos de autor e dos direitos conexos – **Art. 10º**
- **Titulo V** – disposições sobre tentativa, auxilio e cumplicidade, sanções e medidas – **Art. 11º a 13º**

- ***Direito processual penal***

As medidas de **direito processual** previstas na Convenção têm como objectivo facilitar e promover uma melhor investigação criminal, relativamente às infracções constantes

no direito penal substantivo, mas também a outras cometidas por meio de um sistema informático e à recolha de provas sob a forma electrónica. Podemos assim considerar que, a nível nacional, as partes deverão adoptar medidas de direito processual que se apliquem a:

- Crimes previstos no Capitulo II, secção I
- Crimes cometidos por meio de um sistema informático
- Recolha de provas sob forma electrónica

Os procedimentos referidos nesta secção abrangem todo o tipo de dados, incluindo três tipos específicos de dados informatizados:

- Dados de tráfego
- Dados de conteúdo
- Dados relativos aos subscritores

Os quais podem existir sob duas formas:

- Armazenados
- Presentes no processo de comunicação

As questões de direito processual, a que a Convenção faz referência, viabilizando a obtenção ou recolha de dados para fins de investigação criminal, aplicam-se a qualquer infracção cometida por meio de um sistema informático ou à prova da mesma existindo esta ultima sob forma electrónica, adaptando os meios de obtenção de prova clássicos, como a busca e apreensão, determinando as condições de aplicabilidade e poderes processuais:

- **Preservação/Conservação expedita de dados informatizados armazenados – art. 16º**
- **Preservação/Conservação expedita e divulgação parcial de dados de tráfego – art. 17º**
- **Injunção de comunicar/ Ordem de produção – art. 18º**
- **Investigação e apreensão de dados informatizados – art. 19º**
- **Recolha de dados de tráfego em tempo real – art. 20º**
- **Intercepção de dados de conteúdo – art. 21º**
- **Jurisdição – art. 22º**

Como referido anteriormente, a revolução operada nas novas tecnologias, introduziu alterações nas redes de comunicação que permanecem constantemente em expansão, abrindo novos caminhos à prática de crimes. Um grande desafio que se coloca é a identificação da pessoa que cometeu a infracção, assim como, do impacto que a mesma teve. Contudo, não é o único problema associado aos crimes cometidos através das novas tecnologias. A versatilidade dos dados electrónicos permite que estes sejam alterados, transferidos ou eliminados em fracções de segundos.

Atendendo a estas novas problemáticas a Convenção preocupou-se com um combate à cibercriminalidade através de uma investigação criminal eficaz que pudesse conduzir ao êxito da mesma. As medidas tradicionais foram adaptadas aos novos meios tecnológicos dando origem a novas medidas que garantissem a eficácia da investigação.

Qualquer artigo desta secção faz referência às "autoridades competentes" considerando-se como tal qualquer autoridade judicial, administrativa ou outra que zele pela aplicação da lei e se encontre, ao abrigo dos poderes concedidos pelo direito interno, que permita ordenar, autorizar, ou executar as medidas processuais previstas.

Esta secção inicia-se com disposições comuns que são aplicáveis a qualquer artigo que preveja uma medida processual – **Art. 14º e 15º.**

O **art. 14º** sob a epígrafe "**Âmbito de aplicação das disposições processuais**", obriga a que as partes adoptem as medidas legislativas necessárias a estipular os poderes e procedimentos previstos nesta secção para fins de investigação criminal ou acções penais específicas, atendendo às infracções previstas na Convenção, a outras infracções cometidas por meio de um sistema informático, e à recolha de prova sob a forma electrónica relativamente a uma infracção penal.

Existem, contudo, duas excepções a este âmbito de aplicação. A primeira prevista no **art. 21º** ("**Intercepção de dados de conteúdo**") estabelece que o poder de intercepção de dados de conteúdo deverá ser limitado a um conjunto de infracções graves a ser determinado pela legislação nacional, pois esta medida é considerada por muitos Estados invasiva da privacidade.

A segunda excepção permite que a parte reserve o direito de aplicar as medidas prescritas pelo **art. 20º** ("**Recolha, em tempo real, de dados de tráfego**") somente às infracções ou categorias de infracções especificadas na reserva formulada, desde que estas não sejam mais restritas do que as de aplicação do art. 21º. Muitos Estados consideram ambas

as medidas como invasivas da privacidade adoptando para ambas o mesmo conjunto de infracções. Contudo, outros Estados não consideram estas medidas com o mesmo nível, pois a recolha de dados de tráfego, não recolhe nem divulga por si só o conteúdo da comunicação. Diferentemente a recolha em tempo real poderá revelar a origem e destino das comunicações. Como tal a Convenção permite que as partes "exerçam o seu direito de reserva a limitarem a mesma, de forma a permitir a aplicação tão alargada quanto possível, dos poderes e procedimentos definidos para a recolha, em tempo real, dos dados de tráfego"

É de referir que a aplicação das medidas processuais previstas na Convenção estão sujeitas às condições e salvaguardas previstas no **art. 15 "Condições e garantias".** Embora as partes adoptem estes poderes e procedimentos processuais, fica na sua esfera jurídica a implementação das definições e aplicação daqueles, devendo sempre existir um equilibro entre os requisitos de aplicação da lei e a protecção dos direitos fundamentais do homem. Isto devido à diversidade de sistemas jurídicos e princípios existentes entre os Estados participantes. Existem algumas normas comuns ou salvaguardas mínimas a que as partes devem de aderir, decorrentes das obrigações assumidas perante instrumentos internacionais, como é o caso da Convenção do Conselho da Europa para a Protecção dos Direitos do Homem e Liberdades Fundamentais dos Cidadãos, datada de 1950, assim como dos seus protocolos adicionais, Convenção Americana sobre os Direitos do Homem, 1969, Carta Africana dos Direito do Homem e dos Povos, 1981 e Pacto Internacional relativo aos Direitos Civis e Políticos, sem nunca esquecer a Declaração Universal dos Direito do Homem.

Uma outra salvaguarda exigida pela Convenção prende-se com a exigência das medidas – poderes e procedimentos processuais – integrarem o princípio da proporcionalidade de acordo com o direito interno de cada parte, como por exemplo no que diz respeito à intercepção de dados no equilíbrio entre a intrusão na privacidade, atendendo às infracções graves cometidas, como referido anteriormente.É igualmente exigido que as condições e salvaguardas respeitantes ao direito processual sejam supervisionadas por um órgão independente.

- **Preservação/conservação expedita de dados informatizados armazenados – Art. 16**

Aplicam-se a dados de tráfego armazenados que foram já recolhidos e arquivados pelos detentores de dados, como por exemplo os fornecedores de serviços. São dados informatizados já existentes e em curso de armazenamento. Convém, porém, distinguir entre

Preservação de dados e Arquivamento de dados. O primeiro significa manter os dados que já existem e estão armazenados, protegidos de qualquer alteração ou deterioração. O segundo significa guardar e manter na sua posse para o futuro e durante um período de tempo dados cuja produção se encontra em curso. Esta distinção revela-se importante pois os artigos 16º e 17º referem-se apenas à preservação de dados por meio de um sistema informático, pressupondo a pré-existência de dados, a sua recolha e armazenamento.

Para que se proceda à preservação de dados, as partes devem emitir uma ordem, no âmbito de uma investigação criminal ou acção penal específica, referente a "dados específicos informatizados e armazenados, que se encontrem na posse ou sob o controlo de uma pessoa" (art. 16º) durante um período de tempo até à sua divulgação.

É de notar na legislação nacional de muitos Estados a imposição aos detentores de dados que os dados de carácter pessoal não sejam arquivados mas sim apagados, nos casos em que não exista um objectivo comercial que justifique o arquivamento daqueles. Na União Europeia podemos referir a **Directiva 95/46/CE e a Directiva 97/66/CE** que determinam a eliminação dos dados quando o seu armazenamento não se mostre necessário. Contudo, cada Estado poderá formular excepções a este princípio, atendendo aos objectivos e fins das investigações criminais, como prevenção e repressão das infracções cometidas.

A preservação de dados reveste uma importância extrema nas investigações, pois impede que aqueles se alterem ou se eliminem. Dado ao carácter volátil destes dados, caso não se proceda à sua preservação, as provas poderão ser facilmente perdidas.

Para os órgãos incumbidos de proceder à investigação criminal, muitas vezes, a melhor forma de preservar a integridade dos dados é proceder à sua busca ou apreensão. Esta medida mais rígida, pode ser contornada por exemplo nos casos em que o detentor dos dados seja de confiança ou uma empresa reconhecida e com nome. Nestes casos as autoridades competentes procedem à emissão de uma ordem de preservação de dados, evitando um impacto negativo na empresa e diminuindo os prejuízos que poderão advir para a sua reputação.

Tendo em conta que os crimes relacionados com computadores são praticados mediante a transmissão de comunicações por meio informático, comunicações estas de conteúdo ilegal, torna-se importante identificar a origem e destino destas, de forma a identificar o infractor. Acresce que nestes casos, as provas, como o conteúdo das comunicações ou conteúdo dos próprios actos, deverão ser conservados pelos fornecedores de

serviços, de forma a garantir que as de cariz relevante não são perdidas, como por exemplo as mensagens de correio electrónico.

Face à importância que a preservação de dados num âmbito de uma investigação criminal ou acção penal específica pode ter, as partes devem implementar um poder que permita a emissão de uma ordem de preservação de dados informáticosespecificados (deve constar da ordem que tipo de dados devem ser preservados), enquanto medida provisória (pois aguarda-se a execução de outras medidas jurídicas para obtenção ou divulgação de dados), durante um período de tempo (a ordem deve fazer referencia ao período de tempo exacto - prazo máximo de 90 dias passível de ser renovado) a fim de mais tarde serem divulgados. Cabe a cada parte determinar a forma de preservação de dados e determinar se estes devem ou não permanecer intactos (se tal não acontecer, os utilizadores legítimos poderão continuar a aceder aos dados). De notar que nem todos os Estados dispõem de meios para a preservação de dados, pelo que, em muitos casos esta pode ser feita mediante a busca, apreensão ou ordem de produção. Esta preservação de dados poderá incidir sobre qualquer tipo de dados que seja especificado na ordem, sejam estes dados comerciais, médicos ou pessoais.

A aplicação das medidas de preservação deverá atender sempre às condições particulares dos dados, visto que, muitos fornecedores de serviços procedem à sua eliminação decorrido algum tempo, devido às suas políticas comerciais, ou até mesmo pelo facto do suporte de armazenamento ser necessário para o registo de outros dados.

Sob o fornecedor de serviço ou pessoa que receba a ordem de preservação de dados recai um dever de confidencialidade, durante um período de tempo, relativamente à execução dos procedimentos, para que o alvo da investigação não tome conhecimento da mesma e para garantir, igualmente, o seu direito à privacidade.

Não esquecer que os poderes e procedimentos previstos no art. 16º estão sujeitos às condições e salvaguardas dos art. 14º e 15º.

- **Preservação/conservação expedita e divulgação parcial de dados de tráfego – art.17º** (remete-nos para os arts. 14º, 15º, 16º)

É aqui definido obrigações especificas relativamente à preservação de dados constante no art. 16º, prevendo igualmente a divulgação expedita de determinados dados de tráfego com o objectivo de determinar se estiveram envolvidos outros fornecedores de serviços na transmissão das comunicações especificadas.

Como já mencionado, a obtenção de dados de tráfego armazenados que estejam associados a comunicações anteriormente feitas, poderá ser de extrema importância para a identificação do infractor, assim como da origem e destino da comunicação. Tendo em conta que estes dados podem ser armazenados por curtos períodos de tempo, dado que as leis destinadas a proteger a privacidade poderão proibir o armazenamento de longa duração, é importante perceber se existe mais algum interveniente. Pode acontecer que na transmissão da comunicação participe mais que um fornecedor de serviço, o que se poderá traduzir na detenção repartida de dados de tráfego, pois muitas vezes estes são partilhados por aqueles para fins comerciais, técnicos ou de segurança. Assim, nestes casos, mais que um fornecedor de serviço poderá deter informações relevantes sobre a origem ou destino da comunicação que se quer investigar.

Este artigo prevê as situações em que os dados de tráfego são repartidos entre fornecedores de serviços, onde cada um detém uma parte importante para a detecção de toda a comunicação. Assim, possibilita a que se proceda a uma preservação expedita dos dados de tráfego junto de cada um dos referidos fornecedores de serviços, não determinando, contudo, os meios através dos quais devera ser realizada, cabendo as partes faze-lo atendendo ao seu sistema jurídico e económico. Poderá consistir na emissão de uma ordem dirigida a cada um dos fornecedores, numa notificação sucessiva ou na obrigatoriedade do primeiro fornecedor que a receba notificar o próximo.

Assim que o fornecedor receber a notificação de uma ordem de preservação expedita de dados, deve de imediato proceder à sua divulgação junto das autoridades competentes, de uma quantidade suficiente de dados de tráfego de forma a permitir a identificação de outros fornecedores de serviços, bem como o rumo da comunicação transmitida.

- **Injunção de comunicar / ordem de produção – art. 18º**

(remete-nos para os art. 14º e 15º)

A ordem de produção prevista no art. 18º consiste na emissão de uma ordem que investe as autoridades competentes de poderes necessários para obrigar uma pessoa que se encontre no seu território a fornecer os dados armazenados especificados ou um fornecedor de serviços que ofereça os seus serviços no território da parte, a prestar informações relativas aos subscritores (dados informatizados ou informações). A expressão "posse ou controlo" refere-se à informação relativa aos subscritores que se encontre na posse física do fornecedor de serviços ou armazenada à distância mas sob o controlo daquele, abrangendo toda e qualquer

informação do subscritor detida pelo fornecedor de serviços. Trata-se de uma medida menos coerciva, evitando outros meios como a apreensão ou busca, e que se revela benéfico para os administradores de dados, como os fornecedores de serviços de Internet (ISP), colaborando voluntariamente com as autoridades competentes, evitando qualquer responsabilidade contratual ou não contratual decorrente da investigação.

As modalidades de produção desta ordem estão à disposição das partes, podendo referir o momento em que a divulgação ocorrerá e como deve a mesma ser feita, se através de texto, forma on-line, impresso ou em disquete.

- **Busca e apreensão de dados informáticos armazenados – art. 19º**

A busca (procura, leitura, inspecção – pesquisa e analise de dados) e apreensão (terminologia informática) diz respeito a dados já existentes e que permitem reunir provas de uma determinada infracção. As legislações nacionais já dispõem de disposições processuais sobre a busca e apreensão, contudo estas dizem respeito a dados tangíveis. Como os dados informatizados armazenados podem não ser tangíveis, o art. 19º pretende estabelecer um poder equivalente, permitindo a mesma eficácia na investigação. O suporte físico onde se encontram armazenados os dados intangíveis (ex. disco rígido) deverá ser apreendido e retirado do local, ou ser feita uma copia sob a forma tangível (ex. impressão) ou sob a forma intangível (ex. disquete). Nestes casos em que são efectuadas cópias, deverão as partes instituir um poder relativo à realização das mesmas. Existem casos em que os dados não se encontram no computador alvo de busca, mas são acessíveis a partir deste, sendo necessária a implementação de novas medidas que permitam a extensão destas medidas processuais ao sistema em que os dados se encontram efectivamente armazenados.

É permitido no art. 19º a delegação de poderes às autoridades competentes para apreender, ou de forma semelhante, adquirir e guardar os dados informatizados alvo de busca e acesso, que se encontram em suporte informático e em suporte de armazenamento de dados informatizados. Refira-se que apreender consiste em transportar para fora do local em questão o suporte físico onde os dados foram registados ou efectuar e guardar uma cópia.

Assim, a apreensão consiste em:

⇒ Reunir provas, por meio da realização de cópias dos dados

⇒ Confiscar dados, efectuando cópias dos mesmos e bloqueando o acesso aos originais.

Esta disposição processual obriga a um administrador de sistema a colaborar em tudo o que se afigure necessário na operação de busca e apreensão, evitando uma sobrecarga em termos económicos para as empresas ou para os subscritores enquanto os dados tivessem inacessíveis. Esta obrigação de colaborar isenta o fornecedor de serviços de quaisquer responsabilidades na divulgação de dados.

- **Recolha de dados informatizados em tempo real – art. 20º e 21º**

É aqui previsto a recolha em tempo real de dados de tráfego e da intercepção em tempo real de dados de conteúdo associados a comunicações específicas transmitidas por meio de um sistema informático normalmente os meios tradicionais de telecomunicações (cabo, fibra, redes sem fios, sistemas telefónicos moveis etc.)

Permite-se, desta forma, a recolha e intercepção pelas autoridades competentes e pelos fornecedores de serviços, das comunicações específicas transmitidas por meio de um sistema informático, antes mesmo de ser recebida por outro sistema. É de notar o importante papel dos fornecedores de serviços – nesta matéria, pois são eles que possibilitam a comunicação por meio de um sistema informático.

O presente artigo reporta-se às comunicações em curso de produção, sendo que a recolha acontece aquando a transmissão da comunicação – tempo real – não interferindo na dita comunicação que chega da mesma forma ao destinatário.

Podem ser recolhidos dois tipos de dados:

- *Dados de tráfego* – qualquer dado informatizado relacionado com uma comunicação feita mediante um sistema informático no qual se refere a origem, destino, caminho, hora e data, dimensão;

- *Dados de conteúdo* – conteúdo informativo da comunicação; teor e significado da comunicação.

Os requisitos exigidos por lei para aplicação desta medida de recolha bem como as infracções em que é possível recorrer é basicamente igual nos dois casos, diferindo apenas no que respeita à intercepção de dados de conteúdo onde as partes deverão instituir um conjunto de infracções graves, pois no que respeita aos dados de tráfego será, em princípio, aplicável a qualquer infracção abrangida pela Convenção. No primeiro caso e devido ao elevado grau de intrusão na vida privada, devem ser criadas salvaguardas que imponham o equilíbrio entre os interesses da investigação e os direitos fundamentais do Homem, como por exemplo a

supervisão por parte de um órgão judiciário, especificidade das comunicações ou das pessoas alvo da intercepção; necessidade, subsidiariedade e proporcionalidade.

- **Recolha de dados de tráfego em tempo real – art. 20º**

(remete-nos para os arts. 14º e 15º)

Como já foi referido anteriormente, os dados de tráfego podem sofrer alterações ou mesmo serem eliminados, dai a importância de os recolher em tempo real, impossibilitando qualquer modificação. Permitem, pois, a identificação de origem e destino (ex. números de telefone, numa chamada telefónica), e dos dados conexos (hora, data, duração por exemplo da intrusão no sistema da vitima) de comunicações que forneçam provas de um crime, assim como dos seus cúmplices, realizadas no seio do território de uma parte.

A ordem, proveniente de autoridade investida de poderes, que autorize a recolha deverá especificar quais as comunicações em que os dados de tráfego devem ser recolhidos.

As autoridades podem, igualmente, obrigar um fornecedor de serviços a recolher ou registar dados de tráfego ou exigir que este colabore e apoie aquelas em tudo o que for necessário para a execução da medida de recolha ou registo dos dados.

Como foi mencionado acerca de outras medidas processuais, é exigido aos fornecedores de serviços e à pessoa que recolha os dados, confidencialidade, pois a medida só será eficaz se não for do conhecimento da pessoa visada. Tem a Parte legitimidade para impor medidas adicionais para obrigar à confidencialidade ou à não divulgação de informação sobre que estão a ser alvo, como por exemplo através de processo penal por obstrução à justiça.

- **Intercepção de dados de conteúdo – art. 21º**

(remete-nos para os arts. 14º e 15º)

A intercepção de dados de conteúdo revela-se desde sempre importante para determinar se a comunicação é ferida de carácter ilícito, bem como para reunir provas de crimes passados ou futuros. Sendo possível, devido à tecnologia informática, transmitir grandes quantidades de dados, como imagens, som, texto, e aceder ilicitamente a sistemas informáticos, impõem-se uma medida que consiga fazer face a estes acontecimentos em tempo real. Se tal não for possível, caía por terra qualquer investigação que não se reportasse a crimes passados. Muitas vezes só é possível combater eficazmente contra a criminalidade através da intercepção de comunicações em tempo real.

É aqui aplicável tudo que foi dito relativamente à recolha de dados de tráfego – obrigação de colaboração e prestação de apoio por parte dos fornecedores de serviços, assim como do dever de confidencialidade. É contudo de realçar o facto desta medida só ser aplicável a determinadas infracções graves definidas por legislação nacional.

- **Jurisdição –art. 22º**

São aqui definidos critérios segundo os quais as partes ficam obrigadas a estipular a sua jurisdição relativamente às infracções penais constantes dos art. 2º a 11º da Convenção.

Parágrafo 1 a) – *Princípio da territorialidade* – Cada parte fica obrigada a punir a prática dos crimes previstos na Convenção quando estes sejam cometidos dentro do seu território – seja a pessoa ou sistema.

Parágrafo 1 b) e c) – *Variante do princípio da territorialidade* – Cada parte deverá estipular uma jurisdição penal relativamente a infracções cometidas a bordo de um navio ou avião de sua propriedade.

Parágrafo 1 d) – *Princípio da nacionalidade* – os cidadãos de um Estado obrigar-se-ão a respeitar a legislação nacional mesmo encontrando-se fora do seu território.

Parágrafo 2 – possibilidade das partes formularem reservas relativamente às bases de jurisdição previstas no parágrafo 1, com excepção da prevista na a).

- ***Cooperação internacional***

A Convenção preocupou-se, igualmente, com a **cooperação internacional**, prevendo no seu capítulo III a assistência mútua em caso de crimes tradicionais e crimes informáticos, assim como no que diz respeito à matéria de extradição. Vem regular a assistência mútua tradicional quando não existe uma base jurídica entre as partes, como um tratado, legislação idêntica, aplicando-se nesta medida as regras constantes na Convenção. Por outro lado, quando a referida base jurídica existe deverá ser, também, aplicável à assistência prestada ao abrigo da Convenção.

Este capítulo prevê, ainda, o acesso transfronteiriço a dados informatizados armazenados, assim como a constituição de uma rede 24/7, que consiste em assegurar a assistência entre as partes, vinte e quatro horas por dia, 7 dias por semana.

A cooperação internacional entre as Partes deve ter um âmbito alargado, para que aquelas cooperem eficazmente e diminuam os obstáculos que possam surgir na troca de informação e de provas a nível internacional.

O **art. 23º** da Convenção sob a epígrafe " **Princípios gerais relativos à cooperação internacional**" define o âmbito em que assenta a cooperação entre as partes. Deve abranger todas as infracções penais relacionadas com sistemas informáticos e dados informatizados – Art. 14º, parágrafo 2 a) e b) – assim como à recolha de provas sob a forma electrónica sobre uma infracção penal especifica.

É, contudo, permitido às partes nos **artigos 24º** (**Extradição**), **33º** (**Assistência Mútua relativamente à intercepção de dados de tráfego em tempo real**) e 34º (**Assistência Mútua relativamente à intercepção de dados de conteúdo**), que introduzam alterações no que diz respeito à aplicação destas medidas.

Refira-se que a cooperação internacional prevista na Convenção deve ser realizada em conformidade com outros instrumentos internacionais legislativos e com o direito interno de cada Parte.

Como referido, a cooperação deve ter um âmbito alargado, assim deve, igualmente sê-lo a assistência mútua e como tal deve abranger as mesmas infracções previstas para a cooperação internacional e respeitar os restantes normativos internacionais – **art. 25º** "**Princípios gerais relativos à assistência mútua**". As partes devem, no seu sistema jurídico, dispor dos meios necessários para levar a cabo as medidas de assistência mútua, principalmente dos mencionados nos arts. 29º a 35º.

A volatilidade dos dados informáticos que facilmente são eliminados, modificados ou armazenados por curtos períodos de tempo exigem que os pedidos e respostas de assistência mútua sejam céleres, de modo a que as provas não se percam. O parágrafo 3º do art. 25º aponta duas formas de atingir a eficácia nas investigações que exijam a colaboração entre as Partes:

- Investir as Partes de poderes necessários para emitir pedidos urgentes de cooperação através do recurso a meios de comunicação expeditos, em vez dos tradicionais (documentos escritos, selados, correio postal etc);
- Solicitar às Partes as respostas pelos mesmos meios expeditos

Poderá ser acordado a forma de autenticidade as comunicações bem como determinar se é exigida uma protecção especial de segurança e se necessário receber confirmação do pedido pelos meios tradicionais.

A assistência mútua encontra-se sujeita aos termos e condições das legislações internas e aos tratados de assistência mútua já celebrados que prevêem salvaguardas relativamente aos direitos de uma pessoa que se encontre no território da parte requerida e possam ser objecto de um pedido de assistência mútua. No caso de uma medida de apreensão e busca, esta não será executada a pedido da Parte requerente se não for também admissível no sistema jurídico da Parte requerida.

O parágrafo 4º do mencionado artigo ressalva casos em que as disposições da Convenção deverão ser sempre aplicáveis independentemente de instrumentos já existentes de assistência mútua entre as partes.

A dupla criminalidade pode ser uma condição necessária para prestação de assistência, ou seja, a conduta subsumível ao tipo de crime punível pela Parte requerente, deverá ser considerada como tal à luz da legislação da Parte requerida. Isto, porque, existem muitos sistemas jurídicos que diferem entre si, sendo que esta exigência poderá facilitar em muito a assistência prestada.

São previstos para o auxílio mútuo:

- **Informação espontânea – art. 26º** - transmitir a outra parte informações (sem pedido prévio) obtidas no âmbito das investigações nacionais, sempre que se ache necessário à outra parte para investigações ou procedimentos previstos na Convenção;
- **Procedimentos relativos a pedidos de assistência mútua em caso de inexistência de acordos internacionais aplicáveis – art. 27º** - no caso daquela inexistência aplicam-se os nº 2 a 9 deste art.; caso exista acordo, as partes podem decidir livremente aplicar o presente art.; - existência de autoridades competentes responsáveis pelos pedidos de auxilio, executados em conformidade com o requerido pela outra parte, podendo o auxilio ser recusado com base no art. 25º nº4 ou nº4 do art. 27º, ou adiado;
- **Confidencialidade e limitação de utilização – art. 28º** - a comunicação de informações pode ser sujeita a confidencialidade e não ser usada para outros fins que não os elencados no pedido;
- **Preservação/Conservação expedita de dados informáticos armazenados** – art. **29º** - pedido de uma parte para que a outra conserve dados armazenados através de um sistema informático situado no território dessa outra parte, com o intuito de proceder a um pedido de auxilio para busca ou outro acesso, apreensão, ou divulgação.

- **Divulgação expedita dos dados de tráfego preservados/conservados – art. 30º** - quando a parte encarregue da conservação expedita de dados (art.29º) toma conhecimento que existem outros fornecedores de serviço, presta essa informação à parte requerente disponibilizando os dados de tráfego necessários para a identificação daquele, assim como do trajecto utilizado para a transmissão da comunicação.
- **Auxílio mútuo relativamente ao acesso a dados informáticos armazenados** – art. 31º - uma parte solicita à outra a busca, apreensão, ou divulgação de dados armazenados através de um sistema informático situado no território desta, incluindo os dados conservados.
- **Acesso transfronteiriço a dados informáticos armazenados com autorização ou quando disponíveis ao publico** – art. 32º - uma parte pode, sem autorização da outra, aceder a dados informáticos acessíveis ao público (independentemente da sua localização geográfica), ou através de sistema informático situado no seu território, aceder a dados situados fora daquele, com o consentimento legal ou voluntário de quem de direito.
- **Auxílio mútuo relativamente à recolha de dados de tráfego em tempo real** – art. 33º - deverá ser garantido o auxílio mútuo entre as partes para a recolha em tempo real de dados de tráfego de "comunicações especificas transmitidas no seu território por meio de um sistema informático", atendendo às disposições do direito interno sobre esta matéria.
- **Auxílio mútuo relativamente à intercepção de dados de conteúdo** – art. 34º - auxilio prestado entre as partes para recolha ou registo em tempo real de dados relacionados com o conteúdo das comunicações especificas.
- **Rede 24/7** – art. 35º - ponto de contacto assegurado por cada parte, disponível 24 horas por dia, 7 dias por semana, que garante a prestação de auxílio nas investigações e procedimentos relativos às "infracções penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma elecrónica", obedecendo a critérios estabelecidos pela CC e lei interna.

2.1.2.Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adoptado em Estrasburgo em 28 de Janeiro de 2003

- ***O Entendimento***

Respeitando a legislação interna de cada Estado, assim como a liberdade de expressão, impondo-se um equilíbrio entra este e os actos de natureza racista ou xenófoba e aproveitando a convenção do Cibercrime no que respeita aos meios de cooperação internacional, com propósito de harmonizar as legislações, surgiu o protocolo adicional à Convenção sobre o Cibercrime e tem em conta os seguintes instrumentos:

- Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais e o seu Protocolo n.º 12 sobre a proibição geral de discriminação;
- Convenção sobre o Cibercrime;
- Convenção Internacional das Nações Unidas sobre a Eliminação de Todas as Formas de Discriminação Racial, assinada em 21 de Dezembro de 1965;
- Acção Comum da União Europeia, de 15 de Julho de 1996;
- Plano de Acção, adoptado pelos Chefes de Estado e de Governo do Conselho da Europa por ocasião da sua Segunda Cimeira (Estrasburgo, 10 e 11 de Outubro de 1997,

- ***O Protocolo***

O **art. 1º**, sob a epígrafe "**objecto"**, inserido no Capítulo referente às disposições comuns, dispõe que o Protocolo pretende complementar a Convenção sobre o Cibercrime através da criminalização de actos racistas e xenófobos praticados através de sistemas informáticos.

Ainda no mesmo capítulo, o **art. 2º** - "**definição**" - para efeitos de uma coerente interpretação considera:

- «Material racista e xenófobo» "qualquer material escrito, imagem ou outra representação de ideias ou teorias que defende, promove ou incita ao ódio, à discriminação ou

violência contra um qualquer indivíduo ou grupo de indivíduos em razão da raça, cor, ascendência, origem nacional ou étnica e religião, se for utilizado como pretexto para qualquer um destes elementos"

Todos os outros conceitos deverão ter a mesma interpretação que consta na CCib.

O Capítulo II do Protocolo - "**Medidas a adoptar a nível nacional**" - é composto por 5 arts. a serem considerados infracções penais, a nível interno pelo Estados Partes, quando praticados através de sistema informático, de forma intencional e ilegítima.

- **Difusão de material racista e xenófobo através de sistemas informáticos -art. 3º** - disponibilização ao público de material racista e xenófobo;
- **Ameaça por motivos racistas e xenófobos** - **art. 4º** - ameaça contra: "um indivíduo por força da sua pertença a um grupo identificado pela raça, cor, ascendência, origem nacional ou étnica e religião, se for utilizada como pretexto para qualquer um destes elementos ou um grupo de indivíduos identificado por qualquer uma dessas características";
- **Insulto por motivos racistas e xenófobos** - **art. 5º** - insulto público " dirigido a um indivíduo por força da sua pertença a um grupo identificado pela raça, cor, ascendência, origem nacional ou étnica e religião, se for utilizado como pretexto para qualquer um destes elementos ou dirigido a um grupo de indivíduos identificado por qualquer uma dessas características";
- **Negação, minimização grosseira, aprovação ou justificação do genocídio ou dos crimes contra a humanidade** - **art. 6º** - disponibilização ao público de material que de alguma forma negue, minimize ou aprove crimes de genocídio ou outros contra a humanidade definidos no direito internacional ou por tribunal internacional;
- **Auxilio e instigação** - **art. 7º** - à pratica de qualquer infracção prevista no protocolo.

As reservas ou a possibilidade de adoptar condições especiais às infracção previstas nos arts. anteriores constam nos números 2 e 3 de cada um.

São, literalmente, aplicáveis ao protocolo os arts. 1º, 12º, 13º, 22º, 41º, 44º, 45º, 46º da CCib, como dispõe o **art- 8º** do protocolo - "**Relações entre a Convenção e o presente Protocolo**". Cada parte tem o direito de retirar a reserva efectuada ao abrigo do art. 12º, logo que as circunstancias o permitam - **art. 13º** - "**Estatuto e retirada de reserva**". Existe a possibilidade de especificar o ou os territórios a que se aplica o protocolo, podendo posteriormente estende-los ou retira-los - **art. 14º** - "**Aplicação territorial**"

2.1.3. Decisão-Quadro 2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação

- **Publicado no Jornal Oficial nº L 069 de 16/03/2005 p. 0067 – 0071**

A decisão quadro tem como objectivos "reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes, responsáveis pela aplicação da lei nos Estados-Membros"[9], atendendo a uma aproximação do direito penal interno, no que diz respeito aos ataques contra os sistemas de informação; garantir a punibilidade destes ataques através de sanções penais eficazes; possibilitar uma cooperação judiciária neste âmbito; harmonização das legislações através de disposições comuns.

Existe uma preocupação cada vez maior com a possibilidade de ataques aos sistemas de informação internos dos Estados Membros, podendo comprometer uma sociedade de informação segura, um espaço de liberdade, de segurança e justiça, exigindo nestes moldes uma actuação por parte da União Europeia.

Para que seja possível fazer face a estas ameaças impõe-se uma abordagem global em matéria de segurança das redes e de informação, como foi referido «Plano de Acção "eEurope", na Comunicação da Comissão intitulada "Segurança das redes e da informação: proposta de abordagem de uma política europeia" e na Resolução do Conselho de 28 de Janeiro de 2002, sobre uma abordagem comum e acções específicas no domínio da segurança das redes e da informação[10]».

A Decisão teve por base:

⇒ Resolução do Parlamento Europeu de 5 de Setembro de 2001, na tentativa de sensibilizar os Estados Membros para os problemas associados à segurança de informação;

⇒ As diversas lacunas e divergências nas legislações nacionais de cada Estado Membro podem conter efeitos negativos no combate a este tipo de criminalidade e dificultar em muito a cooperação internacional que se exige a este nível, pelo que se impõe uma harmonização das legislações penais neste âmbito;

⇒ "O Plano de Acção do Conselho e da Comissão sobre a melhor forma de aplicar as disposições do Tratado de Amesterdão relativas à criação de um espaço de

[9] Decisão Quadro 2005/222/JAI do Conselho de 24 de Fevereiro de 2005
[10] JO C 43 de 16.2.2002, pág. 2

liberdade, de segurança e de justiça[11], o Conselho Europeu de Tampere, de 15 e 16 de Outubro de 1999, o Conselho Europeu de Santa Maria da Feira, de 19 e 20 de Junho de 2000, o Painel de Avaliação da Comissão e a Resolução do Parlamento Europeu de 19 de Maio de 2000 mencionam ou requerem medidas legislativas contra a criminalidade de alta tecnologia, nomeadamente definições, incriminação e sanções comuns"[12];

⇒ Para reforçar a segurança das infra-estruturas da informação e combater a cibercriminalidade é necessário complementar os trabalhos realizados pelas organizações internacionais, tanto ao nível do Conselho da Europa, como dos trabalhos do G8, de modo a aproximar as legislações e a cooperação transfronteiriça;

⇒ "Todos os Estados-Membros ratificaram a Convenção do Conselho da Europa, de 28 de Janeiro de 1981, para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal. Os dados de carácter pessoal, tratados no contexto da aplicação da presente decisão-quadro, serão protegidos em conformidade com os princípios estabelecidos na referida Convenção"[13];

⇒ Torna-se impreterível estabelecer definições comuns no âmbito dos sistemas de informação e de dados informáticos para que a decisão-quadro seja aplicável de forma coerente, assim como adoptar elementos constitutivos comuns às infracções penais[14];

⇒ Deverá ser assegurada, por cada Estado-Membro, uma cooperação judiciária eficaz em referência aos arts. 2º,3º,4º e 5º da decisão-quadro;

⇒ Apesar da necessidade de combater eficazmente o cibercrime, os Estados Membros não devem excessivamente criminalizar condutas, atendendo nomeadamente às pessoas autorizadas;

⇒ As sanções devem ser adequadas e as penas mais graves aplicadas aos casos de criminalidade organizada[15] e de danos ou interesses lesados mais elevados;

⇒ Deve ser tida em conta a Recomendação do Conselho 25/6/2001, no âmbito das medidas de cooperação entre os Estados Membros;

Adoptou a decisão-quadro 2005/222/JAI.

[11] JO C 19 de 23.1.1999, pág. 1
[12] Considerando nº (6)
[13]Considerando nº (9)
[14]Cf. Arts. 2º,3º,4º e 5º da decisão-quadro
[15]Conf. Acção Comum 98/733/JAI Conselho 21/12/98

- ***A Decisão-Quadro***

No seu **art. 1º "Definições"** voltamos a ter uma referência às definições constantes na Convenção sobre o Cibercrime adoptada em Budapeste em 2001. Assim, estão previstas as seguintes:

"a) "Sistema de informação", qualquer dispositivo ou qualquer grupo de dispositivos interligados ou associados, um ou vários dos quais executem, graças a um programa, o tratamento automático de dados informáticos, bem como dados informáticos por eles armazenados, tratados, recuperados ou transmitidos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;

b) "Dados informáticos", qualquer representação de factos, informações ou conceitos, de forma a serem processados num sistema de informação, nomeadamente um programa capaz de permitir que um sistema de informação execute uma dada função;

c) "Pessoa colectiva", qualquer entidade que beneficie desse estatuto por força do direito aplicável, com excepção do Estado ou de outras entidades de direito público no exercício das suas prerrogativas de autoridade pública e das organizações internacionais de direito público;

d) "Não autorizado", acesso ou interferência não consentidos pelo proprietário, por outro titular do direito do sistema ou de parte dele, ou não permitidos nos termos do direito nacional."

Como abordado acerca das considerações tidas em conta na decisão-quadro, devem ser adoptadas nas legislações dos Estados Membros, as seguintes infracções penais:

- **Acesso ilegal aos sistemas de informação – art. 2º** - o acesso intencional não autorizado deve ser punível como infracção penal, pelo menos quando não seja de menor gravidade, ou então apenas aquando a violação de uma medida de segurança;
- **Interferência ilegal no sistema – art. 3º** - impedir ou interromper o funcionamento de um sistema, de forma não autorizada, através de uma modificação nos dados informáticos;
- **Interferência ilegal nos dados – art. 4º** - modificação de dados informáticos – apagar, danificar, alterar, suprimir;
- **Instigação, auxílio, cumplicidade e tentativa – art.5º** - na prática de alguns dos crimes mencionados nos arts. 2º,3º,4º, a instigação, o auxílio e a cumplicidade,

devem ser puníveis como infracções penais; a tentativa, igualmente, podendo em todo o caso não ser aplicada ao art. 2º.

As **sanções** aplicadas por cada Estado Membro aos crimes constantes nos arts. 2º a 5º, devem ser "efectivas, proporcionadas e dissuasivas" – **art. 6º**.

Se as acções previstas no nº 2 do art.2º e nos arts. 3º e 4º, forem cometidas por uma organização criminosa, deve ser aplicada pena privativa da liberdade com duração máxima de dois a cinco anos[16], tal como previsto no **art. 7º** - circunstâncias agravantes, ou ainda nos casos em que resultem danos ou interesses lesados de elevado grau.

Mais uma vez, remetemos a análise da responsabilidade das pessoas colectivas ao abrigo da decisão-quadro, para o capítulo inserido no âmbito daquela.

O **art. 10º** versa sobre a **competência de cada Estado Membro**, impondo que cada um defina as suas competências no âmbito das infracções previstas, incluindo os casos de extradição e quando exista um conflito de competências positivo entre os Tribunais de cada Estado Membro.

A rede 24/7 prevista na Convenção sobre o Cibercrime, adoptada em Budapeste, 2001, é referida, também, pela decisão-quadro que reforça o papel que aquela desempenha como rede de contacto operacional entre os Estados Membros – **art. 11º - Intercâmbio de Informações**.

A Decisão-Quadro entrou em vigor a 16 de Março de 2005, tendo os Estados Membros adoptado as medidas necessárias para cumprir com esta até 16 de Março de 2007.

[16]Definida deste modo na Acção Comum 98/733/JAI

2.2 Direito Comparado

- **Brasil**

O Projecto de Lei Brasileiro nº 2793/11, aprovado na Câmara, tipificando crimes cibernéticos no Código Penal (Decreto Lei nº 2.848/40) foi fortemente criticado por ter resultado do escândalo de roubo de fotografias da actriz Carolina Dieckman, que foi alvo de invasão no seu computador.

Sobre este tema é possível encontrar duas opiniões divergentes, por um lado os que defendem a criação de leis para criminalizar condutas, por outro lado os que defendem as liberdades. Aqueles consideram que o sistema jurídico deve tornar mais rápida e eficaz a punição de quem comete crimes digitais, fazendo uso ou não da internet e de outras redes de comunicação de dados. Estes têm a preocupação de essas leis não punirem os utilizadores com pouco ou quase nenhum conhecimento técnico sobre as ferramentas que usam ou até mesmo os profissionais que as usam de modo legitimo para pesquisas e desenvolvimento.

Tomam como exemplo a Alemanha que aprovou uma lei semelhante à aprovada na Câmara e que seguiu para o Senado. A lei Alemã detém uma das melhores ferramentas de teste de segurança de rede – Kismac (an open-source and free sniffer/scanner application) que, contudo, tornou-se proibida, a não ser com autorização expressa.

O Projecto Lei Brasileiro tipifica como crimes a invasão, a cópia, a reprodução e a divulgação não autorizadas de sistemas informatizados e dados, sendo que o código incluirá um capítulo específico sobre crimes digitais.

Coloca-se a questão de saber se antes de estabelecer punições, não se deveria estabelecer um conjunto de direitos e deveres dos utilizadores da internet assim como dos fornecedores de serviços, orientando-os para o uso correcto da internet, ficando-se no âmbito apenas civil.

Se ficarmos apenas no âmbito civil a punição que pode resultar é unicamente de indemnização ou reparação, o que se revela claramente insuficiente para inibir o criminoso de praticar o crie.

Após o escândalo em torno das fotografias que foram retiradas do computador da actriz Carolina Dieckman e posteriormente divulgadas, foi aprovada a *Lei 12737* que ficou designada pelo apelido da actriz. A lei veio estabelecer penas de multa e prisão para os vários tipos de crimes digitais como a invasão de computadores, a criação de programas que permitem inviabilizar sistemas e mecanismos de segurança, assim como a divulgação ou

comercialização de dados, sendo que consoante os casos e os danos que provoquem as penas podem ser agravadas.

Antes da Lei 12737 ter sido aprovada, lei esta encabeçada pelo deputado Paulo Teixeira (PT-SP), uma outra lei, aprovada na Câmara Brasileira, designada como "Lei Azeredo", foi mantida durante anos em discussão por ter sido considerada demasiado restrita, como por exemplo ao impor aos provedores o dever de fiscalizar os usuários, pelo que apenas foram mantidos quatro artigos e apresentada como alternativa a Lei 12737.

- **PROJECTO DE LEI DA CÂMARA, Nº 35 de 2012**

Autor: Deputado - Paulo Teixeira e outro(s) Sr(s). Deputado(s)

Ementa: Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de Dezembro de 1940 - Código Penal; e dá outras providências.

Explicação da ementa:

O Projecto Lei tipifica como crimes os ilícitos informáticos, alterando artigos do CP Brasileiro para que seja considerado crime a "invasão de dispositivo informático, consistindo em devassar dispositivo informático alheio, mediante violação indevida de mecanismo de segurança com o objectivo de adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular, instalar vulnerabilidades ou obter vantagem ilícita"[17]. Os infractores incorreram numa pena de prisão de três meses a um ano e pena de multa, sendo que quando exista elevado prejuízo económico comercialização ou transmissão a terceiro, ou se o crime for praticado contra autoridades públicas, as penas podem ser aumentadas.

Altera a redacção de outro art. do CP, para passar a dispor: "Interrupção ou perturbação de serviço telegráfico, telefónico, informático, telemático ou de informação de utilidade pública, que incorre nas mesma penas"

- **Alemanha**

O art. 10º da Constituição Alemã consagra o direito à inviolabilidade da correspondência e telecomunicações, relacionado com o direito à privacidade consagrado no art. 2º da mesma lei. O Código de Processo Penal Alemão prevê no seu Capítulo VIII, a regulamentação dos meios de obtenção de prova. Atendendo aos novos métodos de ingerência em comunicações, como meio de obtenção de prova, como é o caso das buscas online, o legislador Alemão optou por admiti-las em casos que existam indícios de um perigo concreto

[17] Cf. Projecto Lei da Câmara, nº35 de 2012

para a vida, integridade física, liberdade da pessoa e bens da comunidade. Os art. 100ª. E 100b. da StPO, constituem referência em matéria de métodos de investigação, nomeadamente quanto à intercepção e gravação de telecomunicações.

A Lei das Telecomunicações de 22 de Junho de 2004 ("TKG") e o Regulamento de Vigilância das Telecomunicações ("TKÜV") estabelecem os detalhes técnicos e deveres sobre as informações fornecidas pelos fornecedores de serviços de comunicação. Com a necessidade de transposição da Directiva 2006/24/CE[18]de 15 de Março do Conselho e do Parlamento, surgiu a Lei da Nova Regulamentação da Vigilância das Telecomunicações e outros Meios de Investigação Encoberta e aproveitando esta necessidade, atendendo também à Convenção sobre o Cibercrime, o legislador Alemão resolveu aglomerar os novos aspectos relacionados com as comunicações electrónicas e criminalidade informática num só diploma legal, que trouxe como novidade a possibilidade de serem realizadas buscas online sem necessidade de despacho judicial.

- **Itália**

Devido à Convenção sobre o Cibercrime, o ordenamento jurídico italiano viu-se obrigado a introduzir alterações nas disposições legais que previam meios de obtenção de prova, com a aprovação da "Legge 18 marzo 2008, nº48" que ratificou e aprovou a referida Convenção. Esta lei introduziu várias alterações no Código Penal ("Codice Penale"), nomeadamente, nos tipos legais referentes à criminalidade informática e no Código de Processo Penal ("Codice di Procedura Penale"),aditando nos Capítulos sobre aprova, normas relacionadas com os sistemas informáticos ou telemáticos. Em cumprimento do previsto na Ccib, a nova lei italiana adaptou a sua legislação com os novos meios de obtenção de prova – exames, revistas, buscas[19], apreensões e intercepção de comunicações – adaptados à nova realidade informática, de modo a conseguir através dos meios de prova tradicionais chegar aos sistemas informáticos[20]. A transposição da Directiva 2006/24/CE introduziu alterações ao art. 132º do "Codice in matéria di protezione dei dati personali", impondo aos fornecedores de

[18] Conservação de dados no domínio das telecomunicações

[19] O legislador italiano não determinou a admissibilidade das buscas online, prevendo apenas pesquisas a dados informáticos que se relacionam com as comunicações e tráfego, os quais podem ser pedidos aos fornecedores de serviços de internet – art. 254-bis do "Codice di Procedura Penale"

[20] Cf. Art. 266-bis do "Codice di Procedura Penale" – admissibilidade da intercepção do fluxo de comunicações relativos a sistemas informáticos ou telemáticos – consagração da intercepção de correio electrónico em investigação de crimes informáticos.

serviços de internet, se notificados nesse sentido, tenham que conservar e proteger os dados relativos ao tráfego informático para fins de prevenção e repressão criminal.

Como podemos verificar o legislador italiano preferiu introduzir alterações aos artigos já existentes em vez de criar novos diplomas legais.

- **Espanha**

O ordenamento jurídico espanhol, consagra num só artigo – art. 579º da "Ley de Enjuiciamiento Criminal" a admissibilidade da apreensão de correspondência, das escutas telefónicas e da observação das comunicações postais, telegráficas ou telefónicas. O Código de Processo Penal espanhol, consagra no seu Título VIII, arts. 545º a 588º de forma exaustiva todos os meios de obtenção de prova. A doutrina e jurisprudência consideram excluída das previsões do Código de Processo Penal a possibilidade de intercepção de comunicações electrónicas, nomeadamente o correio electrónico, não constando, igualmente, na lei criminal espanhola referencias a buscas em suporte digitais, nem acesso aos dados de tráfego e localização, matéria esta regulada em diploma autónomo. É a "Ley 32/2003 de 3 de noviembre, de general de telecomunicaciones" que contempla o regime das escutas telefónicas previsto no Código de Processo Penal, prevendo no art. 33º que os operadores que exploram redes públicas de comunicações electrónicas ou que prestam serviços deste tipo disponíveis ao público, estão obrigados a realizar as intercepções autorizadas de acordo com os preceitos legais. Tal lei prevê um conjunto de dados que podem ser fornecidos por aquelas entidades que exploram redes públicas de comunicações electrónicas, protegendo dados de carácter pessoal e a intercepção de comunicações electrónicas pelos serviços técnicos. Refira-se, ainda neste âmbito, a "Ley 34/2002 de 11 julio, de servicios de la sociedad de la información y de comercio electrónico" que impõe respeito pelos direitos de intimidade pessoal, familiar e protege os dados pessoais na sociedade de informação.

A Directiva nº2006/24/CE foi transposta para ordem jurídica espanhola pela "Ley 25/2007 de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y las redes públicas de comunicaciones", diploma este, muito próximo da Lei portuguesa nº32/2008 de 17 de Julho, consagrando ambas, como limite máximo de obrigação de conservação de dados, mencionados na Directiva, o período de 1 ano.

2.3 Nacionais

Em Portugal, a matéria da criminalidade informática está regulada:

⇒ Código Penal;

⇒ Lei nº 109/2009 de 15 de Setembro;

⇒ Lei da Protecção de Dados Pessoais (Lei nº 67/98, de 26 de Outubro);

⇒ Lei da Protecção Jurídica de Programas de Computador (Decreto-Lei nº 252/94, de 20 de Outubro);

⇒ Código de Direitos de Autor e dos Direitos Conexos (Decreto-Lei nº 63/85, de 14 de Março);

⇒ Regime Geral das Infracções Tributárias (Lei nº 15/2001, de 05 de Junho)

Para o estudo em causa não importa analisar todas as leis, bastando referir alguns despachos e pareceres importantes, sendo que a Lei do Cibercrime será analisada em sede própria.

2.4 Aprovação dos instrumentos internacionais; Parecer da Procuradoria Geral da República

- **Resolução Assembleia da Republica nº88/2009**

A Resolução Assembleia da Republica nº88/2009, aprova a Convenção sobre o Cibercrime , adoptada em Budapeste em 23 de Novembro de 2001.

Com a resolução a AR, resolve nos termos da alínea I) do art. 161º e do nº5 do ar. 166º da CRP, aprovar a Convenção sobre o cibercrime, publicando em anexo àquela o texto integral na sua versão autenticada na língua inglesa e a tradução em Português.

Formula, contudo, no seu art. 2º determinadas reservas relativamente ao art. 24º nº5 da Convenção sobre o Cibercrime que trata das questões de extradição de pessoas. Assim, Portugal não concederá a extradição de pessoas:

- Que devam ser julgadas por um tribunal de excepção ou cumprir pena decretada por este;

- Quando se prove que o processo não oferece garantias juridicas à salvaguarda dos direitos do homem, ou que cumpram pena em condiçoes desumanas;
- Quando à infracção cometida corresponde pena ou medida de segurança de caracter perpetuo;
- Só será concedida a extradição quando a pena aplicável for superior a um ano;
- Quando à infracção cometida corresponda pena de morte;
- não concederá a extradição de cidadãos Portugueses;
- só é autorizado o "trânsito em território nacional de pessoa que se encontre em condições em que a sua extradição possa ser concedida".

- **Decreto do Presidente da República nº 91/2009 de 15 de Setembro**

O PR decreta, nos termos do art. 135º b) da CRP que ratifica a Convenção sobre o Cibercrime, aprovada pela Resolução da AR nº 88/2009 em 10 de Julho de 209.

O art. 2º é composto pela reserva constante na Resolução da AR.

Foi assinado a 29 de Agosto de 2009 e referendado a 9 de Setembro de 2009.

- **Resolução da Assembleia da República n.º 91/2009**

A Assembleia da República resolve, nos termos da alínea i) do artigo 161.º e do n.º 5 do artigo 166.º da Constituição, aprovar o Protocolo Adicional à Convenção sobre o Cibercrime relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adoptado em Estrasburgo em 28 de Janeiro de 2003.

- **Despacho da Procuradoria-Geral da República 2011**

O despacho da PGR considerou as problemáticas da cibercriminalidade, atendendo à Lei 109/2009 de 15 de Setembro que transpôs para a ordem jurídica interna a Decisão Quadro 2005/222/JAI, e ao papel fundamental que o Ministério Público desempenha neste domínio.

Enquanto titular da acção penal, exige-se que se debruce sobre aquelas problemáticas, nomeadamente nas questões de direito material e processual, sendo que nesta última é de realçar o art. 11º que prevê a possibilidade de investigar outros crimes que não só os previstos na Lei do Cibercrime, mas que tenham sido cometidos por meio de sistema informático, alargando aqui o âmbito de aplicação da Lei 109/2009, por aplicação a um elevado número de inquéritos pelo MP.

A complexidade associada à cibercriminalidade, impõe que o MP seja eficaz a classificar os actos com relevância criminal nesta área, assim como na obtenção de prova em suporte digital, de forma que os processos sejam dirigidos de modo adequado e consistente e que a realidade associada a este fenómeno seja feita de modo real e efectivo.

Pedro Miguel Figueira Verdelho, Procurador da República, com qualificações em matéria da cibercriminalidade é designado para assegurar/coordenar o desenvolvimento da coordenação do Cibercrime no Distrito Judicial de Lisboa, com possibilidade de se estender a todo o território.

Atendendo a estas considerações e ao abrigo dos arts. 11º e 12º nº2 b) do Estatuto do MP, instalou-se junto à Procuradoria-Geral da República um gabinete, dependente desta, com o objectivo principal de coordenar a actividade do MP no domínio da cibercriminalidade. Para tal é criada uma plataforma que permite aos magistrados do MP a troca de informações e um fórum entre o MP, os órgãos de polícia criminal e os prestadores de serviços, canais de comunicação para a solicitação de informação a fornecedores de serviços e criação de protocolos de cooperação com aqueles. Tendo em conta que se trata de uma inovação no âmbito da cibercriminalidade, os magistrados devem ter acções de formação sobre a prova digital.

- ## Parecer da Procuradoria-Geral da República nº11/2011

O parecer da PGR versa sobre os seguintes temas:

- Software
- Programa do computador
- Crime informático
- Cibercrime
- Pirataria informática
- Reprodução ilegítima

- Órgãos de polícia criminal
- Investigação criminal
- Pesquisa de dados informáticos
- Preservação expedita de dados
- Apreensão
- Competência
- Competência reservada
- Polícia judiciária
- Autoridade de segurança alimentar e económica
- Actividade económica
- Fiscalização
- Direitos de autor
- Propriedade intelectual

Apenas alguns dos temas do parecer serão abordados, pois apenas esses estão directamente relacionados com o presente estudo.

Este parecer resulta de um pedido da Autoridade de Segurança Alimentar e Económica sobre a sua competência no âmbito da Lei 109/2009, visto que têm surgido divergências no seu entendimento e do MP.

O parecer inicia-se com uma referência ao crime de reprodução ilegítima de programa protegido, previsto e punido pelo art. 8.º da lei do Cibercrime, sendo que a sua prática envolve a utilização de um sistema informático, logo são-lhes aplicáveis as disposições processuais contidas nos artigos 12.º a 17.º daquele diploma, conforme dispõe o seu artigo 11.º, n.º 1, alíneas *a*) e *b*), da mesma lei. A competência para a investigação destes crimes está cometida à Polícia Judiciária, de acordo com o disposto no artigo 7.º, n.º 3, alínea *l*), da Lei de Organização da Investigação Criminal, atendendo a que apenas a esta entidade podem pelo MP ser delegadas a execução dos actos de inquérito. É da competência exclusiva da PJ a investigação de crimes informáticos, pelo que a actuação da Autoridade de Segurança Alimentar e Económica (ASAE) no âmbito do crime referido, está "limitada exclusivamente à prática dos actos cautelares e urgentes, quer para obstar à sua consumação, quer para assegurar os respectivos meios de prova"[21]. Quando proceda a apreensão de objectos por fundadas suspeitas de conterem algo ilícito deve comunicar tal facto à Polícia Judiciária e ao

[21]Parecer PGR nº11/2011, parágrafo 3º

MP para validação. Contudo está impedida de proceder à pesquisa de dados informáticos armazenados em sistemas informáticos.

Dos crimes previstos na Lei n.º 109/2009, o crime usualmente investigado pela ASAE consta no seu *artigo 8.º, soba epígrafe* "Reprodução ilegítima de programa protegido", ou seja, um acto de reprodução destinado a explorar economicamente uma obra à revelia do autor. Este crime é passível de distinção do usual crime informático que se baseia numa actividade em torno de um computador ou uma rede com o intuito de proceder a um ataque ou ser usado como meio de um crime.Se considerarmos a natureza do crime de reprodução ilegítima de programa protegido, podemos concluir não ser necessário para a investigação do mesmo, preservar ou pesquisar dados informáticos, correio electrónico ou registos informáticos de natureza semelhante, pois apenas se pretende encontrar programas instalados que não detenham a devida licença.

Entendeu a ASAE que não se torna necessário obter a autorização da autoridade judiciária competente, não sendo aplicáveis a este caso as normas constantes dos arts. 12.º, 15.º, 16.º e 17.º da Lei do Cibercrime. São de parecer "que o crime de "Reprodução ilegítima de programa protegido", embora inserido numa lei designada por lei do Cibercrime, não é verdadeiramente um crime informático, uma vez que está em causa uma actividade onde um computador, ou uma rede de computadores, é utilizada como uma ferramenta, uma base de ataque ou como um meio de crime" [22].

Face à exposição apresentada pela ASAE, cumpriu à Procuradoria emitir parecer sobre o assunto em apresso.

A Procuradoria antes de abordar a questão da competência da ASAE no âmbito da cibercriminalidade, achou por conveniente realizar algumas considerações sobre programa de computador, pois a lei actual[23] não define o que se entende por aquele, diversamente da antiga Lei da criminalidade informática que o considerava ser no artigo 2.º, alínea *c*), "um conjunto de instruções capazes, quando inseridos num suporte explorável em máquina, de permitir à máquina que tem por funções o tratamento de informações, executar ou produzir determinada função, tarefa ou resultado".

Tendo o *software* passado a ser desenvolvido e comercializado como produto autónomo dos computadores surgiu a necessidade de conferir uma tutela jurídica específica, de forma a impedir a ilicitude das cópias não autorizadas. Com a evolução operada nos meios

[22] Parecer da PGR nº11/2011, parte I, parágrafo 12º
[23] Lei 109/2009

de tecnologia, foi de fácil percepção a possibilidade de copiar os programas de computador, sendo estes objecto de pirataria, existindo um mercado onde podiam ser comercializados.

São referidos diversos instrumentos internacionais[24] e nacionais, com relevância para a tutela jurídica a ser concedida aos direitos de autor e direitos conexos[25], tomando como exemplo o artigo 14.º do Decreto -Lei n.º 252/94 sob a epígrafe "Tutela Penal" que dispõe "1 — Um programa de computador é penalmente protegido contra a reprodução não autorizada. 2 — É aplicável ao programa de computador o disposto no n.º 1 do artigo 9.º da Lei n.º 109/91, de 17 de Agosto". É remetido para o n.º 1 do artigo 9.º da Lei n.º 109/91, de 17 de Agosto "Reprodução ilegítima de programa protegido" (lei da criminalidade informática) que dispõe "1 — Quem, não estando para tanto autorizado, reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei será punido com pena de prisão até três anos ou com pena de multa".

O legislador considerou os programas de computador merecedores de tutela penal, sancionando os actos de reprodução não autorizada, com vista a combater a pirataria informática e proteger a propriedade intelectual, para que esta não saía do domínio do seu autor sem a sua autorização.

A Lei 109/2009 no seu capítulo I apresenta um conjunto de definições. Sendo aqui relevante a que se refere a sistema informático e dados informáticos[26], neste último é também englobado o antigo conceito de "programa protegido". No que diz respeito às disposições penais materiais, importa referir a descrição constante no art. 8º nº1 da Lei do Cibercrime - "Reprodução ilegítima de programa protegido" - "1 — Quem ilegitimamente reproduzir, divulgar ou comunicar aopúblico um programa informático protegido por lei é punido compena de prisão até 3 anos ou com pena de multa". Esta reprodução envolve tantos os downloads de programas para qualquer suporte (computador, disquete, CC-ROM) como a transmissão em rede daqueles.

As medidas de direito processual previstas na Lei do Cibercrime, vieram dar cumprimento às obrigações impostas pela Convenção sobre o Cibercrime, nos seus arts. 16º e 17º, que se tornam essenciais nas investigações criminais neste domínio. Para descoberta da verdade, torna-se imprescindível a qualquer investigação, a rapidez na preservação de dados de forma a conservar as provas. Neste caso de preservação expedita de dados pressupõe-se que se esteja já no âmbito de um processo de investigação do crime, sendo este realizada

[24] Parecer da PGR nº11/2011, página 2 e 3
[25] Nº 1 e 2 do artigo 201.º, integrado no Título IV - CDADC
[26] Ver art. 2º da Lei 109/2009

quando a autoridade judiciária competente assim o entenda, seja o Ministério Publico, Juiz de instrução ou Juiz de julgamento. Note-se que esta medida também pode ser ordenada pelo órgão de polícia criminal com a autorização da autoridade judiciária competente referida ou quando haja urgência ou perigo na demora, sendo que, neste último caso, tem que dar notícia imediata do facto à autoridade judiciária e transmitir -lhe o relatório previsto no CPP.

Diferentemente da medida processual de preservação expedita de dados é a pesquisa de dados informáticos num sistema informático, que nos remete não só para a Lei do Cibercrime, mas também para o art. 174º nº do CPP, revestindo a natureza de "busca". Sucede nos casos em que "houver indícios de que dados informáticos relacionados com um crime ou que possam servir de prova se encontram num determinado sistema informático é ordenada a busca informática". Esta busca é ordenada por despacho pela autoridade judiciária competente, devendo esta, presidir à diligência sempre que tal seja possível. A lei do Cibercrime, no seu art. 15º nº1, pressupõe que a pesquisa de dados informáticos seja tomada no decurso de um processo, competindo à autoridade já referida, podendo contudo os órgãos de polícia criminal proceder à pesquisa, em determinadas situações, sem prévia autorização daquela.

Á semelhança do art. 178.º, nº 4, do CPP, o artigo 16.º, nº 2, da lei do Cibercrime prevê a possibilidade de o órgão de polícia criminal efectuar apreensões, sem prévia autorização da autoridade judiciária, no decurso de pesquisa informática a um sistema informático legitimamente ordenada, bem como quando haja urgência ou perigo na demora, sendo sempre sujeitas a validação no prazo máximo de 72 horas (nº 4).

No âmbito das medidas cautelares dos órgãos de polícia criminalno que diz respeito aos meios de prova, revela especial interesse o art. 251º, nº 1,alínea *a*), do CPP, que permite a realização de uma busca "sempre que tiveremfundada razão para crer que aí se ocultam objectos relacionados com o crime,susceptíveis de servirem a prova e que de outra forma se poderiam perder".

As medidas de apreensão, diferentes da busca, têm como objectivo juntar ao processo, como meio de prova, os objectos que tiverem servido à prática de um crime ou que constituam um benefício resultante daquele, podendo os órgãos de polícia criminal proceder a tal medida, sem autorização prévia da autoridade judiciária competente, quando haja "*periculum in mora"*.

Feitas estas considerações, importa agora reporta-las para uma vertente de resposta ao pedido formulado pela ASAE. Trata-se em primeiro lugar de saber se as disposições

processuais previstas nos arts. 12º a 17º da lei do Cibercrime são aplicáveis à investigação do crime de reprodução ilegítima de programa protegido tipificado no nº 1 do artigo 8º do mesmo diploma.

Entendeu a PGR que a resposta tem que ser afirmativa, pois este ilícito criminal assume a natureza de crime informático, constante na Lei do Cibercrime. O "conceito de dados informáticos, no qual também se integram os programas de computador, não restarão dúvidas de que a prática deste crime envolve a utilização de um sistema

informático. Consequentemente, as normas processuais contidas nos citados preceitos desse diploma podem e devem, quando necessário e verificados os respectivos pressupostos, ser convocadas no âmbito da sua investigação e perseguição criminal"[27] - art. 11º, nº 1, alíneas *a*) e *b*)da Lei do Cibercrime.

Outra questão é a competência da ASAE para investigar o crime de reprodução ilegítima de programa protegido, sendo que a alínea *l*) do nº 3 do art. 7º da Lei nº 49/2008, de 27 de Agosto, que aprova a (LOIC), é da competência reservada da Polícia Judiciária.

Como é sabido a direcção do inquérito cabe ao Ministério Público, assistido pelos órgãos de polícia criminal, conforme se dispõe no artigo 263º, nº 1, do CPP. Os órgãos de polícia criminal, de acordo com a definição contida na alínea *c*) do artigo 1º do CPP, são "todas as entidades e agentes policiais a quem caiba levar a cabo quaisquer actos ordenados por uma autoridade judiciária ou determinados por este Código". A LOIC no seu art. 3º dispõe que são órgãos de polícia criminal de *competênciagenérica*: "(*a*) a Polícia Judiciária; (*b*) a Guarda Nacional Republicana;

e (*c*) a Polícia de Segurança Pública" (nº 1), sendo órgãos de polícia criminal de *competência específica* todos aqueles a quem a lei confira esse estatuto (nº 2), como sucede com a ASAE.

Esta entidade, na definição dada pelo Decreto -Lei n.º 274/2007, de 30 de Julho, "congrega num único organismo a quase totalidade dos serviços relacionados com a fiscalização e com a avaliação e comunicação dos riscos na cadeia alimentar, com significativos ganhos de eficiência e maior eficácia, procedendo a uma avaliação científica independente dos riscos na cadeia alimentar e fiscalizando as actividades económicas a partir da produção e em estabelecimentos industriais ou comerciais", tendo como competências: colaborar com as autoridades judiciárias nos termos do disposto no CPP, procedendo à investigação dos crimes cuja competência lhe esteja especificamente atribuída por lei.

[27] Parecer PGR nº11/2011, página 7

Segundo o artigo 15.º, a ASAE detém poderes de autoridade e é órgão de polícia criminal (nº 1).

No âmbito das competências da ASAE, deverá incluir -se a fiscalização dos locais onde se proceda a actividades que envolvam objectos informáticos, atendendo com especial relevo a vertente económica associada aos programas de computador, sendo que a sua protecção jurídico visa tutelar os direitos económicos dos seus autores. Se, por exemplo, no meio da sua actividade, esta entidade detectar objectos que contenham programas informáticos ilícitos, deve proceder à apreensão de tais suportes, de acordo com o nº 2 do art. 201.º do CDADC. Esta competência corresponde à que é prevista no nº 4 do art. 178º, conjugado com a alínea *c*) do nº 2 do art. 249º, ambos do CPP. Será com fundamento em motivo de urgência e de necessidade que a ASAE deverá proceder, no exercício das suas competências, à imediata apreensão dos computadores ou de qualquer outro equipamento informático em relação aos quais existam fundadas suspeitas de conterem instalados programas informáticos não licenciados.

Quanto à questão de saber em que termos se desenvolve a actuação da ASAE no âmbito da Lei do Cibercrime, entende a PGR que a competência para a investigação dos crimes previstos naquela lei está reservada à Polícia Judiciária, pelo que apenas a esta poderá ser delegada a execução de actos de inquérito pelo MP. A ASAE está limitada à prática dos actos cautelares e urgentes, para impedir a prática de crimes e assegurar os meios de prova, pelo que deve proceder à "apreensão dos suportes físicos autónomos de computadores" (CD - ROMs, pen, disks, disquetes, etc.) que contenham programas informáticos ilícitos, comunicando o facto à Polícia Judiciária, em prazo não excedente a 24 horas, e ao Ministério Público para sua validação. Dado o carácter de competência reservada à PJ na investigação de crimes informáticos, não pode a ASAE proceder à pesquisa de dados informáticos armazenados em sistemas informáticos.

Em conclusão a PGR, no seu parecer, entende que o crime de reprodução ilegítima de programa protegido, assume a natureza de crime informático e a sua prática envolve a utilização de um sistema informático, pelo que lhe são aplicáveis as disposições processuais contidas nos artigos 12.º a 17.º da Lei do Cibercrime - art. 11º da mesma lei. A competência para a investigação do referido crime está reservadaà Polícia Judiciária, sendo que a actuação da ASAE está limitada aos actos cautelares e urgentes, podendo proceder à apreensão dos suportes físicos exteriores de computador que contenham programas informáticos ilícitos, como dos próprios computadores se existirem suspeitas de aí estarem instalados os referidos

programas estando apenas vedada a pesquisa de dados informáticos armazenados em sistemas informáticos.

3.1. A Lei 109/2009 de 15 de Setembro aprova a Lei do Cibercrime

3.1.1. A exigência de uma lei adequada e eficaz

A criminalidade informática está intimamente ligada à questão dos cidadãos exercerem livremente as suas liberdades e verem os seus direitos respeitados. Assim nos demonstra a CRP no seu art. 35º que prevê a protecção das pessoas contra o tratamento de dados pessoais, atendendo à proibição de tratamento de determinados dados pessoais, assim como o direito de acesso aos dados que se encontrem em registos informáticos.

Mostrando-se insuficiente esta protecção, apesar de consagrada na lei fundamental, sentiu-se necessidade de transpor estes direitos para leis ordinárias, combinando a evolução tecnológica operada e os direitos dos cidadãos.

O Código Penal prevê crimes praticados por meio informático, contudo revelando-se extremamente ineficaz e insuficiente para fazer face à evolução informática, surgiu em 1991 a Lei 10/91, de 17 de Agosto, cumprindo com as garantias já enunciadas na CRP e adaptando a legislação nacional à Convenção 108 do Conselho da Europa relativa à protecção das pessoas sobre o tratamento automatizado de dados pessoais. A LCI permitiu contemplar de um modo mais abrangente os crimes informáticos.

A Comunidade Europeia vem desde há muito mostrando a sua preocupação com esta matéria, tendo inclusive se pronunciado através da Directiva nº95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995, transposta para o direito interno com a Lei 67/98 de 26 de Outubro[28], conjugada com a Lei nº41/2004 de 18 de Agosto[29].

Preocupado com os temas da segurança e liberdade de utilização das tecnologias de informação e comunicação aliada à criminalidade informática que tem visto o seu âmbito aumentar em muito, o Estado tornou-se imperioso em, com equilíbrio, garantir os direitos dos cidadãos (liberdade, segurança e privacidade).

Através da Resolução da Assembleia da República nº88/2009 e Decreto do Presidente da República nº92/2009, publicados em 15 de Setembro, Portugal ratificou a Convenção sobre o Cibercrime, adoptada em Budapeste em 23 de Novembro de 2001 e no

[28] Lei da Protecção de Dados Pessoais
[29] Lei deProtecção de Dados Pessoais nas Telecomunicações

seu seguimento e atendendo à problemática ora verificada, surgiu a Lei do Cibercrime, aprovada pela Lei nº109/2009 de 15 de Setembro, tipificando inúmeros crimes – elementos do tipo legal integram o meio informático - em que se torna claro a sua intenção de proteger os bens jurídicos mencionados – segurança e liberdade de utilização da informática. Estamos já no âmbito em que o bem jurídico protegido integra a realidade informática, prevista nos elementos tipificadores.

Torna-se importante realçar que o próprio CP, e por ter sido o primeiro instrumento legislativo a prever esta matéria, tipifica como crime a "Devassa por meio informático", "Violação de correspondência e telecomunicações" e "Burla informática", sendo que a LC vem tipificar outros crimes informáticos que serão sumariamente analisados "Falsidade informática", "Dano relativo a programas ou outros dados informáticos", "Sabotagem informática", "Acesso ilegítimo", "Intercepção ilegítima"e "Reprodução ilegítima de programa protegido". Acresce que encontramos em legislação avulsa outros crimes informáticos, como podemos verificar no art. 128º do Regime Geral das Infracções Tributárias, art. 11º do DL nº122/2000 de 4 de Julho, Titulo VI do Código dos Direitos de Autor e Direitos Conexos (art. 217º e ss.).

3.1.2. Novidades introduzidas com a Lei do Cibercrime

A Lei n.º 109/2009 – LC - integra num só diploma legal todas as normas respeitantes ao cibercrime, incluindo normas de direito penal material, com a criação de novos tipos de crimes, assim como normas processuais, que se consideram excepções às regras do CPP, terminando com disposições relativas à cooperação internacional.

- A LC tornou crime a produção e difusão de um vírus, que passa a ser punido com pena de prisão com limite máximo 10 anos. A modificação, destruição de programas ou outros dados informáticos, assim como a perturbação destes constitui crime segundo a nova lei.

- Os comportamentos que instiguem ou auxiliem qualquer crime previsto na LC passam também a ser criminalizados. Esta é uma inovação que a Lei do Cibercrime introduziu no sei da cibercriminalidade, pois a LCI não previa qualquer tipo de sanção para estes crime, pois tratava-se já de uma lei com mais de 15 anos, completamente desvirtuada da realidade ligada às redes de comunicação, tornando-se imperativo uma nova lei que garantisse o combate ao cibercrime de forma eficaz.

- A introdução ilegítima em sistema informático alheio é punida com uma pena que pode ir até um ano de prisão, ou no caso de sistemas onde existem segredos comerciais ou industriais ou dados confidenciais protegidos por lei, até cinco anos.
- Passa a ser punível a reprodução ou divulgação de programas protegidos por lei com uma pena de prisão até três anos ou pena de multa.
- A falsificação de dados com o intuito de provocar um equívoco nas relações jurídicas, produzindo documentos ou dados falsos é punida com pena de prisão de limite máximo de cinco anos ou com pena de multa de 120 a 600 dias. Nos casos de falsificação de dados dos cartões de crédito, a pena aplicável é de um a cinco anos de prisão.

No que diz respeito às disposições de direito penal material, a LC, não introduziu grandes novidades aos crimes já previstos no âmbito da Lei de criminalidade informática – LCI.

- A grande inovação acontece precisamente nas normas processuais, prevendo agora a lei normas específicas para o cibercrime, assim como para crimes cometidos por meio de sistema informático e ainda que exijam recolha de prova em suporte electrónico, como veremos.
- Muitas da novas normas processuais resultaram da obrigação de transpor para a ordem jurídica interna a Convenção sobre o Cibercrime, assim como adequar a legislação interna à realidade informática, tendo como por exemplo a necessidade de preservação de dados que pode ser imprescindível à investigação, dado o seu carácter temporário e de fácil deterioração.
- Outra medida inovadora foi o mecanismo da injunção, que se prende com a enorme dificuldade, por parte de quem investiga, a aceder a informação que se encontra armazenada nos modernos sistemas informáticos, devendo a entidade que detém tal informação colaborar com as autoridades.

Como referido a LC, manteve a tipologia de crimes já existentes no seio da LCI, alterando poucos aspectos nos tipos legais, contudo introduziu novos meios de investigação e produção de prova específicos para o combate à criminalidade informática. Estas introduções podem ser confirmadas no Capitulo III com disposições processuais que facilitam a investigação do crime e a prova do mesmo, no Capitulo IV com medidas de cooperação

internacional neste âmbito e no Capitulo V questões relacionadas com a aplicação no espaço da lei penal portuguesa e competência dos tribunais.

- À apreensão de mensagens de correio electrónico é aplicável o mesmo regime de apreensão de correspondência, para que se realize a intercepção e registo de dados informáticos é necessária autorização do juiz e apenas quando seja indispensável para a descoberta da verdade. Neste âmbito aplicam-se ao conteúdo de comunicações ou apenas de dados de tráfego o que o CPP prevê quanto à intercepção de comunicações telefónicas.

Importa salientar que estes novos meios processuais têm que ser conjugados com outras legislações avulsas, como a Lei da Cooperação Judiciária Internacional em matéria penal, aprovada pela Lei nº144/99 de 31 de Agosto, a Lei nº5/2004 de 10 de Fevereiro no que diz respeito à obtenção de prova, o DL nº290-D/99 de 2 de Agosto sobre a validade, eficácia e valor probatório dos documentos, assinaturas e comunicações electrónicas, a Lei nº7/2004 de 7 de Janeiro, o DL nº41/2004 de 18 de Agosto relativa à protecção de dados pessoais e a Lei nº32/2008 de 17 de Julho sobre a conservação de dados.

- Outra novidade trazida com a LC é a criação de uma estrutura que serve como ponto de contacto, no seio da Policia Judiciaria, permanentemente disponível para a cooperação com outras autoridades internacionais.

A transposição das normas europeias para o direito interno de cada Estado Membro gerou algumas polémicas, sobretudo na Alemanha e Reino Unido, pela possibilidade da polícia poder aceder livremente aos computadores pessoais dos suspeitos e revistar seus registos e dados.

Em Portugal, no decorrer de uma investigação, a lei permite que se realizem pesquisas em dados informáticos, através de autorização judicial, podendo contudo serem realizadas sem este em casos especiais, como no terrorismo, criminalidade violenta ou altamente organizada, havendo fortes indícios da possível prática de um crime que coloque em perigo a vida ou integridade de qualquer pessoa.

3.1.3. Criticas à Lei do Cibercrime

Na opinião da Associação para o Software Livre (ANSOL), a LC está mal redigida pois veio criminalizar os sujeitos que escrevem software e investigam na área de segurança informática.

O representante da ANSOL, afirma que a "forma de investigar na área da segurança consiste precisamente na escrita e difusão de 'software' com a intenção de explorar vulnerabilidades de outros 'software'. É desta forma que são encontradas as vulnerabilidades e, normalmente, a única forma de convencer um fabricante comercial de 'software' a investir dinheiro na correcção dos erros no seu 'software'".[30]

Estes actos, segundo a LC, passam a ser criminalizados com pena de prisão, pelo que o presidente da ANSOL afirma que "ao ilegalizar a escrita e publicação de 'software' na área da segurança informática, os legisladores estarão a pôr em causa a segurança nacional a prazo, pois terão ilegalizado actos essenciais ao desenvolvimento de 'software' robusto e menos susceptível a vulnerabilidades".

A par da opinião da ANSOL, a direcção da Associação Liberdade na Era Digital (LED) realça que existem artigos que vão "obstaculizar a maior parte do ensino e investigação sobre segurança informática, na medida em que tornam ilícitas a produção ou a distribuição, mesmo no contexto de um estabelecimento de ensino e de programas informáticos que possibilitem a intercepção ilegítima de transmissões de dados ou o acesso a sistemas informáticos".[31]

[30] Rui Seabra in Artigo SOL
[31] Sandra Pinto in Artigo SOL

3.1.4. A Lei do Cibercrime

A Lei n.º 109/91 foi revogada pela Lei n.º 109/2009, de 15 de setembro, que aprovou a lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, 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, adotada em Budapeste em 23 de novembro de 2001.

A análise aos artigos da LC será feita como pressuposto da qualificação de uma determinada acção/omissão penalmente relevante, resultante do comportamento humano dominável pela vontade, exceptuando-se, claro, os casos de coacção e actos inconscientes.

Importa pois determinar o tipo legal de crime previsto, pois só através da tipicidade podemos concluir pelos outros elementos do crime. Trata-se de um juízo provisório de punibilidade, pois só com a sua verificação faz sentido avançar para uma análise dos seus elementos objectivos e subjectivos, imputando ou justificando o resultado que o agente produziu.

Para que se verifique a ilicitude do acto, tem que existir uma conduta que contrarie uma norma de direito que pretende tutelar bens jurídicos, sendo estes que justificam a sua existência. Torna-se imprescindível compreender que bem jurídico se pretende proteger com aquela norma.

Para que o agente seja criminalmente responsável não pode existir uma causa de exclusão da ilicitude, sendo que o mesmo se aplica à culpa, encarada como um juízo de desvalor sobre o agente que optou por actuar ilicitamente.

Podemos estar perante um concurso de crimes e de normas, pelo que a medida da pena só é determinada após a interpretação das normas.

A Constituição da República Portuguesa prevê, no seu art. 29º, os casos em que a lei criminal deve ser aplicada, pelo que o agente que pratique um dos actos previstos nos tipos de crime da LC, só pode ser punido quando se verifiquem as circunstâncias de aplicabilidade da lei criminal, respeitando os preceitos do art. 18º do mesmo diploma que estabelecem regras à restrição de direitos liberdades e garantias.

No Capitulo I, define o **artigo 1º** que "A presente lei estabelece as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptando o direito interno à Convenção sobre Cibercrime do Conselho da Europa".

Importa, para este trabalho, fazer referência às **definições** constantes no **art. 2º**, que transpõem para a ordem jurídica interna as constantes na Convenção sobre o Cibercrime, são elas:

- "*Sistema informático*, qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção;"[32]
- "*Dados informáticos*, qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função;"
- "*Dados de tráfego*[33], os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente;"
- "*Fornecedor de serviço*[34], qualquer entidade, pública ou privada, que faculte aos utilizadores dos seus serviços a possibilidade de comunicar por meio de um sistema informático, bem como qualquer outra entidade que trate ou armazene dados informáticos em nome e por conta daquela entidade fornecedora de serviço ou dos respectivos utilizadores; "
- "*Intercepção*", o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros;"
- "*Topografia*, uma série de imagens ligadas entre si, independentemente do modo como são fixadas ou codificadas, que representam a configuração tridimensional das

[32] A LC adita a parte final que vai de encontro ao art.1º a) da DQ 2005/222/JAI
[33] Definição diferente da dada pela Lei nº41/2004 de 18 de Agosto que distingue entre dados de tráfego e dados de localização
[34] Na definição dada pela CCib "Prestador de serviços", a LC preferiu optar por "Fornecedor de serviços"

camadas que compõem um produto semicondutor e na qual cada imagem reproduz o desenho, ou parte dele, de uma superfície do produto semicondutor, independentemente da fase do respectivo fabrico;"

- "*Produto semicondutor*, a forma final ou intermédia de qualquer produto, composto por um substrato que inclua uma camada de material semicondutor e constituído por uma ou várias camadas de matérias condutoras, isolantes ou semicondutoras, segundo uma disposição conforme a uma configuração tridimensional e destinada a cumprir, exclusivamente ou não, uma função electrónica."

A LC optou por não transpor a definição de "pessoa colectiva" constante na DQ 2005/222/JAI considerada "qualquer entidade que beneficie desse estatuto por força do direito aplicável, com excepção do Estado ou de outras entidades de direito público no exercício das suas prerrogativas de autoridade pública e das organizações internacionais de direito público"

- **Disposições materiais**

As disposições materiais constantes no capítulo II da LC encontram-se previstas nos arts. 3º a 8º, sendo que os arts. 9º e 10º reportam-se à responsabilidade das pessoas colectivas e perda de bens, respectivamente.

Assim, a LC considera crime:

- **Falsidade informática – art. 3º**
- **Dano relativo a programas ou outros dados informáticos – art. 4º**
- **Sabotagem informática – art. 5º**
- **Acesso ilegítimo – art. 6º**
- **Intercepção ilegítima – art. 7º**
- **Reprodução ilegítima de programa protegido – art. 9º**

3.1.4.1. Falsidade informática

A falsidade informática, tipo de crime, previsto no art. 3º da LC, não introduziu grandes alterações ao tipo já conhecido com a LCI[35]. É de salientar, apenas, que na revogada LCI, exigia-se que os dados ou programas fossem susceptíveis de servirem como meio de prova, onde a sua visualização produzisse os mesmos efeitos de um documento genuíno, ou seja, não era necessária a efectiva produção de documentos ou dados, enquanto que no novo art. 3º da LC e como iremos constatar, o elemento objectivo centra-se na produção de "dados ou documentos não genuínos" e o subjectivo na "intenção de provocar engano nas relações jurídicas". De resto transpôs para a ordem jurídica interna, algumas expressões e exigências do o art. 7º da Convenção sobre o Cibercrime.

Ao analisarmos o art. 3º da LC, podemos concluir que estão aqui previstos vários tipos de crime. O nº1 deste art., tem como objectivo aproximar a nova lei do cibercrime das evoluções operadas no mundo da tecnologia, como oportunamente já analisado.

Pretende-se através da tipicidade determinar o tipo legal de crime, sendo que o legislador ao tipificar determinados comportamentos pretendeu tutelar certos bens jurídicos, como já referido na introdução a este tema.

Os elementos objectivos do tipo pretendem imputar o resultado ao agente, através de uma análise ao agente, conduta praticada, objecto e resultado. É necessário que o resultado possa ser imputado ao agente que praticou a acção, ou seja, é necessário que se verifique um nexo de causalidade entre a acção e o resultado, como resulta do previsto no art. 10º do CP sob a epígrafe "Comissão por acção e por omissão", inserido no capítulo dos "Pressupostos da Punição. Assim "quem (…) introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos", preenche o tipo objectivo do crime de falsidade informática, previsto no art. 3º da LC.

Ao considerar como crime estas acções o legislador pretendeu tutelar a integridade das relações jurídicas enquanto interesse público, nomeadamente a veracidade dos documentos ou dados utilizados no âmbito destas relações. Estes dois elementos são constantemente utilizados nas relações jurídicas da sociedade, daí a importância que revestem como meios probatórios, nomeadamente os documentos. As constantes mudanças que se têm verificado no mundo da informática obrigam a que se tutele determinados bens como a

[35] Art. 4º LCI

segurança jurídica nas relações entre os sujeitos. A consequência que poderá advir de uma falsificação de documento ou dado que cause engano numa determinada relação jurídica é bastante para que se tipifique como crime tal conduta. Pensemos, por exemplo, no caso em que um sujeito modificou dados informáticos de um notário, produzindo desta forma uma escritura pública de compra e venda de uma casa, com intenção de obter para si, indevidamente, o bem imóvel. Um outro exemplo pode ser o caso em que o agente introduz dados informáticos, num sistema informático do Estado, produzindo um documento que servirá de base a um concurso público ou então os casos de «phishing», como refere o **Acórdão do Supremo Tribunal de Justiça** de 18-12-2013, Processo nº 6479/09.8TBBRG.G1.S1[36] "(do inglês fishing «pesca») pressupõe uma fraude electrónica caracterizada por tentativas de adquirir dados pessoais, através do envio de e-mails com uma pretensa proveniência da entidade bancária do receptor, por exemplo, a pedir determinados elementos confidenciais (número de conta, número de contrato, número de cartão de contribuinte ou qualquer outra informação pessoal), por forma a que este ao abri-los e ao fornecer as informações solicitadas e/ou ao clicar em links para outras páginas ou imagens, ou ao descarregar eventuais arquivos ali contidos, poderá estar a proporcionar o furto de informações bancárias e a sua utilização subsequente".

Sem esquecer o facto de que estas condutas podem preencher outro tipo de crime, para além da "falsidade informática", podemos concluir que o resultado destas acções, introdução e modificação de dados informáticos, pretende causar engano nas relações jurídicas, daí que o legislador tenha tido o cuidado de tutelar a integridade das mesmas, dado o seu interesse público, ao punir tal conduta.

Estamos, perante uma imputação do resultado ao agente que teve "intenção de provocar engano nas relações jurídicas", elemento subjectivo do crime, através da produção de "dados ou documentos não genuínos". Estamos perante um duplo dolo, conforme dispõe o art. 13º e 14º do CP, que prevê a actuação do agente em dois momentos: provocar engano nas relações jurídicas; com a produção de dados ou documentos não genuínos. A lei exige um dolo específico – provocar engano nas relações jurídicas – sendo que o agente, conhecendo os elementos da factualidade típica, teve intenção de praticar tal acto.

Pode dizer-se que o agente pretende que os documentos ou dados ilicitamente produzidos sejam considerados legítimos nas relações jurídicas. Aqui os actos do agente,

[36] www.dgsi.pt

digam-se actos de "falsificação" incidem sobre um programa ou dados informáticos com vista a obter documentos ou dados de forma ilegítima.

Com os elementos objectivos e subjectivos do tipo preenchidos, teremos sempre que analisar se não se verifica nenhuma causa de exclusão da ilicitude do acto, previstas nos artigos 32º a 39º do CP, sendo que a falta de um qualquer pressuposto objectivo ou subjectivo, ali previstos, determina a inexistência de uma causa de justificação. Só após comprovada a sua ausência pode ser dado à conduta do agente um juízo de culpa, de desvalor sobre quem optou por agir ilicitamente. Para que esta se verifique o agente tem que ter conhecimento da ilicitude e liberdade de decisão para mesmo assim praticar tal conduta, afastando-se a culpa nos casos em que se verifique uma causa de exclusão, seja em termos de inimputabilidade, art. 19º e 20º do CP, seja por erro não censurável sobre a ilicitude ou sobre as proibições, arts. 17º nº1 e 16 nº1 do CP ou mesmo por estado de necessidade desculpante ou medo quando actue em legitima defesa – arts. 35º e 33º nº2 do CP.

Para quem pratique as acções descritas no nº1 do art. 3º da LC, a moldura penal é até 5 anos de prisão ou 120 a 600 dias de multa. Atendendo a esta vertente e de acordo com os artigos 22º e 23º do CP a tentativa é punível, pois ao crime previsto corresponde pena de prisão superior a 3 anos, sendo que nestes casos a pena é especialmente atenuada, visto que os actos não se chegaram a consumar.

É punido como autor, quem executar o facto – autor – tomar parte dele – co-autor – ou determinar outra pessoa à prática do acto desde que haja execução – instigador, assim prevê o art. 26º do CP. Se retomarmos um dos exemplos a cima descritos, seria igualmente punido como a autor, não só quem praticou a acção de introduzir ou modificar dados para gerar uma escritura pública, como quem por exemplo pagou ao agente determinada quantia monetária para que este praticasse a acção. No caso de alguém prestar auxilio material ou moral, no caso concreto apoiar por exemplo, o agente a introduzir ou modificar os dados, é punido como cúmplice, sendo a sua pena especialmente atenuada – art. 27º do CP.

O nº2 do art. 3º, prevê os casos em que a acção praticada no número anterior incide sobre "dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistemas de comunicação ou a serviço de acesso condicionado". Estamos perante os casos de falsificação informática em cartões bancários, cartões SIM, considerado como uma identificação do titular do cartão para aceder a uma determinada rede móvel. O mesmo se aplica a outros que permitam o acesso a um serviço condicionado.

Estamos perante uma agravação do tipo legal, com uma agravação da pena, tendo o legislador intenção de tutelar dados financeiros. Atendendo à tutela que se pretende dar a este tipo de dados, inclusive pelo art. 35º da CRP, sentiu-se necessidade em aumentar a moldura penal nos casos em que o agente pode seriamente colocar em risco dados financeiros considerados na prática como dados de elevada importância. Quem, com intenção de provocar engano nas relações jurídicas, introduzindo, modificando ou apagando dados informáticos que incidam sobre "dados registados ou incorporados em cartão de crédito (…)", produzindo dados ou documentos não genuínos é punido com uma pena de prisão de 1 a 5 anos.

A protecção que a lei dá aos cartões bancários, impõe que se conjugue esta disposição com o previsto nos art. 267º nº1 c) e 262º nº1 do CP. A lei prevê como tipo de crime a falsificação de moeda, art. 262º CP, punindo tal conduta com pena de prisão. Os cartões de crédito são equiparados à moeda pelo art. 267º nº1 c). A questão que se coloca é a de saber se a falsidade informática tal como vem prevista no art. 3º nº2 da LC, não colide com o disposto no CP que pune quem falsificar moeda, com intenção de a pôr em circulação.

À primeira vista há que relembrar que o CP não define o que considera «contrafacção», contudo no seu art. 256º elenca diversas situações de «falsificação ou contrafacção de documentos». Como refere Pedro Miguel Figueira Verdelho, no seu comentário das Leis Penais Extravagantes[37], "Embora este tipo de linguagem se afigure, numa primeira abordagem, pouco conciliável com as realidades informáticas e os documentos digitais, é importante considerar, a este propósito, que o Código Penal considera o chamado «documento informático» como um verdadeiro documento", reconhecendo inclusive a existência de «documento electrónico»[38], considerando-o documento físico. A intenção do legislador na redacção desta norma não foi proteger os crimes de falsificação cometidos por meio informático, até porque se analisarmos o art. 262º do CP, apenas se exige que exista falsificação de moeda com intenção de a pôr em circulação, diferentemente do art. 3º da LC que exige que a falsificação do documento ou dado seja feita por meio informático, através de uma das acções tipificadas no artigo, com a intenção de provocar engano nas relações jurídicas. A LC exige elementos ausentes do CP, para punir tal conduta pelo que se pode considerar que o nº2 do art. 3º da LC retira qualquer aplicação prática da remissão operada pela alínea c) do nº1 do art. 267 do CP, como refere Pedro Miguel Figueira Verdelho[39].

[37] Albuquerque, Paulo Pinto de e Branco, José, Volume I, pág. 507, 2010, Universidade Católica Editora
[38] Art. 2º do DL nº 290-D/99 de 2 de Agosto
[39] Albuquerque, Paulo Pinto de e Branco, José, Volume I, pág. 507, 2010, Universidade Católica Editora

O nº 3 prevê os casos em que o agente é um utilizador dos meios elencados no nº1 e 2 do mesmo artigo, onde da sua acção resulte prejuízo a outrem ou benefício ilegítimo para o agente ou terceiro. Diferentemente do que sucede nos números anteriores, na forma simples do tipo de crime, aqui é exigido ao agente um dolo especifico "intenção de causar prejuízo a outrem ou obter beneficio ilegítimo", sendo a medida da pena prevista no nº1 e 2º.

O nº4 pretende tutelar as situações de comercialização de dispositivos que resultem das acções previstas no nº2. Esta norma corresponde ao previsto no art. 6º da Convenção sobre o Cibercrime, sob a epígrafe "Utilização indevida de dispositivos" e pretende punir a difusão dos crimes previstos no nº2 do mesmo artigo. A pena aplicável ao agente que praticar a acção descrita na norma é de 1 a 5 anos de prisão.

O legislador na parte final do nº4 "sob o qual tenha sido praticada qualquer das acções prevista no nº2", quis e de acordo com a Convenção sobre o Cibercrime, punir os casos de produção, distribuição e de mera detenção daqueles dispositivos. Apesar da redacção não ser a mais correcta, entende-se ser esta a opção do legislador e não aquela que resulta da letra da lei – a efectiva utilização dos dispositivos.

Note-se que o nº5 do art. 3º da LC, prevê uma agravação na pena nos casos em que as acções descritas nos números anteriores foram praticadas por um funcionário no exercício das suas funções, dada a especial censurabilidade, a pena a aplicar é de 2 a 5 anos de prisão.

O Ministério Público tem legitimidade para promover o processo penal de acordo com o art. 48º do CPP, exceptuando-se os casos em que o procedimento criminal dependa de queixa ou de acusação particular, arts. 49º, 50º, 51º e 52º do CPP. Para que tal aconteça a lei tem que prever expressamente os casos em que o processo penal dependa de queixa ou acusação particular, sendo que nos casos em que nada é referido, entende-se que o Ministério Público tem legitimidade para impulsionar o processo, tratando-se, portanto, de um crime público.

Há, ainda que referir, no âmbito da análise ao tipo de crime "falsidade informática" que esta distingue-se do dano relativo a programas ou outros dados informáticos, previsto no art. 4º do mesmo diploma legal, pois apesar de nos dois casos estarmos perante a introdução, modificação, supressão, interferência no tratamento de dados, a falsidade informática impõe um dolo especifico, " a intenção de provocar engano nas relações jurídicas", conforme dispõe o nº1, através de documentos ou dados não genuínos e produzidos através de uma das formas elencadas.

Jurisprudência[40]:

Acórdão do Tribunal da Relação do Porto de 21-11-2012

Processo nº: 1001/11.9JAPRT.P1

Relator: Borges Martins

Sumário: "I - O crime de "Passagem de Moeda Falsa", p. e p. pelos artigos 265º, n.º 1, al. a) e 267º, n.º 1, al. c), do Código Penal protege a "confiança ou fé pública na moeda" (Prof. Beleza dos Santos, in RLJ, 64, 275/276, 290/291 e 305/307), a "segurança e funcionalidade (operacionalidade) do tráfego monetário ou ambos" (Prof. Almeida Costa, in Comentário Conimbricense do Código Penal, II, 739), falando-se também na "pureza ou autenticidade do sistema monetário", ou mais explicitamente na "integridade ou intangibilidade do sistema monetário em si mesmo considerado (cfr. Comentário Conimbricense do Código Penal, II, 749), no interesse público da genuinidade respectiva de que é garante e nele encabeça o banco emissor";

II - Trata-se de um crime material ou de resultado que se consuma quando a moeda falsa penetra na esfera de disponibilidade do destinatário, sendo um delito de execução livre ou não vinculada;

III – O crime de **falsidade informática** p. e p. pelos artigos 3°, n°s 1 e 3, da Lei 109/2009 de 15.09, visa proteger a integridade dos sistemas de informação, pretendendo-se impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados - Preâmbulo da Convenção sobre Cibercrime do Conselho da Europa, in D R Iª Série A, 15-09-2009;

IV- O crime de Passagem de Moeda Falsa e o crime de **falsidade informática** estão em relação de concurso efectivo".

Acórdão do Tribunal da Relação de Lisboa de 10-07-2012

Processo nº: 7876/10.1JFLSB.L1-5

Relator: LUÍS GOMINHO

Sumário: "I. O crime de falsidade informática previsto no art.3, nºs1,2 e 3, da Lei nº109/09, de 15Set., não veio esvaziar de sentido a al.c, do nº1, do art.267, do Código Penal,

[40] www.dgsi.pt

continuando este preceito a abranger a conduta que se traduza em adulteração de cartões de crédito;

II. No crime de contrafacção de moeda o bem jurídico protegido é a integridade ou intangibilidade do sistema monetário legal em si mesmo considerado, aqui representado pelos cartões de crédito por via da sua equiparação àquela".

Acórdão do Tribunal da Relação de Lisboa de 30-06-2011

Processo nº: 189/09.3JASTB.L1-5

Relator: FILOMENA LIMA

Sumário: "Iº Aderindo todos os agentes a um propósito comum e sendo as acções de cada um idóneas e necessárias à produção do resultado pretendido por todos, nomeadamente através de actos que garantam segurança e impunidade, estamos perante uma situação de co-autoria;

IIº O bem jurídico protegido pelo crime de contrafacção de moeda (art.262, do Código Penal), é a intangibilidade do sistema monetário, incluindo a segurança e credibilidade do tráfego monetário;

IIIº Para o efeito, o cartão de crédito constitui verdadeira moeda, tutelando aquele tipo legal a fiabilidade e confiança na circulação da moeda na versão moderna do chamado dinheiro de plástico;

IVº O bem jurídico protegido pelo crime de falsificação informática (art.3, nº1, da Lei nº109/09, de 15Set.), é a integridade dos sistemas de informação;

Vº Tendo os agentes duplicado e utilizado cartões de crédito e tido acesso a dados que se encontravam em cartões de débito, produzindo com estes dados documentos não genuínos para os utilizar no levantamento de dinheiro ou pagamento de bens, praticaram, em concurso efectivo, aqueles dois crimes;

VIº A simples existência de ATM espalhados pela cidade e o facto de a primeira acção não ter sido logo detectada, não é susceptível de integrar a facilitação ou solicitação exterior à prática do crime, indiciadora de menor grau de culpa em cada nova actuação, que permita reconduzir a conduta à figura do crime continuado".

3.1.4.2 Dano relativo a programas ou outros dados informáticos

O art. 4º prevê o tipo de crime relativo a dano em programas ou dados informáticos, através de uma utilização indevida. Esta conduta era já prevista na LCI, no seu art. 5º, mas agora o novo art. da LC, introduz novidades constantes na Convenção sobre o Cibercrime[41] e da Decisão-Quadro 2005/222/JAI, relativo a ataques contra sistemas de informação, não no seu nº1, que reproduz o que constava do antigo art. 5 da LCI, retirando a exigência de dolo especifico. Pretendeu o legislador, à semelhança do que sucedeu com outros artigos, tutelar situações em que a conduta do agente preenche o tipo de crime, independentemente da intenção que subjaz à acção praticada.

Deve conjugar-se este artigo com o que dispõe o art. 2º b) da LC referente à definição de «dados informáticos».

O tipo objectivo do crime de dano relativo a programas ou outros dados informáticos consiste na acção ilegítima de "apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso". O agente pode actuar, apagando dados do sistema, destruindo o próprio sistema, por exemplo por agressão física, danificar programas informáticos que estão em curso no próprio sistema, sendo que todas estas acções podem tornar não utilizáveis tais dados ou programas. Tomemos como exemplo o agente que sem autorização apaga dados dos utentes de um serviço público de saúde, impossibilitando a sua consulta por parte dos médicos. Sem considerarmos a possibilidade de enquadrar esta conduta noutros tipos de crime, será de considerar que com esta acção, o agente preencheu a conduta prevista no nº1 do art. 4º da LC pois sem para tal estar autorizado apagou dados informáticos tornando não acessível a sua consulta.

A LC revogou a exigência de dolo específico antes previsto pela LCI "causar prejuízo a outrem ou obter benefício ilegítimo". Neste caso basta que o agente de forma ilegítima modifique dados ou programas informáticos de forma a interferir na sua capacidade de uso, para que a sua conduta preencha o tipo objectivo do crime. Deixa de se exigir que o agente actue com aquela especial intenção, pondo de parte o motivo pelo qual o agente actuou, bastando que represente aquele facto actuando com intenção de o realizar – art. 14º CP. Ao contrário do que sucede com o crime de falsidade informática, aqui o agente pode ser punido a título negligente, nos casos em que por exemplo exista violação de um dever de

[41] Art. 4º da Convenção sobre o Cibercrime

cuidado. Se o sujeito modificou dados ou programas, sem representar a possibilidade de que os iria tornar inacessíveis, actuou de forma negligente, sendo punido de acordo com as regras do art. 15º do CP.

Nos casos em que se não verifique erro sobre os elementos de facto ou de direito do tipo de crime – art. 16º do CP, para que a acção seja penalmente relevante, o agente tem que praticar as acções previstas no nº1, sem permissão legal ou sem para tal estar autorizado, pelo que se por exemplo for autorizado por lei ou pelo titular do direito, verifica-se uma causa de exclusão da ilicitude, não sendo por isso punido. Pensemos no caso em que o titular de um determinado sistema informático autoriza o agente a apagar dados, impossibilitando a sua consulta futura, neste caso o agente apesar de preencher o tipo objectivo do crime de "dano relativo a programas ou dados informáticos", não preenche a ilicitude do acto, não sendo por este punido.

O juízo de censura que recai sobre o agente, atendendo ao que dispõe o art. 40 do CP, sobre as "Finalidades da pena e medidas de segurança", impõe que não se verifique uma das causas que excluem a culpa, como analisado anteriormente.

Quem praticar uma das acções previstas no nº1, preenche o tipo objectivo do crime, verificando-se que não existem causas que justificam a ilicitude ou excluem a culpa, o agente é punido com pena de prisão até 3 anos ou pena de multa. Aplicam-se aqui as mesmas considerações tecidas no artigo anterior no que respeita à punibilidade do autor, co-autor e cúmplice.

O nº2 do art. 4º dispõe que a tentativa é punível, pelo que o agente que praticar actos de execução deste tipo de crime, previstos no art. 22º do CP, sem que este chegue a consumar-se, é, igualmente punido. O nº1 do art. 23º do CP dispõe que "salvo disposição em contrário, a tentativa só é punível se ao crime consumado respectivo corresponder pena superior a três anos de prisão", ora o nº2 do art. 4º da LC é considerado uma disposição em contrário, pelo que sendo a pena de prisão aplicada até 3 anos, o agente é na mesma punido pela tentativa. Contudo e de acordo com o nº2 o art. 23º do CP, a pena sofre uma especial atenuação.

O nº3 do art. 4º da LC, é uma novidade trazida pela LC, que vai de encontro ao que dispõe a Convenção sobre o Cibercrime no seu art. 6º. Assim pretende-se criminalizar quem difundir os meios previstos no nº3, os chamados «malwares»[42], com vista a praticar o crime de dano previsto no nº1. Trata-se mais uma vez de uma antecipação penal que pretende evitar

[42] Ver Pág 22 - Tipos de ataques

a consumação de outros tipos de crimes, nomeadamente do crime de dano que se pode vir a verificar pela conduta tipificada. Estamos aqui perante um crime de perigo, surgido pela evolução da realidade informática que obrigou o legislador a prever situações em que a difusão de um vírus, por exemplo por via de spam, seja punível mesmo que não chegue a produzir os seus efeitos. Esta opção do legislador foi criticada, nomeadamente por operadores de segurança dos sistemas de redes, ao considerarem que os testes que estes realizam possam ser considerados crimes. Contudo, esta opinião não logrou pelo facto de ser necessário para preencher o tipo de crime de dano previsto no art. 4º da LC a falta de permissão legal ou autorização do proprietário. Assim o legislador apenas quis tipificar como crime as condutas de acesso ilegítimo e não nos casos em que, por exemplo, o dono do sistema dá autorização para a realização de testes.

O nº4 e 5º do art. 4º da LC prevêem uma agravação na medida da pena aplicável em função da produção de um determinado resultado – quando o dano causado for de "valor elevado" ou "consideravelmente elevado". Pretende o legislador tutelar de uma forma mais exigente os casos em que da actuação do agente resulte um dano maior no património do lesado. Estando em causa valores de extrema importância, como a paz social e a confiança e segurança nos meios electrónicos, compreende-se que a pena aplicável seja agravada. Deve conjugar-se esta disposição com o art. 18º do CP "Agravação da pena pelo resultado", sendo que o agente tem que ser imputado pelo menos a título de negligência.

O último número deste artigo, estabelece que o "procedimento penal depende de queixa", nos casos do nº1, 2 e 4 – nº6 do art. 4º da LC. Assim, para que o Ministério Público tenha legitimidade para diligenciar no âmbito do processo, deve existir uma queixa, por quem tenha igualmente, legitimidade para o fazer, de forma a impulsionar a acção penal, art. 49º do CPP. Na classificação dos tipos de crimes, devemos incluir este tipo nos crimes semi-públicos. Contrariamente acontece nos casos em que o dano for de "valor consideravelmente elevado", de acordo com o nº5, tratando-se de um crime público, não sendo necessária queixa para o desenrolar do procedimento penal, cabendo ao Ministério Público impulsionar o processo – art. 48º do CPP.

Como anteriormente referido, a LC tutela situações semelhantes às do Código Penal. Por exemplo o crime de dano, previsto no art. 212º do CP, é considerado um crime de dano comum. Ambas as normas pressupõem uma actuação não autorizada, sobre coisa alheia, considerando-se crimes contra o património, embora em perspectivas diferentes. No crime de dano previsto no CP, o agente destrói, danifica, desfigura ou torna inacessível coisa alheia,

enquanto que para o tipo objectivo do crime de dano previsto na LC se encontrar preenchido, o agente sem estar autorizado para tal, apaga, altera, destrói ou danifica, tornando inutilizáveis ou inacessíveis programas ou outros dados informáticos. Em ambos os casos o agente actua sobre um objecto alheio, seja uma "coisa alheia" como dispõe o CP ou sem permissão legal em programas ou dados informáticos como previsto na LC. O bem jurídico protegido nas duas normas não é exactamente o mesmo, pois no crime de dano previsto no CP o bem jurídico tutelado é o património, enquanto que a LC vai mais longe, não se preocupando apenas com a integridade patrimonial do objecto, mas sim com a integridade e funcionalidade dos dados ou programas informáticos.

O crime de dano relativo a programas ou outros dados informáticos, pretende proteger a integridade e fiabilidade de dados e o bom funcionamento dos programas informáticos, sendo exactamente este o bem jurídico tutelado por esta norma. A Constituição da República Portuguesa no seu art. 35º dispõe sobre a utilização da informática, garantindo aos cidadãos o acesso aos dados informáticos que lhes digam respeito. Os dados e programas informáticos a correr num sistema informático estão aptos a produzir determinadas acções e/ou funcionalidades, pelo que se pune uma acção não autorizada de um terceiro sobre estes.

Paralelamente ao crime de dano previsto no CP que protege os bens corpóreos, a LC vem tutelar uma outra vertente, nomeadamente os danos deliberados que possam ocorrer em programas ou dados informáticos. A LC vai um pouco mais longe, tutela o correcto funcionamento e utilização dos programas ou dados informáticos, não se limitando apenas por uma interferência ilegítima nos mesmos. A LC pretende efectivamente proteger os dados ou programas informáticos, daí a sua natureza informática, prescindindo inclusive da consumação do acto. [43]

Importa, ainda, distinguir o crime de dano previsto no art. 4º da LC com o crime de burla previsto no art. 221º nº1 do CP. O tipo objectivo da burla é a intenção de obter para si ou para terceiro enriquecimento ilícito, causando prejuízo patrimonial a outrem através da manipulação informática de dados ou programas informáticos. Mais uma vez, o bem jurídico tutelado pelo crime previsto no art. 221º nº1 do CP é de natureza patrimonial.

A Lei de Protecção de Dados Pessoais, prevê no seu art. 45º o crime de "viciação ou destruição de dados pessoais". Esta lei pretende tutelar só e directamente os dados pessoais, enquanto que a LC tutela todos os tipos de dados informáticos, independentemente da sua

[43] Rodrigues, Benjamim Silva, Direito Penal – Parte Especial I, Direito Penal Informático-Digital, Coimbra 2009, pág. 332

natureza. Benjamim Silva Rodrigues[44] defende que a LPDP prevalece sobre o crime previsto na LC, nas situações em que se trate dos "dados pessoais", dado o carácter da sua relação de especialidade, deixando desta forma, esta actuação, menos protegida devido à moldura penal que se apresenta menos gravosa, não excluindo de todo a sua conjugação com a LC.

3.1.4.3. Sabotagem informática

O art. 5º da LC, mantém-se no essencial idêntico ao antigo art. 6º da LCI, introduzindo pequenas inovações, como mencionado em pontos anteriores, que se tornaram imprescindíveis para fazer face a novas realidades e novas formas de tecnologia de informática. A crescente utilização da internet no dia-a-dia dos cidadãos para a realização de compras, pagamentos, transferências, e nas actividades de diversas empresas como a introdução de informações em bases de dados, a utilização de programas informáticos para o desenvolvimento da sua actividade, tornaram clara a necessidade de proteger a dignidade dos sistemas informáticos que possibilitam tais acções da sociedade.

A LC obedeceu aos critérios impostos pela legislação internacional, designadamente, a Convenção sobre o Cibercrime[45] e a Decisão-Quadro 2005/222/JAI do Conselho[46], integrando agora no art. 5º outras acções integradas no tipo de crime já conhecido..

Preenche o tipo objectivo do crime "quem sem permissão legal ou sem para tanto estar autorizado (…), entravar, impedir, ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento ou impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático". Para que seja possível imputar o resultado ao agente, este tem que actuar de acordo com as acções descritas, para que a interferência no sistema informático seja resultado daquelas acções. Pretende-se punir quem, por exemplo, interferir num determinado programa que se encontra a decorrer num sistema informático, causando dificuldades neste, mesmo sem que daí resultem danos ou prejuízos nos dados e programas. Não se exige uma especial intenção, pois o agente tem que actuar apenas com intenção de interferir no sistema informático, deve conhecer a

[44] Rodrigues, Benjamim Silva, Direito Penal – Parte Especial I, Direito Penal Informático-Digital, Coimbra 2009, pág. 455
[45] Artigo 7º
[46] Artigo 3º

realidade e actuar com intenção de praticar tal acto, independentemente do motivo que o levou a tal conduta, este é o dolo, elemento subjectivo do tipo, exigido pelo nº1 do art. 5º.

A lei exige que o agente actue sem para tanto estar legitimado, pelo que nos casos em que este esteja autorizado pelo titular do direito, a interferir no sistema através da alteração, por exemplo, de programas informáticos estamos perante uma causa de exclusão da ilicitude, não sendo aquele punido por tal conduta.

Se estiverem preenchidos os elementos objectivos e subjectivos do tipo, sem se verificar uma qualquer causa de justificação da ilicitude - art. 32º 34º, 36º 38º e 39º do CP ou de exclusão da culpa - art. 16º nº1, 17º nº1, 19º, 20º, 35º e 33 nº2 do CP, o agente é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

O bem jurídico protegido pela norma da LC é a segurança dos sistemas informáticos e das comunicações electrónicas, no seu pleno e normal funcionamento.

A grande alteração, operada no nº2[47], aliás como em quase todos os tipos de crimes previstos na LC, é a criação de um novo tipo de crime que consiste na difusão das condutas praticadas no nº1 do mesmo artigo, ou seja, por exemplo de vírus e outros programas ilícitos destinados a permitir a sabotagem informática, traçando a mesma moldura penal que está prevista no nº1. Pretende-se, mais uma vez, punir os actos preparatórios da prática de outros crimes, neste caso concreto os actos anteriores à utilização dos dispositivos para os fins ilícitos. Ex. Controlo de redes através de botnets[48] ou provocação de DOS e DDOS. A difusão de software destinada à criação de redes ilegais com estes propósitos passa a ser punível na mesma medida do nº1.

O nº3 dispõe que nos casos de difusão, nº2, a tentativa não é punível. O agente que pratique actos de execução, sem que o crime chegue a consumar-se não é punido por aqueles actos. Contrariamente acontece ao agente que nas mesmas condições pratique os actos referidos no nº1. Aqui é explicito que a LC pretendeu punir a tentativa, remetendo a sua aplicabilidade para os arts. 22º e 23º do CP.

Os nº4 e 5º agravam a medida da pena, de 1 a 5 anos de prisão ou de 1 a 10 anos, em função da agravação do resultado produzido, ou seja, em função da dimensão do dano emergente como fruto de uma crescente preocupação com os ataques informáticos que causam perturbação grave das comunicações informáticas – DOS e DDoS[49]. A alínea b) do nº5 prevê uma forma qualificada de sabotagem consoante a gravidade das suas consequências.

[47] Com referência ao art. 6º nº1 a) e b) da Convenção sobre o Cibercrime
[48] Ver pág. 22 – tipos de ataques
[49] Ver pág. 22 – tipos de ataques

Aqui os efeitos produzidos pelo agente causam uma perturbação grave ou duradoura num sistema informático, indispensável para a sociedade. Estamos a falar de encerramento ou bloqueamento de sites, dos ataques informáticos a grande escala que causam um forte impacto. O combate a este tipo de condutas é uma imposição da Decisão-Quadro – art. 7º.

Se atendermos ao bem jurídico tutelado no art. 5º da LC, compreendemos o porquê de se tratar de um crime público, cabendo ao Ministério Público uma acção directa no âmbito da sua protecção, art. 48º do CPP.

É de todo importante saber distinguir entre o crime de dano relativo a programas ou dados informáticos do crime de sabotagem informática, art. 4º e 5º da LC, respectivamente. No primeiro punem-se actos relacionados com dados informáticos e programas, enquanto que no segundo punem-se os actos que perturbem o funcionamento de um sistema informático ou comunicação de dados. Os bens jurídicos tutelados por ambos só se distinguem pelo objecto do crime, enquanto que no crime de dano o objecto do crime são dados informáticos, na sabotagem informática o objecto é o sistema informático.

O legislador pretendeu tutelar, aqui, o correcto funcionamento de um sistema informático, no seu todo. É natural que existam situações em que a mesma conduta se enquadra nos dois tipos. A diferença que reside nos dois é que no crime de dano o que se protege são os dados e os programas e no crime de sabotagem é todo o sistema informático.

No acesso ilegítimo, crime também previsto na LC, o bem jurídico protegido é a segurança do sistema informático, diferentemente dos casos de sabotagem informática onde o bem jurídico protegido é o do proprietário ou utilizador de um sistema informático em funcionalidades normais. Protege-se a liberdade e disponibilidade de gerir, operar e controlar os sistemas informáticos, sem qualquer tipo de perturbação, de forma a garantir a confidencialidade e integridade dos mesmos. A este propósito, **Acórdão do Tribunal da Relação de Coimbra de 15-10-2008, processo nº 368/07.8TAFIG.C1, sendo relatora Alice Santos[50].**

A sabotagem informática prevista pela LC não se confunde com a sabotagem prevista no CP no seu art. 329º. A sabotagem informática, art. 5º da LC, refere-se às ocorridas no âmbito de todo e qualquer sistema informático, não fazendo restrições ao seu âmbito de aplicação. Aplica-se a qualquer sistema informático que tenha sido alvo de uma interferência através dos seus dados ou programas informáticos. Contrariamente o art. 329º do CP preocupa-se com a natureza do crime, dimensão e importância económica, sendo que a

[50] www.dgsi.pt

vertente pública e o impacto nas actividades da população, terão que ser tidos em conta na aplicação deste artigo.

3.1.4.4. Acesso ilegítimo

O art. 6º da LC, por força das exigências de instrumentos internacionais[51], adaptou a redacção já existente na LCI, art. 7º, a novas realidades de forma a garantir a segurança dos sistemas informáticos, eliminando o dolo específico presente na revogada LCI – "intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos". Com a redacção dada a este artigo pela LCI, quando o agente acedesse ilicitamente a um sistema informático sem qualquer intenção de obter beneficio ou vantagem, a sua conduta não preenchia o tipo de crime de acesso ilegítimo. Com a entrada em vigor da LC, criminaliza-se o acto de aceder ilegitimamente a um sistema, independentemente da intenção do agente, basta que se verifique a conduta descrita para que seja imputada ao agente que a praticou. Tal como acontece na Alemanha no § 202ª STGB e em França, artigo 323 nº1 do Código Penal, o acesso ilegítimo não exige a intenção de obter beneficio ou vantagem.

Com o alargamento do âmbito de aplicação deste artigo, o legislador quis punir qualquer acto de acesso a um sistema que viole e coloque em causa a segurança deste. Pretende-se aglomerar todas as outras situações em que o agente aja desprovido de qualquer intenção de obter outros resultados que não seja apenas o de conseguir aceder a um sistema sem autorização do seu proprietário ou sem permissão legal. O simples facto de conseguir penetrar no seio de um sistema, ilegitimamente, é grave o suficiente para merecer tutela penal, atendendo à violação de privacidade causada pelo agente. Aqui, o comportamento posterior do agente não é tido em conta, a não ser nos casos em que a sua conduta preencha outro tipo de crime, pois o acesso pode ser realizado para obter benefícios ou vantagens, aceder a dados confidenciais, explorar falhas de segurança de sistemas, enfim inúmeras acções que podem ser praticadas após o acesso ilegítimo. Nestes casos, há que analisar a conduta do agente, podendo este preencher o tipo de crime de falsidade informática, se acedeu ilegitimamente a um sistema, de forma a causar engano nas relações jurídicas, através da falsificação de dados e produção de documentos ou dados não genuínos, ou o tipo de crime de sabotagem

[51] Art. 2º da Convenção sobre o Cibercrime e Art. 2º da Decisão-Quadro 2005/222/JAI do Conselho

informática, se com o acesso ilegítimo perturbou um sistema informático através de interferência de programas ou dados informáticos.

O acesso " é a entrada no todo ou em parte de um sistema informático (harware, componentes, dados armazenados no sistema instalado, directorias, dados de tráfego e dados relativos ao conteúdo)", Pedro Miguel Figueira Verdelho[52].

O tipo objectivo de crime – acesso ilegítimo a um sistema informático – impõe que este acesso seja realizado de forma não autorizada, o que exclui as situações de teste de seguranças autorizadas pelo titular do sistema, já referidas a propósito do art. 4º e nos casos de sistema aberto ao público, verificando-se uma causa de justificação da ilicitude.

Atendendo à nova redacção dada pela LC, já não é exigido um dolo específico, uma especial intenção por parte do agente, basta que actue com intenção de aceder ilegitimamente a um sistema informático para que a sua conduta preencha o tipo objectivo do crime de "acesso ilegítimo", tendo acesso resultado directamente da conduta praticada, estamos perante um dolo genérico.

Verificados os elementos objectivos e subjectivos do tipo de crime de "acesso ilegítimo", assim como a ausência de causas de justificação da ilicitude ou de exclusão da culpa,quem pratique os actos previstos no tipo de crime aqui previsto, é punido com uma pena de prisão até 1 ano ou com pena de multa até 120 dias.

O nº2 pretende punir a difusão, já mencionada na analise acima exposta referente aos demais artigos da LC., com o intuito de punir os actos preparatórios, mais concretamente a obtenção ilegítima de dados de acesso a sistemas protegidos. Não se trata da sua utilização, pois nestes casos já se poderia enquadrar a conduta noutro tipo de crime – seja do nº1 deste artigo ou no art. 5º sabotagem informática.

Quando o acesso seja feito por violações de regras de segurança, estabelece o nº3 do art. 6º, que a pena de prisão é até 3 anos ou multa.

O tipo de crime de acesso ilegítimo prevê uma forma qualificada atendendo à dimensão dos prejuízos causados ou dos benefícios obtidos, agravando a medida da pena em função do resultado. Assim estabelece o nº4, com agravação da pena de 1 a 5 anos de prisão quando o agente pratica as acções sobre condições que revelam uma especial censurabilidade.

Salvo nos casos de difusão, a tentativa de acesso ilegítimo – nº1, nº3 e 4º, é punível – nº5 do art. 6º da LC. O legislador fez questão de mencionar que a tentativa é punível, caso

[52] Albuquerque, Paulo Pinto de e Branco, José, Volume I, pág. 516, 2010, Universidade Católica Editora

contrário, segundo os princípios do direito penal no âmbito deste tipo de crime a tentativa não seria punível, como resulta no disposto do art. 22º e 23º do CP.

A lei estabelece que o procedimento penal depende de queixa, art. 49º do CPP, nos casos de acesso ilegítimo, nº1, e na sua forma qualificada previstas nos casos do nº3 e ainda quando se verifique um caso de tentativa, nº5. É considerado um crime semi-público, ao contrário do previsto no nº2 e 4, pois como se disse estamos perante um crime na sua forma agravado, pelo que a censura que recai sobre o mesmo, torna imprescindível uma acção directa do Estado, de forma a garantir a segurança que se pretende proteger. Na forma agravada o crime é público, tendo o Ministério Público legitimidade para prosseguir com o procedimento criminal, art. 48º do CPP.

A tutela concedida ao sistema informático, através da incriminação do acesso ilegítimo, pretende preservar a integridade do sistema informático, mais concretamente a inviolabilidade do domicílio informático, conforme consta da Recomendação nº9 (89) do Conselho.

Jurisprudência[53]:

Acórdão do Tribunal da Relação do Porto de 08-01-2014

Processo nº: 1170/09.8JAPRT.P2

Sumário: "V – O crime de acesso ilegítimo, previsto no art.º 6º da Lei n.º 109/2009, de 15/9, (Lei do Cibercrime), estruturalmente acolhe o crime anterior, previsto no art.º 7º da Lei 109/91, de 17/8, com alterações decorrentes dos compromissos internacionais que Portugal assumiu e, em particular, da Convenção sobre Cibercrime do Conselho da Europa.

V – A factualidade incriminada é exactamente a mesma que era antes, não se exigindo, agora, qualquer intenção específica, por exemplo, a de causar prejuízo ou a de obter qualquer benefício ilegítimo pois que apenas se exige o dolo genérico.

V - O bem jurídico protegido é a segurança do sistema informático.

VI - O crime de acesso ilegítimo é praticado por quem actue de forma não autorizada, concretizando-se por qualquer modo normalmente idóneo de aceder a um sistema ou rede informáticos".

[53] www.dgsi.pt

3.1.4.5. Intercepção ilegítima

A estrutura do tipo de crime, previsto na revogada LCI[54], não sofreu grandes alterações, sendo apenas introduzidas algumas novidades impostas pela Convenção do Cibercrime[55]. As expressões "rede informática" e "interceptar comunicações" foram retiradas, surgindo agora a lei mais adaptada à evolução tecnológica adoptando a designação "interceptar transmissões de dados informáticos".

Como dispõe o art. 7 nº1 da LC, estamos perante um tipo de crime, em que o seu tipo objectivo consiste na intercepção ilegítima de transmissões de dados informáticos que se processem no interior de um sistema informático, a ele destinado ou dele proveniente. No caso concreto, o agente, sem para tal estar autorizado, intercepta comunicações que ocorrem num sistema informático, através de meios técnicos, como por exemplo dispositivos de recolha e gravação de comunicações sem fios, uso de software e códigos. Deve conjugar-se este artigo, com a definição de "intercepção" constante na alínea e) do art. 2º da LC " «Intercepção», "o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros" e com a definição de «sistema informático» contida na a) "Qualquer dispositivo ou conjunto de dispositivos interligados ou associados (…)". Não se exige uma qualquer especial intenção por parte do agente, apenas que este actue com intenção de realizar uma intercepção ilegítima de transmissões de dados informáticos – dolo genérico – art. 13º e 14º CP.

De referir que é excluída a ilicitude quando o titular da transmissão de dados dê autorização para que se intercepte tais dados, o que sucede por exemplo nas empresas ligadas às Tecnologias de Informação que desenvolvem software ligado às intercepções de comunicações para fins lícitos. É, igualmente, excluída a ilicitude nos casos dos art. 187º e 189 do CPP, intercepção de comunicações, por força do que dispõe o art. 34 nº 4 CRP, salvaguardando os procedimentos processuais.

O agente que pratique a acção descrita no nº1 do art. 7º da LC incorre numa pena de prisão até 3 anos ou pena de multa.

O nº2 do art. 7º, pune a tentativa deste tipo de crime, sendo que para tal basta o agente tentar interceptar transmissões de dados, mesmo sem obter resultado, sendo aplicável as disposições constantes nos art. 22º e 23º do CP.

[54] Art. 8º
[55] Art. 3º

O procedimento criminal não depende de queixa, classificando-se assim, o crime como público, art. 48º do CP, dado à importância do bem jurídico que tutela por razões de ordem Constitucional.

O legislador pretendeu dar tutela a um dos direitos fundamentais previstos na Constituição da República Portuguesa e consagrado na CEDH no seu art. 8º, a vida privada. É este o bem jurídico protegido pela norma constante na LC, salvaguardando a confidencialidade das comunicações de dados informáticos. A protecção concedida à privacidade no âmbito das intercepções de comunicações como as escutas telefónicas, é aplicada, na mesma medida à intercepção de dados informáticos, pois de acordo com a nossa CRP, no seu art. 34º nº4, as telecomunicações e outros meios de comunicação, são invioláveis. O bem jurídico protegido pela norma da LC é a segurança e privacidade das comunicações electrónicas - da transmissão de dados.

O nº3, inovação já conhecida no âmbito dos tipos de crime já analisados, introduz uma alteração com o objectivos de punir actos preparatórios de outros tipos de crime, operados pela difusão de actos que permitam interceptar dados informáticos.

Cumpre sublinhar a semelhança deste artigo ao previsto no CP no art. 192 nº1 a), sob a epígrafe " Devassa da vida privada", punindo quem "interceptar (…) comunicação telefónica, mensagens de correio electrónico ou facturação detalhada". Ambos os artigos visam proteger a vida privada, contudo o tipo objectivo do crime difere sobre a acção do agente. Na intercepção ilegítima, prevista no art. 7º nº1, o agente, sem permissão, intercepta dados informáticos de um determinado sistema. Este é o principal objectivo – a acção de interceptar dados – seja qual for o motivo ou finalidade e sejam quais forem os dados. Contrariamente, no crime previsto no art. 192º nº1 a) do CP, o agente para devassar a vida privada, actua de acordo com uma ou várias das condutas descritas mas sempre sobre comunicação telefónica, correio electrónico ou facturação detalhada, tendo provavelmente conhecimento do seu conteúdo. Ao analisarmos os elementos subjectivos do tipo verificamos que o art. 7º da LC apenas impõe que o agente actue, tratando-se de um dolo genérico. O art. 192º do CP exige, por outro lado, um dolo específico por parte do agente, uma especial intenção de devassar a vida privada.

O mesmo não se diga do art. 194º nº2 do CP, "Violação de correspondência ou telecomunicações", que exige, da mesma forma que o art. 7º nº1 da LC, um dolo genérico. O agente age com intenção de se intrometer no conteúdo de uma comunicação electrónica, sem qualquer motivo especial e de forma livre e deliberada, tal como na intercepção ilegítima onde

o agente age interceptando os dados informáticos. Ambos preocupam-se com as comunicações e dados, sendo que o primeiro pune a intromissão no conteúdo das comunicações e dados e o segundo pune a sua intercepção.

3.1.4.6. Reprodução ilegítima de programa protegido

Para uma correcta análise do crime previsto no art. 8º da LC, importa conjugar o mesmo com o art. 14º do DL 252/94 de 20 de Outubro - Lei de protecção jurídica de computador, que remete para o art. 9º da LCI, que por interpretação correctiva se deve remeter para o art. 8º da LC. O nº1 do mencionado art. 14º refere que "Um programa de computador é penalmente protegido contra a reprodução não autorizada" e no seu nº2 que "É aplicável ao programa de computador o disposto no nº1 do artigo 9º da Lei nº109/91, de 17 de Agosto.

Esclarece Benjamim Silva Rodrigues, Direito Penal Especial, Direito Penal Informático-Digital, 2009, página 306 que o DL 252/94 refere "programa de computador" ao passo que a LCI dispõe "programa informático". Podemos entender que o legislador quis que a LCI englobasse todo e qualquer programa informático, mesmo que não se enquadre na definição de "programa de computador", como por exemplo nos casos de um programa usado por um robot. Conclusão que pode ser contestada no sentido em que muitas são as opiniões de encarar, igualmente, um robot como um computador dado as suas particularidades técnicas, assunto que não será aqui tratado. Assim, afigura-se pertinente no seio desta matéria apenas referir que o legislador permitiu, com o art. 8º da LC, estender a punibilidade de reprodução, sem legitimidade, de um programa protegido por lei, qualquer que seja o programa informático.

Importa referir que este artigo, quase inalterado ao que constava na antiga LCI, traduz o que vem previsto na Recomendação nº9 (89) do Conselho da Europa. Os instrumentos internacionais que estiveram na base da LC não contribuíram para a formulação desta norma, tendo inclusive suscitado grandes discussões, nomeadamente quanto à tutela penal do direito de autor sobre programas de computador.

Para que faça sentido a aplicação desta norma, deve conjugar-se os arts. 195º e 199º do CDADC e o art. 14º do DL nº 252/94 de 20 de Outubro, para que seja devidamente enquadrado o que se entende por programa protegido por lei.

O tipo objectivo do crime previsto no art. 8º consiste na reprodução, sem autorização, de um programa protegido, punindo com pena de prisão até 3 anos ou com pena de multa o agente que praticar tal conduta. A expressão "reprodução" não tem encontrado unanimidade na nossa doutrina. Os diplomas que regulamentam a matéria de programa protegido, como é o caso do DL 252/94 e do CDADC, numa primeira análise não definem o que se entende por "reprodução", prevendo apenas quando é possível ou não tal conduta consoante as circunstâncias. Resta-nos o art. 176 nº7 do CDADC que tem suscitado alguma controvérsia – "Reprodução é a obtenção de cópias de uma fixação ou de parte qualitativa ou quantitativamente significativa dessa fixação". Alguns autores defendem que o acto de reprodução "implica a fixação do programa num suporte de armazenamento electrónico-digital"[56], como por exemplo um CD Rom, DVD, USB, permitindo a sua utilização posterior. Outros defendem que para haver reprodução não se tona necessária a tal fixação, bastando apenas o armazenamento temporário do programa no computador. Entende Oliveira Ascensão[57] que se deve retomar a expressão tradicional de "reprodução" e restringi-la à criação de cópias. Não me parece de todo plausível este último entendimento, visto que o legislador pretende punir expressamente a reprodução de um programa que está protegido por lei. Independentemente do programa ficar armazenado no computador ou ser carregado para um outro dispositivo, houve efectivamente uma reprodução. Pensemos nos casos em que o agente efectua um «download» de um filme para o seu computador e não o copia para uma «pen» USB. Existiu uma reprodução do filme através do acto de descarregar para o computador, independentemente do destino daquele, o agente com esta conduta teve acesso a um programa protegido por lei, violando os direitos de autor. Não se afigura adequado que o legislador queira criminalizar a conduta de reproduzir programas protegidos, através de cópias para outros dispositivos, deixando de fora o agente que pratique o mesmo acto mas sem o reproduzir em cópias. A aplicabilidade da norma tornar-se-ia vazia, na medida em que o agente poderia obter os programas para o seu computador, fazer uso deles e não ser punido, ao passo que um outro agente que agisse da mesma forma mas realizando cópias do programa para um CD Rom, era punido por lei. Pensemos, por exemplo, num outro caso. O agente descarrega para o seu computador uma versão de um software mais actualizado que o existente no seu computador. Faria sentido deixar impune a conduta que, sem autorização do seu titular, instala um determinado programa informático no seu computador? Não parece

[56] Benjamim Silva Rodrigues, Direito Penal Especial, Direito Penal Informático-Digital, 2009, pág 314

[57] Ascensão, José de Oliveira, "Novas tecnologias e transformação do direito de autor", Estudos sobre o direito da internet e da sociedade da informação, Almedina, 2001

lógico nem de acordo com a «ratio-legis» da norma. O que está em causa é o acto de violar o direito de autor de um determinado programa sem a autorização do seu titular. Hoje em dia é cada vez mais comum as pessoas acederem a programas e dados informáticos, através da internet por exemplo, reproduzindo aqueles através de cópias, sem que para tanto o titular tenha autorizado. Podemos incluir neste âmbito as reproduções que se façam de obras literárias, vídeos, músicas e outros tipos de ficheiros. Foi uma grande revolução operada com o mundo das novas tecnologias, pois à distância de um «clic» qualquer pessoa pode ter acesso a programas que se encontram protegidos por lei, titulares de direitos, tendo inclusive a possibilidade em distribui-los.

Atendendo ao bem jurídico protegido pelo art. 8º, devemos considerar que se pretende proteger qualquer violação que exista a um programa que é protegido por lei, independentemente do destino da reprodução. O que está em causa é a violação dos direitos de autor, num âmbito mais abrangente face às novas realidade informáticas, pois qualquer que seja a reprodução que se faça, sem autorização do seu titular, de um programa protegido, independentemente do seu destino, o agente é punido.

É punido pela mesma norma, quem "divulgar ou comunicar ao público programa informático protegido por lei". Exige-se da mesma forma a falta de autorização por parte do titular do direito para divulgar ou comunicar certo programa informático. Trata-se de toda e qualquer actividade que possibilite a venda, aluguer ou outros actos de circulação do programa informático protegido por lei ao público no seu geral, ou seja, que esteja disponível a quem tiver interesse de lhe aceder.

Estas duas acções e a reprodução ilegítima não se confundem, pode haver uma sem a outra e podem existir as duas no mesmo tipo. Pune-se da mesma forma o agente que reproduz ilegitimamente o programa informático, como quem o difunde ou vende. Para nenhuma das modalidades é exigido dolo específico, pelo que não estará em causa a intenção da reprodução, divulgação ou comunicação ao público, estamos portanto perante um dolo genérico – art. 13º e 14º do CP.

Três considerações a fazer: para preencher, em primeira linha o tipo de crime previsto no art. 8º, o programa deve ser protegido por lei, recorrendo para tanto das disposições constantes na legislação já mencionada; deve também a sua reprodução, comunicação ou divulgação ao público ser efectuada sem autorização das entidades competentes ou do seu autor; não preenche o tipo legal de crime a conduta do agente que

reproduza, divulgue ou comunique ao público programa protegido por lei, cujo direito do titular já caducou[58].

O tipo de crime previsto na LC pune a violação do direito de autor e direitos conexos sobre programas de computador, tendo a Convenção sobre o Cibercrime imposto aos Estados assinantes a adaptação desta matéria ao legislado internamente sobre as violações de direito de autor, ou seja, a nível nacional seriamos remetidos para o Código dos Direitos de Autor e Direitos Conexos. Contudo, a legislação portuguesa, consagrou expressamente este crime na LC, protegendo de forma imediata o direito de autor e direitos conexos sobre programas informáticos, afastando a aplicação de qualquer preceito do CDADC, quando se verifique o tipo objectivo do crime de reprodução ilegítima de programa informático.

O bem jurídico tutelado pelo crime de reprodução ilegítima de programa protegido é a propriedade intelectual, dada a sua estreita ligação com o CDADC, através da protecção dos direitos dos titulares de programas. Pretende-se limitar, quando ocorra sem autorização do seu titular, a proliferação do programa protegido que poderá causar relevante prejuízo patrimonial.

O legislador sentiu necessidade de alargar a punição sobre estes tipos de conduta ao que era já protegido no direito do autor em geral, pois a falta de exigência de intenção lucrativa ou comercial, permite a aplicação do art. 8º da LC a muitos outros casos em que existe uma clara violação do direito de autor, como uma forte resposta à evolução sentida no âmbito de reprodução de programas informáticos.

O nº2 do art. 8º da LC pune da mesma forma "quem ilegitimamente reproduzir topografia de um produto semi-condutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia". A redacção deste número, parece numa primeira abordagem, pouco esclarecedora do que o legislador quis efectivamente criminalizar. Para perceber o alcance desta norma, impõe-se fazer uma remissão para o art. 2 alínea f) e g).

De acordo com o nº3 do art. 8º a tentativa é punível, pelo que deve remeter-se para os arts. 22º e 23º do CP.

O procedimento criminal não dependendo de queixa, pelo que tratando-se de um crime público, pelos bens que visa proteger, o Ministério Público tem toda a legitimidade em impulsionar a acção penal – art. 48º do CPP.

[58] Art. 36º do CDADC – o direito caduca 70 anos após a morte do autor , ou da sua licita divulgação e publicação.

Jurisprudência[59]:

Acórdão do Tribunal da Relação de Coimbra de 12-07-2006

Processo nº: 1161/06

Relator: Carlos Barreira

Sumário: "1. A instalação de um único programa informático licenciado em vários computadores de um empresa traduz-se numa reprodução de programa não autorizada.

2. O tipo legal de crime de reprodução de um programa informático protegido não exige intenção de lucro.

3. Para o preenchimento do tipo legal de crime é irrelevante que o programa não tenha sido reproduzido em suportes magnéticos móveis, mas apenas instalado noutros computadores".

Acórdão do Tribunal da Relação de Coimbra de 30-10-2013

Processo nº: 98/08.3EACBR.C1

Relator: Vasques Osório

Sumário: "O preenchimento da acção típica do crime de reprodução ilegítima de programa protegido, não exige a verificação cumulativa das três modalidades de acção previstas art. 9º, nº 1, da Lei n.º 109/91, de 17 de Agosto a saber, reprodução, divulgação e comunicação ao público, de programa informático protegido;

2.- Reprodução é a fixação da obra num meio que permita a sua comunicação e a obtenção de cópias, integrais ou não, dela, o que engloba a reprodução em CD como a reprodução na memória de computador;

3.- Tendo o arguido instalado um programa informático em computadores da sociedade que geria, sem que tivessem sido obtidas as necessárias licenças da proprietária daquele, o que quis e sabia, está preenchido o tipo do crime de reprodução ilegítima de programa protegido, ainda que a utilização do programa instalado fosse exclusivamente para uso interno da sociedade".

[59] www.dgsi.pt

Acórdão do Tribunal da Relação de Coimbra de 30-03-2011

Processo nº: 1788/04.5JFLSB.C1

Relator: Jorge Jacob

Sumário: "II – O art. 8º, nº 1, da Lei nº 109/2009, de 15 de Setembro (Lei do Cibercrime), que tipifica o crime de reprodução ilegítima de programa protegido, tutela a propriedade intelectual mediante a criminalização da utilização não autorizada de programa informático protegido por lei. Para a consumação do crime basta a reprodução, divulgação ou comunicação ao público, não se exigindo que a lesão do direito de autor se traduza num prejuízo económico (efectivamente verificado) para este.

III – O crime de usurpação p. p. pelos arts. 195º, 197º e 199º do CDADC, tutela o exclusivo de exploração económica da obra, que a lei reserva ao respectivo autor. Este tipo de crime verifica-se, independentemente de qualquer resultado material, desde que ocorra uma utilização não autorizada, independentemente de o agente se propor obter qualquer vantagem económica.

IV – No âmbito do CDADC, a licitude da utilização ou reprodução sem expressa autorização do autor apenas se afirma com a demonstração de que essa utilização ou reprodução se destinou a fim exclusivamente privado, sem prejuízo para a exploração normal da obra e sem injustificado prejuízo dos interesses legítimos do autor, sendo esta tripla conjugação que evidencia a verificação da regra dos três passos, decorrente da assimilação dos princípios previstos originariamente na Convenção de Berna para a Protecção das Obras Literárias e Artísticas, ratificada por Portugal e transposta para o direito nacional através da legislação que tutela aquela matéria".

3.1.4.7. Disposições processuais

O Capitulo III da LC referente às **disposições processuais**, constantes nos **art. 11º** a 19º, inicia-se com o âmbito de aplicação destas disposições. Assim, "com excepção do disposto nos artigos 18.º e 19.º (intercepções de comunicações e acções encobertas), as disposições processuais previstas no presente capítulo aplicam-se a processos relativos a crimes:

a) Previstos na presente lei;

b) Cometidos por meio de um sistema informático; ou

c) Em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico." Sendo necessário conjugar com o regime da Lei n.º 32/2008, de 17 de Julho.

São disposições processuais:

- **Preservação expedita de dados – art. 12º**
- **A revelação expedita de dados de tráfego – art. 13º**
- **Injunção para apresentação ou concessão de acesso a dados – art. 14º**
- **Pesquisa de dados informáticos – art. 15º**
- **Apreensão dos dados informáticos – art. 16º**
- **Apreensão correio electrónico ou registo de comunicações de natureza semelhante – art. 17º**
- **Intercepção de comunicações – art. 18º**
- **Acções encobertas – art. 19º**

A **preservação expedita de dados**[60], prevista no **art. 12º** da LC, aquando a produção de prova, consiste na preservação de dados com receio de perda atendendo à descoberta da verdade e ao princípio do inquisitório. A autoridade judiciária competente ordena a quem tenha a disponibilidade ou controlo desses dados, nomeadamente ao fornecedor de serviços que preserve os dados em causa (nº1). A preservação é da competência da autoridade judiciária que pode autorizar os órgãos de polícia criminal a ordenar, ou nos casos de "periculum in mora" a iniciativa ser destes, tendo contudo de realizar o relatório previsto no art. 253º do CPP (nº2). A ordem de preservação tem que obedecer a determinadas formalidades sob pena de nulidade processual (nº3) e pode ser renovada (nº5).

[60] Este art. é de conjugação obrigatório com os art. 4º e 5º da Lei 32/2008 de 17 de Julho

A revelação expedita de dados de tráfego – art. 13º - quando uma comunicação englobar mais que um fornecedor de serviços, aquele a quem tiver sido ordenada a preservação deve comunicar à autoridade judiciária os restantes fornecedores de serviços, de que tenha conhecimento, envolvidos na comunicação.

Sempre que no decurso do processo se tornar necessário à produção de prova, tendo em vista a descoberta da verdade [61] obter dados informáticos específicos e determinados [62] armazenados num determinado sistema informático, a autoridade judiciaria ordena a quem tenha disponibilidade ou controlo desses dados que os comunique ou permita o acesso a eles – estamos perante uma **injunção para apresentação ou concessão de acesso a dados[63] – Art. 14º**. São previstas restrições a esta injunção no nº 5 e 6, atendendo à qualidade do sujeito.

Diferentemente da apresentação ou acesso a dados, a LC prevê uma outra disposição processual na investigação dos crimes cibernéticos – **a pesquisa de dados informáticos[64] - art. 15º** - que atendendo aos mesmos princípios que aquela permite que a autoridade judiciaria autorize ou ordene por despacho que se proceda a uma pesquisa num sistema informático de modo a obter dados informáticos, específicos armazenados (nº1). Este despacho tem um prazo de validade de 30 dias, sob pena de nulidade processual (nº2). É admitido que os órgãos de polícia criminal possam proceder à pesquisa, sem prévia autorização, nos casos previstos no nº3, sendo que a alínea b) nos remete para o art. 2º do CPP, contudo tem que respeitar as exigências do nº4, sob pena de nulidade e elaborar o relatório previsto no art. 253º CPP. São aplicáveis com as necessárias adaptações e sempre que se afigure necessário as regras de execução das buscas previstas no CPP e no Estatuto do Jornalista.

Se no decurso da pesquisa informática acima descritas forem encontrados dados ou documentos necessários à produção de prova e essenciais para a descoberta da verdade, a autoridade judiciária autoriza ou ordena por despacho a **apreensão dos dados informáticos - art. 16º**. Os órgãos de polícia criminal podem efectuar as referidas apreensões sem previa autorização nos termos do art. 15º e quando haja "periculum in mora" (nº2), sendo sujeitas a validação pela autoridade judiciária (nº4). Não esquecendo o bem jurídico intimidade e

[61] Ver Acórdão do Tribunal da Relação de Coimbra nº380/08 . 0JAAVR – AC1
[62] Cf. Convenção de Budapeste
[63] Conjugar este artigo com as disposições da Lei nº32/2008 de 17 de Julho e 41/2004 de 18 de Agosto
[64] Conjugar este artigo com as disposições da Lei nº32/2008 de 17 de Julho

privacidade, o nº3 exige que os dados pessoais ou íntimos que possam ser apreendidos são apresentados ao juiz, sob pena de nulidade, que pondera a sua junção aos autos tendo em conta o caso concreto.

As apreensões que digam respeito ao exercício da advocacia e actividades médicas e bancárias estão sujeitas às regras e formalidades do CPP (nº5). Assim como o segredo profissional ou de funcionário sujeito ao art. 182º CPP. A apreensão pode revestir uma das formas previstas no nº7.

Se no decurso de uma pesquisa informática forem encontradas **mensagens de correio electrónico ou registo de comunicações de natureza semelhante - art.17º**, o juiz pode autorizar ou ordenar a apreensão daqueles que sejam relevantes para o interesse da verdade ou para a prova, aplicando-se com as necessárias adaptações o regime de apreensão de correspondência previsto no CPP.

O **art. 18º** prevê a **intercepção de comunicações** em processos relativos a crimes previstos na LC ou cometidos por meio de uma sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte electrónico, quando tais crimes se encontrem previstos no art. 187º do CPP. A intercepção só pode ser realizada durante o inquérito com autorização do JIC e mediante requerimento do MP, atendendo à descoberta da verdade e indispensabilidade da prova. A intercepção pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou visar a recolha e registo de dados de tráfego.

É aplicável com as necessárias adaptações e em tudo o que não contrariar o art. 18º o regime da intercepção e gravação de conversações ou comunicações telefónicas constantes nos arts. 187º, 188º e 189º CPP.[65]

O último art. inserido nas disposições processuais, refere-se às **acções encobertas – art. 19º -** admitindo este regime previsto na Lei nº101/2001 de 25 de Agosto, no decurso do inquérito relativamente a crimes previstos na LC ou "cometidos por meio de sistema informático quando lhes corresponda, em abstracto, pena de prisão máximo superior a 5 anos ou ainda que seja inferior, e sendo dolosos, os 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" (nº1). Sendo necessário o recurso a meios e

[65] Ver Acórdão do Tribunal da Relação de Coimbra de 3 de Outubro de 2012

dispositivos informáticos observam-se as regras previstas para a intercepção de comunicações (nº2)[66].

3.1.4.8. Cooperação internacional

O Capítulo IV da LC dispõe sobre as matérias respeitantes à **cooperação internacional**no âmbito dos crimes cibernéticos. Consiste na cooperação das autoridades nacionais com as estrangeiras "para efeitos de investigação ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos, assim como para a recolha de prova, em suporte electrónico, de um crime, de acordo com as normas sobre transferência de dados pessoais previstas na Lei nº67/98 de 26 de Outubro". [67]

De acordo com o imposto pela Convenção sobre o Cibercrime, a Policia Judiciária assegura a manutenção de uma estrutura que garante um ponto de contacto, sem interrupção, para os casos de assistência entre as autoridades – art. 21º.[68]

Pode ser solicitada a Portugal a **preservação e revelação expedita de dados informáticos – art. 22º -** armazenados em sistema informático aqui localizado relativo a crimes previstos no art. 11º. Tem como objectivo a apresentação de um pedido de apoio judiciário para fins de pesquisa, apreensão e divulgação de dados. O nº2 apresenta um conjunto de exigências a que a solicitação deve responder. É aplicável com as necessárias adaptações o que se disse acerca do art. 12º da LC, nomeadamente quanto à execução da solicitação e competência para ordenar a preservação (nº3 e 4 art. 22). Não esquecendo que a ordem de preservação deve obedecer a determinadas formalidades sob pena de nulidade processual (nº5).

Em qualquer caso, esta solicitação dirigida às autoridades portuguesas pode ser recusada caso os dados respeitem a infracção de natureza política ou conexa, atentar contra a soberania, segurança ou ordem pública, quando não forem oferecidas garantias adequadas à protecção dos dados ou quando se concluir que faltará o requisito de dupla incriminação. Estes são os **motivos de recusa** constantes no **art. 23º** da LC.

É de salientar que a pesquisa, apreensão e divulgação dos dados informáticos armazenados em sistema localizado em Portugal, no âmbito da cooperação internacional, só é

[66] Remete para o art. 18º da LC, art. 187º e 190º do CPP
[67] Cf. Art. 20º da LC
[68] Rede 24/7 – art. 35º da Convenção sobre o cibercrime

admissível nos casos em que também o é para os casos nacionais de natureza semelhante – **Art. 24ºAcesso a dados informáticos em cooperação internacional**.

No **acesso transfronteiriço a dados informáticos armazenados quando publicamente disponíveis ou com consentimento**, as autoridades estrangeiras competentes, sem necessidade de pedido prévio às autoridades portuguesas, de acordo com as normas sobre a transferência de dados pessoais na Lei nº67/98 de 26 de Outubro, podem "aceder a dados informáticos armazenados em sistema informático localizado em Portugal, quando publicamente disponíveis e receber ou aceder, através de sistema informático localizado no seu território, a dados informáticos armazenados em Portugal, mediante consentimento legal e voluntario de pessoa legalmente autorizada a divulgá-los".

As autoridades estrangeiras podem formular pedido às autoridades portuguesas para que seja autorizada pelo juiz a intercepção de transmissões de dados informáticos realizadas por via de um sistema informático localizado em Portugal, desde que esta medida esteja prevista em acordo, tratado ou convenção internacional e que seja admissível ao abrigo do art. 18 da LC. – **Intercepção de comunicações em cooperação internacional** – **art. 26º**

3.1.4.9.Disposições finais

Por último, a LC no seu Capitulo V dispõe sobre as **disposições finais e transitórias**, como a **aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses**[69] – **art. 27º -** sendo que a lei penal portuguesa é aplicável nos casos previstos no CP, tratados ou convenções internacionais e ainda aplicável a factos enumerados no nº1. No caso de existir um conflito positivo de competências (dois tribunais consideram-se competentes para conhecer de um dos crimes previstos na LC), deve recorrer-se aos mecanismos instaurados no seio da União Europeia para dirimir a questão (nº2) e decidir em que tribunal o processo vai ter seguimento, sendo que este toma a sua decisão de aceitação ou transmissão atendendo aos factores elencado no nº3. É, aplicável com as necessárias adaptações as regras gerais de competência previstas no CPP (nº4), sendo que em caso de duvida a competência cabe ao tribunal que primeiro tiver conhecimento dos factos.

[69] Importa referir o art. 4º do CP – "Principio da territorialidade" e o art. 7ºdo CP "Lugar da prática do facto"

Em tudo o que não se encontrar previsto na LC são aplicáveis as disposições do CP, CPP e da Lei nº144/99 de 31 de Agosto[70] - **Art. 28ºRegime geral aplicável**.

A **competência da polícia judiciária em cooperação internacional**, para efeitos da presente lei, é desenvolvida no âmbito da Unidade do Cibercrime – unidade orgânica que investiga os crimes previstos na LC – **art. 29º**

Para **protecção de dados pessoais** é aplicável ao seu tratamento o previsto na Lei nº 67/98 de 26 de Outubro – **art. 30º**.

Com a entrada em vigor da LC foi revogada a Lei nº 109/91 de 17 de Agosto[71].

[70]Lei da cooperação judiciária internacional em matéria penal
[71] LCI

4. Protecção de dados pessoais em Portugal, E.U.A. e Brasil

A protecção de dados pessoais é considerada, actualmente, um tema que merece especial destaque nomeadamente quando interligada com a internet e a questão da privacidade. Importa referir alguns instrumentos legislativos que regulam os regimes de protecção de dados pessoais.

O cibercrime limita-se à criminalidade gerada especificamente através da informática usada como instrumento de trabalho e de comunicação. Por exemplo se é enviada uma mensagem injuriosa, através de correio electrónico, está preenchido o tipo penal de injúrias, não se saindo dos tipos penais comuns apesar de serem utilizados meios informáticos. No caso do cibercrime, o bem ou meio informático deve surgir como elemento típico, como tal para estarmos perante tal crime, torna-se necessário que o meio informático seja penalmente relevante.

A protecção jurídica aos dados pessoais é realizada através de uma protecção generalizada, não dependente do carácter informático. Esta protecção deriva do direito à privacidade, que é facilmente violado através da informática, seja pela facilidade de cruzamento de dados, seja pela rápida propagação de informação na internet.

4.1. Portugal – Lei 67/98 de 26 de Outubro

A protecção aos dados pessoais vem regulada tanto na lei de protecção de dados pessoais – Lei nº 67/98 de 26 de Outubro – na lei de conservação de dados - Lei nº32/74 de 17 de Julho – como na Lei do Cibercrime – lei 109/2009 - através da tipificação de certas condutas que podem atentar contra à privacidade (dados pessoais).

A protecção de dados pessoais encontra-se regulada através de duas vias, uma administrativa e outra normativa.

A primeira encontra-se prevista no **nº 2 do art. 35º da CRP**, onde estabelece que a Comissão Nacional de Protecção de Dados é a entidade que regula aquela protecção. É dotada de poderes de autoridade, e tem como competência controlar e fiscalizar o processamento de dados pessoais, seja com funções de investigação ou de decisão administrativa[72]. As entidades que processam dados pessoais têm o dever de informar a Comissão antes da realização do

[72] Cf. Art. 22º nº2, art. 23º nº1 a) e art. 23º nº1 b) a e), respectivamente, da Lei nº 67/98

mesmo, o que permite o controlo daquele processo e o conhecimento dos titulares de dados que desta forma exercem os seus direitos.

Os titulares de dados pessoais têm o direito de serem informados do tratamento dos seus dados, da possibilidade de dissipação dos mesmos pela internet com consequência de utilização ilícita por parte de outra pessoa, podendo questionar qualquer entidade sobre a existência de dados pessoais relativamente à sua pessoa. Estes dados têm que ser acessíveis ao seu titular, podendo sempre que quiser opor-se ao tratamento dos seus dados ou solicitar a sua remoção.

A protecção aos dados pessoais, realiza-se, igualmente através de normas previstas em diversos diplomas legais, onde podemos mencionar, em primeiro lugar a CRP, mais uma vez no seu art. 35º visa proteger os cidadãos da informática, concedendo os devidos direitos aos titulares dos dados e proibindo o tratamento de dados sensíveis [73].

A protecção criminal à privacidade é desde logo prevista no **CP** no seu **art. 192º** "Devassa da vida privada", seguido desde logo pelo **art. 193º** "Devassa por meio da informática", definindo o tipo objectivo na criação, manutenção ou utilização de ficheiro automatizado de dados individualmente identificáveis referentes a aspectos da vida intima. Partindo da análise a este artigo, é possível verificar que não estamos perante uma total repressão à intromissão na vida privada, mas sim ao facto de se recorrer a um ficheiro com aquelas características e por se reportar a um tipo de dados pessoais mais restritos[74].

A **Lei nº 67/98 de 26 de Outubro**, transpôs para a ordem jurídica interna a **Directiva 95/46/CE** que define no seu art. 2º a) dados pessoais como "qualquer informação relativa a uma pessoa singular identificada ou identificável (…)", assim o faz, também, a lei nº67/98 no art.3º a). O **art. 43º** da mesma lei contém uma espécie de crime universal, relativo a infracções de obrigações para protecção de dados pessoais. Quando se trate de dados sensíveis, as penas são elevadas para o dobro, isto porque, a questão da proibição do tratamento de dados sensíveis vem prevista em ambos os diplomas, nos **art. 8º** nº1 (Directiva) e **art. 7º** nº1 (Lei 67/98), permitindo apenas à Comissão referida anteriormente autorizar tal tratamento, desde que o seu titular também o consinta, pois se assim não o for estaremos perante uma ofensa aos direitos de personalidade, nomeadamente o de privacidade. Este consentimento só pode ser afastado nos casos de interesse público superior e quando não for

[73] Dados relativos a convicções filosóficas ou políticas, filiação partidária, fé religiosa, origem étnica e vida privada (saúde e vida sexual por exemplo)

[74] Dados sensíveis

possível por qualquer outra via. A doutrina portuguesa defende que os titulares dos dados pessoais, não são apenas as pessoas singulares, mas também as pessoas colectivas. O tratamento destes dados vem previsto no **art.3º b) e 4º nº1** da Lei nº67/98 que define o que se entende por tratamento de dados e a que dados se aplica.

É ainda de referir que o **art. 44º nº1** tipifica o acesso indevido a dados pessoais, o **art. 45º** a viciação ou destruição de dados pessoais e o **art. 46º nº1** a desobediência qualificada quando depois de notificado não praticar os actos a que está obrigado referente aos dados pessoais.

Podemos constatar que existe uma diferença entre o art. 193º do CP e a Lei 67/98, pois aquele trata apenas dos ficheiros automatizados, enquanto esta abrange todas as formas de tratamento de dados pessoais.

O tratamento dos dados pessoais, atendendo à sua ligação com a vida privada, está sujeito a diversos princípios fundamentais, entre eles o da transparência que impõe à pessoa responsável pelo tratamento o dever de o informar, detalhadamente, ao titular dos dados, assim como actuar sobre eles, de forma legítima e legal, utilizando-os para fins determinados – princípio da finalidade e qualidade dos dados.

Apesar das exigências legais sobre o tratamento de dados pessoais, constatasse que muitas empresas não cumprem as normas previstas e não são punidas por violarem o direito à privacidade do titular dos dados.

4.2. E.U.A

Os E.U.A. adoptaram um sistema de "auto-regulação" onde os sites e usuários relacionam-se directamente, existindo poucas disposições legais sobre esta matéria. O direito à privacidade, é garantido pelas políticas de privacidade das empresas privadas e que geram certificados de segurança. Lembre-se que é um país extremamente ligado ao direito de privacidade que ficou espelhado no "Right to Privacy", contudo existe uma maior liberdade no que diz respeito ao tratamento de dados pessoais, pois são quase inexistentes as normas a regularem esta matéria e as soluções passarem pelo analise do caso concreto. Diferentemente do que acontece na Europa, nomeadamente, em Portugal, onde a preocupação legal com este tema é visível nos vários diplomas que a regulam com um controlo sob a utilização da internet.

No que concerne, por exemplo aos "spams", apenas alguns estados regulam a matéria, pois a nível nacional não existe qualquer diploma. A luta contra o correio electrónico não solicitado, é efectuada através de exigências mínimas sobre este meio de comunicação, tendo como exemplo a impossibilidade de utilização de um nome de domínio de um terceiro para o envio de mensagens, a obrigação de existir instruções nas mensagens que permitam o sistema de eliminação de forma simples e a identificação de um endereço válido para o envio de mensagens, sendo estas ultimas características as que mais importam às empresas.

4.3. Brasil

A protecção aos dados pessoais encontra-se dispersa por vários diplomas. A nível constitucional o direito à privacidade vem também conceder uma protecção aos dados pessoais, assim como o "habeas data"[75] que consagra um direito de acesso a todos os dados que lhes digam respeito e que estejam na posse de entidades públicas. O caso torna-se de difícil resolução quando se trate de bancos de dados privados, como por exemplo os dados inseridos em arquivos informatizados comerciais ou médicos.

Outra protecção é a concedida pelo art. 43º do Código de Defesa do Consumidor, atribuindo direitos e garantias ao consumidor, entre os quais o direito de acesso e rectificação, que veja os seus dados registados e/ou armazenados em bancos de dados, tipificando como crime a negação do acesso ou rectificação de tais dados – art. 72º e 73º. Em certos casos, impõe-se o dever de comunicação ao consumidor de que as suas informações estão ser tratadas para certos efeitos.

Pretende-se que exista um equilíbrio entre as relações, através da imposição de limites ao responsável pelo tratamento dos dados.

O Código de Defesa do Consumidor, estabelece princípios que se aplicam à protecção de dados pessoais, contudo ao faze-lo no âmbito do consumidor impossibilita a aplicação daqueles como um sistema geral de protecção de dados pessoais.

Assim, as questões relacionadas com a protecção de dados pessoais com tratamento informatizado, apenas encontram previsão em diplomas específicos, como o caso da defesa do consumidor, do sigilo bancário ou fiscal ou do "habeas data".

[75] Possibilidade do cidadão aceder às informações sobre os seus dados armazenados por meio de registos ou banco de dados de entidades governamentais e de carácter publico, de forma a puder examina-los e corrigir ou solicitar a remoção de informações erradas ou inexactas. Art. 5º inciso LXXII da Constituição da República Brasileira

Com as batalhas que se travam no âmbito da protecção dos dados pessoais, mormente, o seu tratamento a nível informático, o Brasil tem vindo a criar vários projectos de lei com o intuito de legislar de forma exaustiva aquela protecção, o seu uso e tratamento, pretendendo inclusive adoptar disposições da Directiva nº95/46/CE.

4.4. A protecção do cibercrime VS violação da privacidade - Problema a ser resolvido pela UE

Com o estudo realizado neste trabalho, sobre os aspectos cruciais da LC e suas problemáticas relacionadas com os restantes instrumentos legislativos, não poderia deixar de referir um projecto que tem sido desenvolvido desde 2009 pela União Europeia denominado "INDECT" com um investimento de milhões de euros. Muitas são as críticas em volta deste projecto, contudo apenas me limitarei a referir que se a UE pretende dar continuidade a este projecto terá que pensar em conjuga-lo com as disposições europeias e nacionais sobre a protecção de dados pessoais, pois pelo que foi tornado público, este projecto pode atentar contra direitos básicos, tais como a privacidade. Se analisarmos superficialmente tal situação, podemos concluir que se os cidadãos querem estar protegidos de condutas ilícitas de outros cidadãos e não serem vitimas de crimes, nomeadamente, cibercrimes, terão que abdicar da sua vida privada em prol de um bem maior. É o que acontece quando permitimos a "divulgação" dos nossos dados pessoais com o intuito de evitar ataques terroristas.

O projecto "INDECT" tem sido alvo de muitas críticas, estando longe de se chegar a um consenso. Trata-se de uma tecnologia de vigilância capaz de analisar comportamentos com o objectivo de evitar a consumação de um crime, na vida real ou virtual. Como referido esta tecnologia viola direitos básicos dos cidadãos, como seja o caso da privacidade, pois as câmaras de vigilância utilizadas têm a capacidade de cruzar imagens de reconhecimento biométrico com dados virtuais das pessoas em bases de dados como redes sociais. Desta forma, qualquer pessoa pode estar a ser vigiada quando tome alguma atitude fora do considerado normal ou mesmo quando diga algo considerado pelo sistema como ameaçador, tornando-se assim um potencial suspeito.

5. Desenvolvimentos recentes no âmbito do cibercrime - a responsabilidade penal das pessoas colectivas

5.1. Na Convenção sobre o Cibercrime

- **Art. 12º da CCib – Responsabilidade das pessoas colectivas**

1 – "Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para garantir que as pessoas colectivas possam ser consideradas responsáveis pelas infracções penais previstas na presente Convenção, cometidas em seu benefício por qualquer pessoa singular, agindo individualmente ou enquanto membro de um órgão da pessoa colectiva, que nelas ocupem uma posição de liderança, com base:

a)Nos poderes de representação conferidos pela pessoa colectiva;
b)Na autoridade para tomar decisões em nome da pessoa colectiva;
c)Na autoridade para exercer o controlo no seio da pessoa colectiva.

2 – Para além dos casos já previstos no n.º 1 do presente artigo, cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para garantir que uma pessoa colectiva possa ser considerada responsável sempre que a falta de vigilância ou controlo por parte de uma pessoa singular referida no n.º 1 possibilite a prática de uma das infracções previstas na presente Convenção em benefício da referida pessoa colectiva por uma pessoa singular que aja sob a sua autoridade.

3 – De acordo com os princípios jurídicos da Parte, a responsabilidade de uma pessoa colectiva pode ser penal, civil ou administrativa.

4 – Essa responsabilidade não exclui a responsabilidade criminal das pessoas singulares que tenham cometido a infracção"

Este artigo dedica-se à responsabilidade das pessoas colectivas estando em consonância com as legislações nacionais que reconhecem a nível jurídico a responsabilidade destas entidades.

Desdobra-se em duas vertentes e tem como objectivo responsabilizar as pessoas colectivas (empresas, associações etc..) por actos previstos e puníveis na presente Convenção quando cometidos por uma pessoa que ocupe uma cargo de liderança e em nome da empresa. Mas também quando esta pessoa não exerça o controlo e fiscalização exigida sobre um

funcionário ou representante da pessoa colectiva, nos casos em que tal omissão possibilite a pratica dos crimes previsto na Convenção por parte daqueles.

- O 1º parágrafo exige que se preencham cumulativamente quatro requisitos:

1 – Crime previsto na Convenção

2 – Crime cometido em nome da pessoa colectiva

3 – Crime deverá ter sido cometido por uma pessoa que ocupe um cargo de liderança (inclui-se aqui o auxilio e cumplicidade)

4 – Pessoa deverá ter agido com base nas suas competências – poder de representação ou autoridade para tomar decisões e exercer controlo

Assim, o artigo obriga as partes a disporem dos meios necessários para imputar a responsabilidade a pessoa colectiva, quando as pessoas que ocupam uma posição de liderança cometam um dos crimes previstos na Convenção.

- O 2º parágrafo impõe que se reúnam cumulativamente os seguintes requisitos:

1 – Crime cometido por um funcionário ou representante da pessoa colectiva

2 – Crime cometido por conta e para beneficio da pessoa colectiva

3 – Crime foi proporcionado pela ausência de supervisão ou controlo da pessoa que exerce um cargo de liderança

Pretende-se imputar a responsabilidade a uma pessoa colectiva, não já por acto cometido por uma pessoa que exerça cargo de liderança, mas sim por um funcionário ou representante que agindo no âmbito das suas competências e por falta de controlo daquele cometeu um dos crimes previsto em beneficio da pessoa colectiva.

Entende-se que a falta de controlo deve ser entendida como uma omissão de medidas adequadas no sentido de impedir que o funcionário ou representante se envolva em actividades ilegais, em nome da pessoa colectiva. Estas medidas deverão ter em conta o tipo de empresa, a sua dimensão e normas aplicáveis.

Não é possível considerar este controlo, como um meio exaustivo de verificar passo a passo de cada funcionário ou representante, nem tão pouco vigiar as comunicações feitas por estes.

Em qualquer um dos casos, a responsabilidade da pessoa colectiva não exclui a responsabilidade individual da pessoa que ocupe um cargo de liderança, do funcionário ou do representante.

É referido ainda no presente art. que a responsabilidade da pessoa colectiva poderá ser criminal, civil ou administrativa, dispondo cada parte de liberdade para aplicar cada uma consoante o seu direito interno e princípios jurídicos, conquanto respeitem os requisitos constantes no art. 12º e 13º da Convenção. Este último artigo prevê as sanções e medidas aplicáveis aos crimes previstos no art. 2º ao 10º. As partes estipulam as consequências que resultem das infracções cometidas, ao aplicar sanções que deverão ser " eficazes, proporcionais e dissuasivas". Estas sanções, como referido, poderão ter carácter penal, civil ou administrativo e serem pecuniárias. Será da responsabilidade de cada parte, actuando ao abrigo do seu poder discricionário, a criação das respectivas sanções que seja compatível com o seu sistema jurídico.

- **Art. 13º da CCib - Sanções e medidas**

Nº2 – "Cada Parte deverá assegurar que as pessoas colectivas consideradas responsáveis nos termos do artigo 12.º sejam objecto de sanções ou medidas, de natureza penal e não penal, eficazes, proporcionais e dissuasivas, incluindo sanções pecuniárias"

5.2. Na Decisão Quadro

- **Art.1º - Definições**

c) "Pessoa colectiva", qualquer entidade que beneficie desse estatuto por força do direito aplicável, com excepção do Estado ou de outras entidades de direito público no exercício das suas prerrogativas de autoridade pública e das organizações internacionais de direito público

- **Art. 8 – Responsabilidade das pessoas colectivas**

"1. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que as pessoas colectivas possam ser consideradas responsáveis pelas infracções referidas nos artigos 2.o, 3.o, 4.o e 5.o, praticadas em seu benefício por qualquer pessoa, agindo individualmente ou enquanto integrando um órgão da pessoa colectiva, que nela ocupe uma posição dominante baseada:

a) Nos seus poderes de representação da pessoa colectiva; ou

b) No seu poder para tomar decisões em nome da pessoa colectiva; ou

c) Na sua autoridade para exercer controlo dentro da pessoa colectiva.

2. Para além dos casos previstos no n.o 1, os Estados-Membros devem assegurar que uma pessoa colectiva possa ser considerada responsável sempre que a falta de vigilância ou de controlo por parte de uma pessoa referida no n.o 1 tenha tornado possível a prática, por uma pessoa que lhe esteja subordinada, das infracções referidas nos artigos 2.o, 3.o, 4.o e 5.o, em benefício dessa pessoa colectiva.

3. A responsabilidade de uma pessoa colectiva nos termos dos nºs 1 e 2 não exclui a instauração de procedimento penal contra as pessoas singulares envolvidas na qualidade de autoras, instigadoras ou cúmplices nas infracções referidas nos artigos 2º, 3º, 4º e 5º".

As pessoas colectivas devem ser responsáveis pelas infracções constantes nos arts. 2º, 3º, 4º e 5º da Decisão-Quadro, quando praticadas por qualquer pessoa, em benefício daquela, agindo de forma individual ou enquanto parte de um órgão, com uma posição dominante, baseada:

"a) Nos seus poderes de representação da pessoa colectiva; ou

b) No seu poder para tomar decisões em nome da pessoa colectiva; ou

c) Na sua autoridade para exercer controlo dentro da pessoa colectiva."

Deve ser, igualmente, responsável se existir falta de vigilância ou controlo por parte da pessoa referida anteriormente que desta forma tenha tornado possível a prática, por uma pessoa subordinada, das infracções previstas nos arts. 2º a 5º, em beneficio da pessoa colectiva.

A responsabilidade da pessoa colectiva, não exclui a responsabilidade de pessoas singulares pela prática das infracções, seja na qualidade de autor, instigador ou cúmplice.

- **Art. 9 – Sanções aplicáveis às pessoas colectivas**

Sanções aplicáveis às pessoas colectivas

1 – "Cada Estado-Membro deve tomar as medidas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos do n.o 1 do artigo 8.o seja passível de sanções efectivas, proporcionadas e dissuasivas, incluindo multas ou coimas e eventualmente outras sanções, designadamente:

a) Exclusão do benefício de vantagens ou auxílios públicos;

b) Interdição temporária ou permanente de exercer actividade comercial;

c) Colocação sob vigilância judicial;

d) Dissolução por via judicial.

2. Cada Estado-Membro deve tomar as medidas necessárias para assegurar que uma pessoa colectiva considerada responsável nos termos do nº 2 do artigo 8º seja passível de sanções ou medidas efectivas, proporcionadas e dissuasivas".

As sanções aplicadas às pessoas colectivas devem ter a mesma eficácia que as aplicadas às pessoas singulares, podendo incluir multas e coimas ou aquando a infracção prevista no nº1 do art. 8 a "exclusão do benefício de vantagens ou auxílios públicos; Interdição temporária ou permanente de exercer actividade comercial; Colocação sob vigilância judicial; Dissolução por via judicial".

5.3. No Código Penal

- **Art.11º - Responsabilidade das pessoas singulares e colectivas**

"1 - Salvo o disposto no número seguinte e nos casos especialmente previstos na lei, só as pessoas singulares são susceptíveis de responsabilidade criminal.
2 – As pessoas colectivas e entidades equiparadas, com excepção do Estado, de outras pessoas colectivas públicas e de organizações internacionais de direito público, são responsáveis pelos crimes previstos nos artigos 152.º-A e 152.º-B, nos artigos 159.º e 160.º, nos artigos 163.º a 166.º, sendo a vítima menor, e nos artigos 168.º, 169.º, 171.º a 176.º, 217.º a 222.º, 240.º, 256.º, 258.º, 262.º a 283.º, 285.º, 299.º, 335.º, 348.º, 353.º, 363.º, 367.º, 368.º-A e 372.º a 374.º, quando cometidos:

a) Em seu nome e no interesse colectivo por pessoas que nelas ocupem uma posição de liderança; ou

b) Por quem aja sob a autoridade das pessoas referidas na alínea anterior em virtude de uma violação dos deveres de vigilância ou controlo que lhes incumbem.
3 - Para efeitos da lei penal a expressão pessoas colectivas públicas abrange:

a) Pessoas colectivas de direito público, nas quais se incluem as entidades públicas empresariais;

b) Entidades concessionárias de serviços públicos, independentemente da sua titularidade;

c) Demais pessoas colectivas que exerçam prerrogativas de poder público.

4 - Entende-se que ocupam uma posição de liderança os órgãos e representantes da pessoa colectiva e quem nela tiver autoridade para exercer o controlo da sua actividade.
5 - Para efeitos de responsabilidade criminal consideram-se entidades equiparadas a pessoas colectivas as sociedades civis e as associações de facto.
6 - A responsabilidade das pessoas colectivas e entidades equiparadas é excluída quando o agente tiver actuado contra ordens ou instruções expressas de quem de direito.
7 - A responsabilidade das pessoas colectivas e entidades equiparadas não exclui a responsabilidade individual dos respectivos agentes nem depende da responsabilização destes.
8 - A cisão e a fusão não determinam a extinção da responsabilidade criminal da pessoa colectiva ou entidade equiparada, respondendo pela prática do crime:
a) A pessoa colectiva ou entidade equiparada em que a fusão se tiver efectivado; e
b) As pessoas colectivas ou entidades equiparadas que resultaram da cisão.
9 - Sem prejuízo do direito de regresso, as pessoas que ocupem uma posição de liderança são

subsidiariamente responsáveis pelo pagamento das multas e indemnizações em que a pessoa colectiva ou entidade equiparada for condenada, relativamente aos crimes:

a) Praticados no período de exercício do seu cargo, sem a sua oposição expressa;

b) Praticados anteriormente, quando tiver sido por culpa sua que o património da pessoa colectiva ou entidade equiparada se tornou insuficiente para o respectivo pagamento; ou

c) Praticados anteriormente, quando a decisão definitiva de as aplicar tiver sido notificada durante o período de exercício do seu cargo e lhes seja imputável a falta de pagamento.

10 - Sendo várias as pessoas responsáveis nos termos do número anterior, é solidária a sua responsabilidade.

11 - Se as multas ou indemnizações forem aplicadas a uma entidade sem personalidade jurídica, responde por elas o património comum e, na sua falta ou insuficiência, solidariamente, o património de cada um dos associados"

Este artigo foi introduzido através da reforma operada pela Lei nº59/2007 ao CP, onde passa a ser possível responsabilizar criminalmente as pessoas colectivas, atendendo a um determinado catálogo de crimes previstos no CP, sendo que fora do disposto nos nºs do art.11º e em leis especiais, apenas as pessoas singulares são susceptíveis de responsabilidade criminal. Podemos dizer que o regime previsto nos nºs 2 a 11 do art. 11º do CP é aplicável salvo disposição especial em contrário.

Estamos perante uma norma jurídica que é violada por parte de um sujeito singular (órgão ou representante), sendo que através deste comportamento e verificados certos requisitos, a pessoa colectiva torna-se, igualmente, responsável.

Trata-se de uma responsabilidade derivada e cumulativa, afastando-se a possibilidade de uma responsabilidade da pessoa colectiva autónoma da pessoa singular. É uma responsabilidade derivada, pois depende sempre do facto ilícito praticado por um órgão ou representante da pessoa colectiva, em nome desta e no seu interesse ou por um facto ilícito praticado por subordinado, sob a autoridade de pessoa com posição de liderança, em virtude de violação de dever de vigilância ou de controlo[76]. É também cumulativa pois não exclui a punibilidade dos factos ilícitos que tenham sido praticados pelos agentes singulares.

[76] Cf. Art. 11º nº2 a) e b) CP

O nº2 do art. 11º refere que são abrangidas por esta responsabilidade as pessoas colectivas e equiparadas[77], à excepção do Estado (compreende-se também aqui as Regiões Autónomas, Institutos públicos e Municípios), de outras pessoas colectivas públicas[78] e de organizações internacionais de direito público. Consideram-se equiparadas às pessoas colectivas as sociedades civis e as associações de facto. Exclui-se deste âmbito as pessoas colectivas que sejam responsáveis pelo direito penal tributário ou direito penal fiscal.

A responsabilidade penal das pessoas colectivas mantém-se mesmo que ocorra a sua modificação formal [79] e apenas se extingue com o encerramento da sua liquidação, pois só se considera extinta, a pessoa colectiva, neste momento.

A lei penal Portuguesa aplica-se ainda a factos praticados fora do território nacional, quando praticados por pessoa colectiva ou contra pessoa colectiva que tenha sede em território nacional[80].

Para que seja admissível a responsabilidade penal das pessoas colectivas temos que estar perante um dos crimes elencados pelo nº2 do art. 11º - catálogo de crimes – sendo eles: Art. 152º-A, 152º-B, 159º, 160º, 163º a 166º, 168º, 169º, 171º a 176º, 217º a 222º, 240º, 256º, 258º, 262º a 283º, 285º, 299º, 335º, 348º, 353º, 363º, 367º, 368º-A, 372º a 374º, todos do CP.

A maioria destes crimes é punível a título doloso, à excepção dos de perigo comum, que podem ser punidos a título negligente, sendo que nestes casos a imputação de um crime negligente à pessoa colectiva só será possível mediante a mesma aplicação à co-autoria negligente.

O nexo de imputação à pessoa colectiva do facto típico praticado pela pessoa física implica uma dimensão subjectiva que diz respeito aos sujeitos qualificados que praticam os actos ilícitos – pessoa que exerce um poder de liderança - que podem vir a responsabilizar as pessoas colectivas, e uma dimensão objectiva que recaí sobre os requisitos da conduta típica – em nome e no interesse da pessoa colectiva ou por violação de deveres de vigilância e controlo.

Assim da conjugação das duas alíneas do nº2 do art. 11º do CP podemos considerar que as pessoas colectivas e equiparadas, excluindo as entidades já referidas, são criminalmente responsáveis pelos crimes previstos nos artigos mencionados quando estes sejam praticados, por acção ou omissão:

[77] Entidades equiparadas são as sociedades civis e as associações de facto – nº5 do art. 11º CP
[78] Entidades públicas empresariais, entidades concessionárias de serviços públicos, demais pessoas colectivas que exerçam poder público – nº3 do art.11 CP
[79] Cf. Art. 11º nº8 CP
[80] Cf. Art. 5º nº1 g) CP

- Em seu nome e no interesse colectivo por pessoas que nelas ocupem uma posição de liderança; ou
- Por quem aja sob a autoridade das pessoas mencionadas na alínea anterior em virtude de violação de deveres de vigilância ou controlo a que estão vinculadas e que proporcionou a prática do facto ilícito

Ao contrário de Portugal, que apenas admite a responsabilidade das pessoas colectivas e equiparadas perante um catálogo de crimes, países como a Holanda e Bélgica esta responsabilidade existe para qualquer crime.

Dimensão subjectiva

O art. 11º nº2 a) e b) e nº4 faz referência aos sujeitos qualificados dos quais podem advir actuações ilícitas que possam responsabilizar criminalmente a pessoa colectiva. São estes os que ocupam um cargo de liderança – órgãos e representantes da pessoa colectiva - e quem nela tiver autoridade para exercer o controlo da sua actividade (pessoa a quem a administração delega funções de autoridade, conferindo poderes de domínio sobre a actividade ou sector de actividade). Ainda se inclui neste âmbito as actuações de sujeitos que se encontrem sob a autoridade das pessoas com posição de liderança que por sua vez violaram deveres de vigilância e controlo proporcionando a actuação daqueles.

Exclui-se, assim, os actos cometidos por pessoas singulares que não tenham aquelas qualidades ou autoridade, mesmo quando seja cometido no interesse da pessoa colectiva.

É excluída, pelo nº6 do mesmo artigo, a responsabilidade da pessoa colectiva quando o agente tiver actuado contra ordens ou instruções expressas de quem de direito ou fora das suas funções ou competências, pois embora a pessoa actue na qualidade de órgão ou representante e ainda que no interesse da pessoa colectiva não age em conformidade com a vontade da pessoa colectiva expressa por quem de direito.

Dimensão objectiva

Quando o art.11º faz menção à prática de actos ilícitos em "nome colectivo" não é exigível que o sujeito esteja munido de poderes jurídicos de representação, bastando que actue no âmbito das funções de liderança que lhe foram cometidas – art. 11º nº4.

A actuação com base no interesse colectivo pressupõe que o facto ilícito praticado por pessoa com cargo de liderança, ou por um subalterno nas condições já mencionadas, seja

praticado por ocasião da actividade colectiva e no exercício das suas funções (e não por interesse pessoal, a não ser que da actuação possa tirar proveito pessoal, mas também para a pessoa colectiva) de forma a assegurar o normal funcionamento da pessoa colectiva, mesmo sem obter qualquer proveito económico.

Por outro lado, sempre que seja possível estabelecer uma conexão entre o facto praticado pelo subordinado à violação de deveres de vigilância ou controlo pela pessoa que exerce liderança, a pessoa colectiva é da mesma forma responsável pela conduta ilícita praticada pelo subordinado.

Para a pessoa colectiva ser responsabilizada criminalmente, o facto tem que ser cometido por uma das pessoas acima mencionadas, quando actuem dentro dos seus poderes de autoridade, ou funções atribuídas pela pessoa colectiva, dentro dos fins por esta propostos e ainda nos casos em que exerçam um controlo da sua actividade e quando não actuem com o dever de vigilância e controlo a que são obrigadas e seja praticado, por um subalterno, um acto ilícito no interesse da pessoa colectiva.

A lei acrescenta que para a pessoa colectiva ser responsável o facto tem que ser praticado em nome desta e no seu interesse. Pois se uma das pessoas com aquelas qualidades praticarem um facto ilícito, compreende-se que se ocupam uma posição de liderança, agem em nome da pessoa colectiva e como tal no seu interesse, parecendo ser a própria pessoa colectiva a actuar. Este interesse da pessoa colectiva é a razão de imputação da sua responsabilidade, sendo que teremos sempre que nos socorrer da vontade da pessoa colectiva através da lei e dos Estatutos que definem as condições de formação dessa vontade juridicamente relevante[81].

Refira-se que não se impõe que as pessoas físicas sejam condenadas, apenas que seja apurada a sua culpa para que exista responsabilidade da pessoa colectiva, assim como a actuação seja no interesse desta, sendo condição *sine qua non* para que a vontade das pessoas físicas seja legalmente atribuída à pessoa colectiva e que a vontade desta seja formada nos termos legalmente prescritos.

A imputação dos crimes aos titulares dos órgãos ou representantes, pode ser feita a título de acção ou omissão própria ou imprópria, neste caso quando sobre eles recaia o dever de garante da não produção do resultado. Será com base na actuação da pessoa – dolo ou negligência - que se constituirá a imputação subjectiva à pessoa colectiva, será, em princípio, responsável pelo mesmo titulo que for a pessoa singular.

[81] Ascensão, José deOliveira, Direito Civil/Teoria Geral I, 2ª ed. Coimbra, 2000, p.272

A lei não estabelece nenhuma limitação quanto à forma dos crimes imputáveis à pessoa colectiva, podendo então ser por crimes consumados ou tentados e a título de autor, instigador ou cúmplice, consoante o titulo a que for a pessoa física imputável.

O nº7 do art. 11º prevê a responsabilidade cumulativa ou concorrente dos agentes do crime e da pessoa colectiva. A responsabilidade desta última torna-se essencial na medida em que muitas vezes o tribunal consegue comprovar que o acto foi praticado por um órgão, representante ou pessoa com autoridade para exercer o controlo da actividade, mas torna-se difícil individualizar de entre aqueles qual foi o agente do crime, sendo que esta dificuldade não impede a responsabilização da pessoa colectiva desde que seja possível concluir que o acto só poderia ter sido praticado em razão da sua actuação, mediata ou imediata.

O nº8 prevê que a responsabilidade criminal das pessoas colectivas não se extingue por cisão ou fusão, sendo que no primeiro caso todas as entidades que resultem da cisão são penalmente responsáveis pela prática do crime, apesar da pena poder ser graduada em função das características concretas de cada uma, no caso de fusão será a entidade em que se tiver efectivado a fusão.

As pessoas que ocupem uma posição de liderança são subsidiariamente responsáveis pelo pagamento de multas ou indemnizações, pelo que nas hipóteses da b) e c) é necessário que a insuficiência do património ou a falta de pagamento lhes seja imputável a cada um, no caso da a) impõe-se que a pessoa, em razão da posição que ocupava, pudesse legalmente opor-se à prática do crime, como dispõe o nº9 do art. 11º. Nos casos em que forem responsáveis várias pessoas, a sua responsabilidade é solidária – nº10.

Como decorre do art. 8º do CP, o regime previsto por este diploma para a responsabilidade das pessoas colectivas e equiparadas é de aplicação suplectiva relativamente aos regimes previstos em leis especiais, sendo de aplicação subsidiária as regras gerais, salvo disposição em contrário da lei especial.

Podemos fazer referência a leis penais extravagantes que contemplam a responsabilidade de pessoas colectivas:

- Art. 9º Lei 109/2009 de 15 de Setembro – Lei do Cibercrime
- Art. 6º Lei 52/2003 de 22 de Agosto – Lei de Combate ao Terrorismo
- Art. 7º Lei 15/2001 de 5 de Junho – Regime Geral das Infracções Tributárias

- Art. 3º DL 28/84 de 20 de Janeiro – Regime jurídico das Infracções Antieconómicas e contra a Saúde Pública
- Art. 43º-A Lei 32/2006 de 26 de Julho – Regime Jurídico da Procriação Medicamente assistida
- Art. 96º Lei 5/2006 de 23 de Fevereiro – Regime Jurídico das Armas e Munições
- Art. 3 Lei 50/2007 de 31 de Agosto – Regime de Responsabilidade Penal por comportamentos Antidesportivos

Art. 182º Lei 23/2007 de 4 de Julho – Regime Jurídico de Entrada, Permanência, Saída e Afastamento de Estrangeiros

- **Despacho do PGR – Constituição das pessoas colectivas como arguidas**

O Procurador-Geral da República, em 2011, entendeu que deveria elaborar despacho sobre a constituição das pessoas colectivas como arguidas, face ao desentendimento verificado entre as autoridades na conjugação das disposições penais.

O art. 58º nº1 do CPP prevê as situações de constituição de arguido, contudo nos casos em que a responsabilidade pode ser imputada a pessoas colectivas e respectivos administradores ou gerentes, não o está a ser, sendo apenas estes últimos constituídos arguidos. Atente-se que a responsabilidade das pessoas colectivas encontra previsão legal, tendo consequências no exercício de direitos processuais.

É da competência do MP a apreciação da possibilidade de pessoas colectivas serem penalmente responsáveis, bem como a decisão ou validação da sua constituição como arguida – art. 53º nº2 b) e 58º nº2 e 3 CPP.

Outra questão prende-se com a divergência verificada sobre quem deverá representar a pessoa colectiva, constituída arguida, em juízo, seja no momento da sua constituição ou nos actos processuais posteriores, principalmente quando seja declarada insolvente.

Atendendo ao mencionado anteriormente e ao abrigo do disposto no artigo 12° nº2 b), do Estatuto doMinistério Público, entende o PGR que os Magistrados e Agentes do Ministério Público, considerem:

"1 - Nos casos em que existam fundadas suspeitas da prática de factosilícitos penalmente imputáveis a uma pessoa colectiva, os Magistrados eAgentes do Ministério

Público deverão instruir o órgão de polícia criminal, noqual deleguem competência para a investigação ou a realização de diligências,no sentido de procederem à sua constituição como arguida, através dos seusactuais representantes legais;

2 - O disposto no número anterior aplica-se ainda no caso de ter sidodeclarada a insolvência da pessoa colectiva, mantendo-se, até aoencerramento da liquidação, a representação legal nos termos estatutários.

3 - A constituição da pessoa colectiva como arguida não prejudica aeventual constituição e interrogatório como arguidos dos representantes legaisda pessoa colectiva que possam ser pessoal e individualmenteresponsabilizados pelos factos que constituem objecto do inquérito."

5.4. Na Lei da Criminalidade Informática

A lei da criminalidade informática vivia e total desarmonia com outras leis nomeadamente as relativas à protecção de dados pessoais e às telecomunicações, tornando-se desactualizada face aos novos acontecimentos operados na tecnologia. Daí que depois da Convenção Sobre o Cibercrime se tenha tornado indiscutível a necessidade de Portugal adoptar uma lei adequada à realidade informática e que respeitasse os princípios impostos pela Convenção, nasceu assim a Lei 109/2009. Para o que aqui importa, será feita apenas uma breve referência ao art. 3º da LCI sobre a responsabilidade das pessoas colectivas, uma vez que esta lei encontra-se já revogada.

- **Art. 3º - Responsabilidade das pessoas colectivas**

1- "As pessoas colectivas, sociedades e meras associações de facto são penalmente responsáveis pelos crimes previstos na lei, quando cometidos em seu nome e no interesse colectivo pelos seus órgãos ou representantes.

2- A responsabilidade é excluída quando o agente tiver actuado contra ordens ou instruções expressas de quem de direito.

3- A responsabilidade das entidades referidas no nº1 não exclui a responsabilidade individual dos respectivos agentes.

4- As entidades referidas no nº1 respondem solidariamente, nos termos da lei civil, pelo pagamento de multas, indemnizações e outras prestações em que forem condenados os agentes das infracções previstas na presente lei".

Ao contrário do art. 11º do CP, que prevê a responsabilidade das pessoas colectivas e equiparadas como mera eventualidade, o art. 3º da LCI, responsabiliza expressamente aquelas entidades pelos crimes "cometidos em seu nome e no interesse colectivo pelos seus órgãos ou representantes".

Com a LCI, que operou uma reviravolta na responsabilidade das pessoas colectivas, o legislador não remeteu para outras fontes onde a matéria estava já contemplada, nomeadamente para o DL 28/84 de 20 de Janeiro sobre infracções antieconómicas, pois pretendeu regular tudo na lei da criminalidade informática.

Este art. 3º da LCI prevê o regime para a responsabilidade penal das pessoas colectivas e equiparadas, especificando no seu nº1 que se aplica a pessoas colectivas, sociedade e meras associações de facto.

5.5. Na Lei do Cibercrime

- **Art. 9 – Responsabilidade das pessoas colectivas**

"As pessoas colectivas e entidades equiparadas são penalmente responsáveis pelos crimes previstos na presente lei nos termos e limites do regime da responsabilização previsto no Código Penal"

A responsabilidade penal das pessoas colectivas e equiparadas, prevista no art. 9º da LC, remete-nos para o regime de responsabilização do CP. Como podemos verificar anteriormente, este tipo de responsabilidade está, igualmente, previsto no art. 12º da CCib, assim como no art. 8º da DQ/2005/222/JAI.

- **Diferença entre o art. 3º da LCI e art. 9º da LC**

O art.3º da LCI, agora revogada, regulava de uma forma mais completa o regime da responsabilidade penal das pessoas colectivas e equiparadas. Existia responsabilidade nos casos em que os ilícitos penais fossem "cometidos em seu nome e no interesse colectivo pelos seus órgãos ou representantes", e não quando o agente "tiver actuado contra ordens ou instruções expressas de quem de direito".

- **O art. 9º da LC não prevê o nº2 do art. 12º da CCib**

Hoje, o art. 9º da LC, limita-se a remeter tal responsabilidade para o regime previsto no CP. Esta diferença pode ser explicada se considerarmos que a versão do antigo art. 11º do CP remetia aquela responsabilidade para as leis especiais que a regulassem. Com a alteração feita a este artigo, o art.11º do CP, regula regras específicas da responsabilidade das pessoas colectivas, não se considerando necessária uma regulação especial no âmbito da criminalidade

informática. Contudo, se analisarmos o nº1 daquele artigo, podemos verificar que ao considerar que apenas as pessoas singulares são criminalmente responsáveis, salvo o disposto no nº2 e nos casos especialmente previstos na lei, temos que concluir que se impõe, no âmbito da LC, uma referência expressa a este tipo de responsabilidade.

5.7. Jurisprudência

- **Sentença do Tribunal Judicial da Comarca de Coimbra, 3º Juízo Criminal, processo nº63/97**

Na fundamentação de direito, esta sentença, remete o regime da responsabilidade penal das pessoas colectivas, primeiramente para o art. 11º do CP, fazendo referência ao previsto no seu nº1, para depois concluir pelo previsto no art. 3º da LCI – "as pessoas colectivas, sociedades e meras associações de facto são penalmente responsáveis pelo crimes previstos na lei, quando cometidos em seu nome e no interesse colectivo pelos órgãos ou representantes". Não fica desta forma excluída a responsabilidade singular dos agentes, sendo que as pessoas colectivas são solidariamente responsáveis nos termos da lei civil, pelo pagamento de multas, indemnizações e outras prestações a que forem aqueles condenados. A sentença releva os requisitos do art. 3º da LCI – responsabilidade da pessoa colectiva pelos crimes previstos na LCI, quando os actos ilícitos forem praticados em seu nome e seu interesse.

- **Acórdão do Tribunal da Relação de Lisboa de 05-05-2005, processo nº 3194/2005-9, relator Fernando Estrela**

Sumário**: "**I – Apesar de uma sociedade comercial ter instalado no seu sistema informático software sem autorização dos seus legítimos titulares e, como tal, sendo ilegítima a respectiva utilização, penalmente censurável nos termos dos artºs 14º do DL 252/94, de 20/10 e 9º da Lei nº 109/91, de 17/8 (crime de reprodução de programa protegido); II – É de manter o despacho de não pronúncia recorrido porque, não se reunindo indícios suficientes da prática de tais factos pela funcionária arguida e a quem a autoria material poderia ser imputada, também o não pode ser à pessoa colectiva, cuja responsabilidade civil sempre dependeria da responsabilidade penal de quem tivesse agido como seu órgão ou representante."

6. Os Prestadores de Serviços de Internet

6.1. Quem são

O papel que os prestadores de serviços desempenham no mundo da informática é crucial nos dias de hoje, até porque muito do cibercrime existente passa por estes prestadores e por falhas que estes apresentam. Para o estudo do cibercrime ficar completo não poderia deixar esta matéria em falta, pois se analisarmos com algum detalhe os deveres a que estes prestadores estão obrigados, seja em matéria de protecção de dados pessoais e seu alojamento/armazenamento/conservação, compreendemos o porquê de ser determinante a cooperação destes no combate à cibercriminalidade. Acresce que se a informática gira em torno de muitos serviços fornecidos pelos prestadores de serviços, a cibercriminalidade desenvolve-se no seio destes.

6.2. Natureza jurídica

Existem diversos prestadores de serviços de internet, podendo estar todos inseridos numa só empresa ou em empresas diversas. Podemos dizer que prestador de serviços de Internet é o género do qual as demais categorias são espécies –prestadores de "backbone", prestador de acesso, prestador de correio electrónico, prestador de hospedagem e prestador de conteúdo. Aquele é considerado uma pessoa jurídica que fornece serviços para funcionamento da internet.

- **Prestadores de "backbone"** – são considerados os prestadores "rei" que se encontram no topo da hierarquia dos prestadores, isto porque, são considerados estruturas capazes de lidar com grandes volumes de informação, ou seja, quase a totalidade dos dados transmitidos através da internet, sendo normalmente composto de diversos cabos de fibra óptica de alta velocidade. Estes prestadores são essenciais para o funcionamento da internet pois é através deles que as empresas estabelecem a sua conexão à internet. É comum designar-se gestor da rede de telecomunicações, pois estes prestadores prestam serviços aos prestadores de acesso ou hospedagem que por sua vez revendem a conectividade a terceiros.

- **Prestadores de acesso** - fornecem serviços que possibilitem o acesso dos consumidores à internet, seja através de uma sua conexão a um prestador de "backbone" seja através de infra-estrutura própria para conexão directa. Podemos afirmar que a conexão à internet pode ser efectuada por conexões directas ou por meio de entidades que a disponibilizem, sendo este último caso o mais comum. O prestador de acesso, através de uma ligação a um prestador de "backbone", revende a conectividade a outros usuários, sejam empresas ou utilizadores individuais. Para ser considerado um prestador de acesso, basta que ofereça aos seus consumidores o acesso à internet e não qualquer outro serviço acessório (ex. correio electrónico ou conteúdo para ser visualizado). Em suma, estes prestadores apenas disponibilizam um endereço IP ao usuário para que este se possa conectar à internet. A relação que se estabelece entre os prestadores de acesso e usuários é de consumo, sendo que os contratos celebrados entre estes são de adesão, não permitindo ao usuário a discussão ou modificação das cláusulas.

- **Prestador de correio electrónico –** para que exista um prestador de correio electrónico, é necessário que exista um prévio acesso à internet. Muitos prestadores de acesso são também de correio electrónico, mas nem sempre tal acontece, daí que se imponha a diferença entre ambos. Desta forma um prestador de correio electrónico fornece ao usuário um nome e uma senha para uso exclusivo em um sistema informático que possibilita o envio e recebimento de mensagens electrónicas, disponibilizando um espaço limitado no disco rígido de um servidor remoto para o armazenamento de tais mensagens, o que possibilita ao usuário descarregar para o seu computador tais mensagens ou deixa-las simplesmente no servidor. O prestador pode estabelecer certas restrições ao uso do sistema, nomeadamente quando se trate de actos ilícitos na internet como por exemplo a disseminação de vírus. À semelhança do que acontece entre os provedores de acesso e usuários, a relação dos provedores de correio electrónico com aqueles também é de consumo.

- **Prestadores de hospedagem** – fornecem o serviço de armazenamento de dados em servidores próprios de acesso remoto, possibilitando o acesso de terceiros a esses dados, mediante as condições estabelecidas com o contraente do serviço. Podemos referir que o prestador de hospedagem oferece dois tipos de serviços: o armazenamento de arquivos (informações) num servidor e a possibilidade de acesso a estes mediante as condições estipuladas com o prestador de conteúdo (contraente), que pode optar por disponibilizar o

conteúdo ao publico em geral ou apenas a determinados usuários. Estes prestadores podem oferecer outro tipo de serviços, tais como registo de nomes de domínio, cópias de segurança do conteúdo alojado. De destacar que estes prestadores não exercem controlo sobre o conteúdo armazenado nos seus servidores, que é realizado, normalmente, pelos provedores de conteúdo.

- **Provedores de conteúdo** – disponibilizam na internet as informações criadas pelos prestadores de informação (responsáveis pela criação das informações divulgadas através da internet – autor das informações) utilizando para armazená-las servidores próprios ou de um provedor de hospedagem. Na maioria dos casos os provedores de conteúdo realizam um controlo prévio sobre as informações que divulga.

6.3. Responsabilidade civil dos prestadores de serviços nos E.U.A. e na Europa

Nos E.U.A., as normas jurídicas respeitantes a esta matéria encontram-se no **Communications Decency Act de 1996** e no **Digital Millennium Copyright Act de 1998**.

De referir que as isenções de responsabilidade previstas em qualquer um dos diplomas apenas isenta os prestadores de serviços de indemnizações, sujeitando-os a outras medidas de remoção ou bloqueio do conteúdo ilícito. Acresce que a responsabilidade civil dos prestadores de serviços pelos seus próprios actos deve ser resolvida com o recurso ao Código Civil e Código de Defesa do Consumidor, sendo que quando os actos ilícitos sejam praticados por terceiros, ou quando exista responsabilidade solidária dos prestadores, em caso de dolo ou negligencia, os diplomas a serem aplicados serão outros.

As principais normas europeias que regem a responsabilidade civil dos prestadores de serviços encontram-se nas **Directivas 2000/31/CE e 2001/29/CE**, ambas do Parlamento Europeu e do Conselho, comércio electrónico na União Europeia e direitos de autor e conexos na sociedade de informação, respectivamente.

6.4. Deveres dos prestadores de serviços de internet

Os prestadores de serviços no exercício da sua actividade, submetem-se a diversas situações jurídicas que impõem deveres de conduta, independentemente do que venha previsto nos contratos de adesão, de termos de utilização de serviços ou demais instrumentos jurídicos que limitam a sua responsabilidade. Dependendo dos casos a omissão de tais deveres pode levar à responsabilidade dos prestadores de serviços pela prática de actos próprios ou mesmo de terceiros. Os deveres impostos a estes prestadores podem advir de imposições legais, de deveres morais e de deveres contratuais.

6.4.1. Dever de utilizar tecnologias adequadas

Todos os prestadores de serviços devem garantir qualidade nos seus serviços, utilizando tecnologias próprias e adequadas ao tipo de actividade que exercem respeitando padrões mínimos necessários a uma prestação adequadas, sendo que se for necessário deve investir em equipamentos informáticos e programas de computador novos. A inobservância de tal dever, ou seja, a inutilização de tecnologias apropriadas, como por exemplo a não adopção de anti-vírus ou sistemas de segurança abaixo dos padrões exigidos, responsabiliza directamente o prestador de serviços, quando o acto seja por ele praticado, ou responsabiliza solidariamente quando o acto seja praticado por terceiro que não foi prevenido por falha ou defeito da tecnologia utilizada.

6.4.2. Dever de conhecer os dados dos seus usuários

Os prestadores de serviços permitem aos seus clientes transmitir e aceder a diversas informações através da internet, podendo actuar como intermediários – quando disponibilizam estruturas e servidores – ou directamente – quando actuam como prestadores de conteúdo.

Os utilizadores da internet quando visitam um site ou recebem um mensagem não têm como confirmar que a informação que estão a visualizar seja verídica, pois é possível, a terceiros, sejam eles empresas ou pessoas singulares, omitir a sua identidade, pelo que apenas os prestadores de serviços têm conhecimento de quem são verdadeiramente os sujeitos responsáveis pelo armazenamento, transmissão ou divulgação de dados e informações. Se os dados fornecidos pelos utilizadores de serviços foram insuficientes ou até mesmo falsos, ao ponto de não ser possível determinar a sua localização, os prestadores tornam-se

solidariamente responsáveis pelo acto cometido por terceiro que não possa ser identificado ou localizado.

Assim, impõe-se que os prestadores adoptem meios tecnológicos e equipamentos informáticos capazes de identificar os dados de conexão dos seus utilizadores (no momento da contratação com o utilizador deverá ser exigido os dados, nomeadamente nome, endereço e números de documentos de identificação), mesmo que os dados fornecidos por estes não sejam correctos, a fim de os facultar a quem de direito aquando a ocorrência de um acto ilícito. Devem ser da mesma forma registados os endereços de IP atribuídos a cada utilizador, assim como os números de telefone necessário para estabelecer a ligação à internet e o endereço físico da instalação dos equipamentos informáticos utilizados para ligações de alta velocidade.

6.4.3. Dever de manter informações por tempo determinado

Os prestadores de serviços guardam os dados dos seus utilizadores e das conexões por eles realizadas, possibilitando a sua identificação e localização, de modo a que quando seja praticado um acto ilícito se identifique o seu infractor. Quando se estabelece uma ligação à internet é atribuído um número de IP ficando automaticamente registado no prestador de serviço, permitindo saber quem estava conectado à internet num determinado momento, o mesmo se passa quando se envia uma mensagem de correio electrónico, pois o servidor de correio regista o número de IP que pretende enviar a mensagem, assim como outros dados de conexão. Tal acontece, igualmente, quando o servidor autoriza o armazenamento de certos arquivos, pois previamente existe uma ligação que se estabelece entre o computador do utilizador e o prestador de hospedagem, registando-se neste momento o endereço IP. Podemos verificar que os prestadores de serviços registam automaticamente certos dados técnicos relativamente às conexões efectuadas pelos seus utilizadores, que se revelam de extrema importância, como referido, quando ocorra um facto ilícito.

Quando os prestadores não preservem os dados dos seus utilizadores, respondem solidariamente pelos actos ilícitos cometidos por terceiros que não puderem ser identificados ou localizados.

A preservação de tais dados não pode ser perpétua uma vez que se tornaria impossível aos prestadores de serviços suportar o volume de dados gerados.

6.4.4. Dever de sigilo sobre os dados dos utilizadores – ver constituição – direito à privacidade e lei de protecção de dados pessoais

Os prestadores de serviços estão obrigados ao sigilo sobre os dados pessoais (nome, endereço, números de identificação) e de conexão (endereço IP, datas de login e logout, nome de utilizador) dos seus utilizadores, que não englobam o conteúdo das comunicações ou das transmissões de dados. Tal dever cessa apenas nos casos previstos na lei, nos contratos, por autorização expressa do seu titular ou quando um utilizador pratique acto ilícito.

O dever de sigilo imposto aos prestadores de serviços decorre do direito à privacidade previsto na Constituição, não sendo contudo absoluto.

6.4.5. Dever de não controlar

Os prestadores de serviços estão obrigados a não monitorizar os dados e conexões realizadas nos seus servidores, dever este decorrente da garantia constitucional do sigilo das telecomunicações que comporta excepções apenas em casos especiais – no âmbito penal. Quando exista monitorização, estamos perante uma verdadeira intercepção de comunicações, pelo que só são admissíveis no domínio penal através das normas penais previstas para este âmbito, nomeadamente quando o prestador de serviço tenha participado de alguma forma no acto ilícito ou quando a prova não puder ser feita por qualquer outro meio. Fora dos casos previstos na lei, quando o prestador de serviços controlar os dados, conexões ou comunicações realizadas pelos seus utilizadores incorrerá em responsabilidade criminal.

6.4.6. Dever de não censurar

Os prestadores de serviços não podem censurar a informação transmitida ou armazenada nos seus servidores, devendo apenas remover ou bloquear o acesso a determinada informação se não houver duvidas da sua ilegalidade ou quando judicialmente autorizados. As excepções previstas a este dever apenas ocorrem quando exista violação de alguma norma jurídica ou do próprio contrato ou como referido mediante ordem judicial.

6.4.7. Informar quando seja cometido um acto ilícito por parte de um utilizador

O sigilo imposto aos prestadores de serviços sobre os dados pessoais e de conexão dos seus utilizadores é afastado quando este pratique um acto ilícito através da internet, sendo que nestes casos os prestadores de serviços têm o dever de fornecer tais dados quando sejam

solicitados por autoridade competente ou quando a sua divulgação esteja prevista nos contratos de prestação de serviços. É de realçar que estes dados pessoais e de conexão não se confundem com o conteúdo das comunicações e transmissões efectuadas pelos utilizadores, mas apenas os dados que permitem a sua identificação e localização.

6.5. A cooperação dos prestadores de serviços com as autoridades no combate ao cibercrime e as suas obrigações neste âmbito

6.5.1. O regime previsto na Convenção sobre o Cibercrime

Antes de iniciar a análise a esta matéria convém referir que a Convenção faz referência a "prestador de serviço", tendo a lei portuguesa optado pela designação de "fornecedor de serviço"

- **Artigo 1º - C)**

Um "prestador de serviços""abrange uma ampla categoria de pessoas que desempenham um papel particular no que diz respeito à comunicação ou ao tratamento de dados em sistemas informáticos, sendo que se encontram abrangidas por esta definição tanto as entidades públicas como privadas que proporcionem aos utilizadores a capacidade de comunicarem entre si através de um sistema informático, independentemente de se verificar que a comunicação é feita através de um grupo fechado ou não e se é feita de forma gratuita ou onerosa"[82].

O termo "prestador de serviços" é também aplicável às entidades que procedem ao armazenamento ou tratamento de dados em nome dos seus utilizadores.

Assim, podemos englobar neste conceito tanto os serviços de "hosting" e "caching", quer os serviços de ligação a uma rede.

É deste âmbito excluído um fornecedor de conteúdos, como por exemplo no caso de uma pessoa contratar uma empresa de "hosting" para armazenar a sua página Web.

- **Acesso ilícito e intercepção ilícita**

A melhor forma de prevenir o acesso não autorizado é através da introdução e desenvolvimento de medidas de segurança, sendo que os próprios fornecedores de serviços devem garantir que os seus sistemas estão protegidos contra o acesso ilícito, para que se mantenha a confidencialidade dos seus dados ou privacidade nas comunicações.

"Embora a transmissão de dados de conteúdo prejudiciais ou de códigos dolosos através da internet requeira a assistência de um fornecedor de serviços enquanto

[82] Venâncio, Pedro Dias, A Lei do Cibercrime Anotada e Comentada, Coimbra, 1ª ed., 2001, pag. 166 e 167

intermediários, um fornecedor de serviços que não apresente qualquer intenção criminal não poderá ser responsabilizado ao abrigo no disposto nesta secção"[83]. Desta forma, entende-se que não recai sobre o fornecedor de serviços a responsabilidade de controlo e fiscalização permanente dos conteúdos.

- **Art. 12 – Responsabilidade das pessoas colectivas**

Um fornecedor de serviço não incorrerá em responsabilidade criminal no caso de um utilizador seu, cliente ou qualquer outra pessoa, ter cometido um crime no seu sistema, pois a expressão "agindo sob a sua autoridade" aplica-se exclusivamente a funcionários ou representantes que actuem no seio das suas competências.

- **Direito Processual**

Os redactores da Convenção colocaram a hipótese de ser imposto aos fornecedores de serviços a obrigação de recolher e conservar regularmente os dados de tráfego, por um período de tempo determinado, não tendo ficado nada vinculativo por não se ter chegado a um consenso no seio da redacção da Convenção.

Sobre o direito processual serão feitas apenas breves referências para realçar o papel dos prestadores de serviços, remetendo esta análise para o capítulo referente ao direito processual constante na Convenção sobre o Cibercrime.

- **Preservação/conservação expedita de dados informatizados armazenados – Art. 16**

Aplicam-se a dados de tráfego armazenados que foram já recolhidos e arquivados pelos detentores de dados, como por exemplo os fornecedores de serviços.

Para que se proceda à preservação de dados, as partes devem emitir uma ordem, no âmbito de uma investigação criminal ou acção penal específica, referente a "dados específicos informatizados e armazenados, que se encontrem na posse ou sob o controlo de uma pessoa" (art. 16º) durante um período de tempo até à sua divulgação.

A preservação de dados reveste uma importância extrema nas investigações, pois impede que aqueles se alterem ou se eliminem. Dado ao carácter volátil destes dados, caso não se proceda à sua preservação, as provas poderão ser facilmente perdidas.

[83] Venâncio, Pedro Dias, A Lei do Cibercrime Anotada e Comentada, Coimbra, 1ª ed., 2001, pag. 173 a 176

Para os órgãos incumbidos de proceder à investigação criminal, muitas vezes, a melhor forma de preservar a integridade dos dados é proceder à sua busca ou apreensão. Esta medida mais rígida, pode ser contornada por exemplo nos casos em que o detentor dos dados seja de confiança ou uma empresa reconhecida e com nome. Nestes casos as autoridades competentes procedem à emissão de uma ordem de preservação de dados.

Acresce que nestes casos, as provas, como o conteúdo das comunicações ou conteúdo dos próprios actos, deverão ser conservados pelos fornecedores de serviços, de forma a garantir que as de cariz relevante não são perdidas, como por exemplo as mensagens de correio electrónico.

- **Preservação/conservação expedita e divulgação parcial de dados de tráfego – art.17º**

Este artigo prevê as situações em que os dados de tráfego são repartidos entre fornecedores de serviços, onde cada um detém uma parte importante para a detecção de toda a comunicação. Assim, possibilita a que se proceda a uma preservação expedita dos dados de tráfego junto de cada um dos referidos fornecedores de serviços

Assim que o fornecedor receber a notificação de uma ordem de preservação expedita de dados, deve de imediato proceder à sua divulgação junto das autoridades competentes, de uma quantidade suficiente de dados de tráfego de forma a permitir a identificação de outros fornecedores de serviços, bem como o rumo da comunicação transmitida.

- **Injunção de comunicar / ordem de produção – art. 18º**

A ordem de produção prevista no art. 18º consiste na emissão de uma ordem que investe as autoridades competentes de poderes necessários para obrigar uma pessoa que se encontre no seu território a fornecer os dados armazenados especificados ou um fornecedor de serviços que ofereça os seus serviços no território da parte, a prestar informações relativas aos subscritores (dados informatizados ou informações).

- **Recolha, em tempo real, de dados de tráfego– art. 20º e 21º**

É aqui previsto a recolha em tempo real de dados de tráfego e da intercepção em tempo real de dados de conteúdo associados a comunicações específicas transmitidas por meio de um sistema informático. As autoridades competentes em cooperação com os prestadores de serviços têm competência para procederem a recolha e intercepção das

comunicações específicas transmitidas por meio de um sistema informático, antes mesmo de ser recebida por outro sistema. É de notar o importante papel dos fornecedores de serviços nesta matéria, pois são eles que possibilitam a comunicação por meio de um sistema informático. Esta recolha de dados decorre aquando a transmissão da comunicação – tempo real – não interferindo na dita comunicação.

As autoridades podem obrigar um fornecedor de serviços a recolher ou registar dados de tráfego ou exigir que este colabore e apoie aquelas em tudo o que for necessário para a execução da medida de recolha ou registo dos dados. De realçar que esta colaboração apenas incide no âmbito da real capacidade técnica dos fornecedores de serviços, não os responsabilizando nos casos em que não detêm capacidade para prestar a sua colaboração ou proceder eles mesmo à recolha ou registo de dados, nem os obrigando a adquirir novos equipamentos para tal, a não ser que o sistema ou a pessoa possua essa capacidade, por exemplo nos casos em que bastaria apenas a reconfiguração do sistema ou a instalação de programas que possibilitasse a recolha ou registo.

As obrigações impostas aos fornecedores de serviços apenas se verificam nas situações em que este disponha no território da parte de alguma infra-estrutura ou equipamento possível de permitir a execução das medidas, independentemente da sua sede ou estabelecimento da actividade principal se situar no mesmo território.

Considera-se que uma comunicação é feita no seio do território da parte caso um dos intervenientes na comunicação esteja situado nesse território (pessoa ou computador) ou o equipamento informático que permite a comunicação.

Pode acontecer que as autoridades, por motivos de incompatibilidade com os princípios jurídicos nacionais, não disponham de condições necessárias para executar a recolha e registo de dados, sendo que nestes casos podem obrigar os fornecedores de serviços a prestarem apenas os meios técnicos para que procedam elas à recolha de dados de tráfego em tempo real.

Como foi mencionado acerca de outras medidas processuais, é exigido aos fornecedores de serviços e à pessoa que recolha os dados, confidencialidade, pois a medida só será eficaz se não for do conhecimento da pessoa visada.

6.5.2. Directiva 2000/31/CE – comércio electrónico

- **Art. 14**

O art. 14º estabelece que o prestador de serviço que possibilite o armazenamento no servidor não é responsável pela informação aí armazenada sempre que actue com diligência (remoção e impedimento de acesso) quando tiver conhecimento de que a informação alojada é ilícita.

Não existe responsabilidade quando o prestador tiver conhecimento da informação ilegal e actuar de imediato de forma a esta ser removida e se tornar inacessível ao público. Como os prestadores não estão obrigados a um controlo prévio da informação neles alojada, o conhecimento referido só é possível quando os factos ilícitos lhes forem comunicados por terceiros.

6.5.3. Directiva 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 comunicação

Esta directiva dispõe que "as medidas nacionais relativas ao acesso ou à utilização de serviços e aplicações através de redes de comunicações electrónicas pelos utilizadores finais devem respeitar os direitos fundamentais dos cidadãos, nomeadamente em relação à privacidade e ao direito a um processo equitativo previsto no art. 6 da Convenção Europeia para a Protecção dos Direitos do Homem e das Liberdade Fundamentais".

Para o que importa ao tema a ser estudado, podemos referir que "No caso de violação de dados pessoais, o prestador dos serviços de comunicações electrónicas acessíveis ao público comunica, sem atraso injustificado, a violação à autoridade nacional competente. Caso a violação de dados pessoais possa afectar negativamente os dados pessoais e a privacidade do assinante ou de um indivíduo, o prestador notifica essa violação ao assinante ou ao indivíduo sem atraso injustificado." – Art. 4º nº 3 . "Os Estados Membros asseguram que o armazenamento de informações ou a possibilidade de acesso a informações já armazenadas no equipamento terminal de um assinante ou utilizador só sejam permitidos se este tiver dado o seu consentimento prévio com base em informações claras e completas, nos

termos da Directiva 95/46/CE, nomeadamente sobre os objectivos do processamento.", Art. 5º nº 3.

Alguns Estados Membros impõem a vigilância dos dados em circulação na rede aos seus prestadores de serviços, é o caso[84]

- França – Loi Hadopi (Lei n.º 2009-669, de 12 de Junho de 2009, favorecendo a difusão e a proteçãoda criação na Internet)
- Reino Unido – o Digital Economy Act, proposto em 20 Novembro de 2009, entretanto retirado no que respeita à vigilância e suspensão do acesso
- Espanha – Ley Sinde (Lei 2/2011, de 4 de Março, de Economia Sustentável)

Estamos aqui perante dados de tráfego já definidos na Convenção sobre o Cibercrime e na Lei do Cibercrime Portuguesa, dados de localização e dados conexos necessários para identificar o assinante ou utilizador.

A Directiva relativa à Conservação de dados vem impor obrigações aos "fornecedores de serviços de comunicações electrónicas publicamente disponíveis ou de uma rede pública de comunicações em matéria de conservação de determinados dados por eles gerados ou tratados, tendo em vista garantir a disponibilidade desses dados para efeitos de investigação, de detecção e de repressão de crimes graves, tal como definidos no direito nacional de cada Estado-Membro." - Art. 1º nº 1. Sendo que "Os Estados-Membros devem assegurar que as categorias de dados […] sejam conservadas por períodos não inferiores a seis meses e não superiores a dois anos, no máximo, a contar da data da comunicação." - Art. 6º.

O regime aqui previsto tem sido alvo de inúmeras críticas por parte dos Estados Membros, nomeadamente, através da Jurisprudência dos tribunais nacionais, em face do Princípio do Primado do Direito da U.E. sobre os Direitos nacionais, os Tribunais Nacionais apenas têm poder para avaliar as leis de transposição, considerando inconstitucionais vários preceitos das mesmas, como ocorreu já na Alemanha, na Roménia e na Bulgária. Contudo e devido a estes acontecimentos nos Estados Membros o Tribunal de Justiça da União Europeia está em vias de o fazer relativamente à própria Directiva.

[84] Ver ponto 2.2 Direito Comparado - Tese

- ***Portugal***

Actualmente o regime legal vigente não prevê a imposição aos prestadores de serviços intermediários de uma obrigação geral de controlo sobre os conteúdos transmitidos e difundidos através dos seus serviços. É, apenas, previsto para os intermediários de alojamento principal a obrigação de retirada dos conteúdos manifestamente ilícitos após o conhecimento de que os mesmos se encontram alojados nos seus servidores.

O RJCE, pressupõe uma actuação a posteriori do intermediário no sentido da remoção do conteúdo ilícito após a sua colocação na internet. De acordo com o **art.4ºnº5** deste diploma, nos casos em que o "prestador de serviços intermediários" seja parte interessada na colocação de conteúdos, como por exemplo o caso do site "Ebay", que lucra com a venda do produto final, já poderá ser exigível ao prestador de serviços que actue activa e preventivamente na remoção de conteúdos ilegais que sejam colocados e/ou difundidos na rede pelos serviços que disponibiliza.

- **Lei nº 32/2008 de 17 de Julho**

Em Portugal, a Directiva foi transposta para a ordem jurídica interna através da Lei 32/2008 de 17 de Julho relativa conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações.

O **art. 2º** da presente lei fornece definições essenciais para a interpretação da mesma, pois o **art. 3º** ("Finalidade do tratamento") prevê que "a conservação e a transmissão dos dados têm por finalidade exclusiva a investigação, detecção e repressão de crimes graves por parte das autoridades competentes", sendo a mesma autorizada ou ordenada por despacho do juiz, sujeito às regras do **art. 9º** ("Transmissão de dados" - quando existam razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria de outra forma de difícil ou impossível obtenção) não podendo o titular dos dados opor-se à conservação ou transmissão. Como tal, temos sempre que nos recorrer do art. 2º, nomeadamente da g) e f) do nº1 que define crime grave e autoridades competentes, respectivamente.

É imposto aos fornecedores de serviços que conservem os dados previstos no **art. 4º** ("Categorias de dados a conservar"), pelo período de um ano a contar da data da conclusão da comunicação.", **Art. 6º**. O processo de transmissão de dados deve cumprir com as exigências constantes no **art.9º**, sendo que apenas pode autorizada a transmissão de dados relativos a "suspeito ou arguido; a pessoa que sirva de intermediário, relativamente à qual haja fundadas razões para crer que recebe ou transmite mensagens destinadas ou provenientes de suspeito ou arguido; ou a vítima de crime, mediante o respectivo consentimento, efectivo ou presumido" – nº 3 a) a c). Por fim a "decisão judicial de transmitir os dados deve respeitar os princípios da adequação, necessidade e proporcionalidade, designadamente no que se refere à definição das categorias de dados a transmitir e das autoridades competentes com acesso aos dados e à protecção do segredo profissional, nos termos legalmente previstos" – nº4

A Lei 32/2008 respeita os limites impostos a nível constitucional, seja pelo art. **18º nº2** que estabelece os casos em que é permito a lei restringir direitos, liberdades e garantias, o **art. 34º nº4** que proíbe a ingerência das autoridades na correspondência, telecomunicações e outros meios de comunicação, salvo nos casos de processo criminal e o **art. 35º nº2** que protege os dados pessoais

- **Lei do Cibercrime**

É de salientar, em primeiro lugar, que a Lei 109/2009 – LC – refere no seu art. 11º nº2 que as disposições processuais constantes na LC não prejudicam o regime da Lei 32/2008, sendo sempre necessário conjugar as duas leis.

Os **art. 12º a 17º**da LC estabelecem requisitos de acesso dos órgãos de investigação policial e dos Tribunais a estes dados, e por outro, as obrigações de colaboração dos fornecedores de serviços responsáveis pelo tratamento desses dados. Como a análise a estas obrigações foi já analisada em sede da CCib remetemos o estudo destes artigos para a análise geral feita à LC e aos artigos da CCib sobre a mesma matéria.

Assim, a lei do Cibercrime exige que os ISP preservem os dados informáticos referentes a um sistema informático, ou os dados relativos a um cliente, atendendo ao que dispõe a Directiva do Comércio Electrónico, excluindo mais uma vez qualquer dever de vigilância na transmissão de conteúdos. A responsabilidade neste ultimo caso apenas surge

quando são informados pelo titular do direito ofendido ou autoridade competente e nada fizerem para interromper os actos ilícitos.

- **Lei nº 7/2004 de 7 de Janeiro**

O DL nº7/2004 de 7 de Janeiro, dispõe no seu **art. 4º** que prestadores intermediários em rede são os que "prestam serviços técnicos de acesso, disponibilização e utilização de informações ou serviços em linha independentes da geração da própria informação ou serviço".

A responsabilidade do prestador intermediário de serviços, engloba tanto a responsabilidade civil, como penal, existindo especificidades para cada um dos regimes.

Podemos traçar alguns aspectos do regime legal destes prestadores:

- A actividade do prestador de serviços está sujeita à lei do país de origem, à excepção de algumas matérias como é o caso da propriedade intelectual[85];
- Estão sujeitas ao princípio da liberdade de exercício de actividade[86];
- A responsabilidade dos prestadores está sujeita ao regime comum da responsabilidade[87];
- Não existe um dever geral de vigilância dos conteúdos transmitidos[88], contudo, em determinados casos e aquando a colaboração em investigações, este verifica-se[89];
- Pode existir um agravamento ou desagravamento da responsabilidade dependendo do serviço prestado[90];
- Utilização de um mecanismo de notificação e retirada em caso de ilicitude de conteúdos armazenados[91]

A LCE, no seu **art. 13º**, prevê deveres que devem ser cumpridos pelos prestadores de serviços, entre eles, o dever de informação, o dever de resposta e cumprimento das decisões provenientes de entidades competentes em matéria de fiscalização e ainda dos tribunais. O

[85] Art. 4º nº1, 5º nº1 e 6º a) LCE
[86] Art. 3º nº3 LCE
[87] Art. 11º LCE
[88] Art. 12º LCE
[89] Art. 13º LCE
[90] Art. 14º a 17º LCE
[91] Art. 18º LCE

art. 14º do mesmo diploma legal exclui a responsabilidade dos prestadores desde que estes se dediquem a prosseguir licitamente a sua actividade, seja ela de facultar o acesso a uma rede ou de transmitir informações em rede, sem qualquer ingerência no seu conteúdo, na origem ou destino da sua transmissão, ou seja, a actividade do prestador é meramente técnica sem qualquer conhecimento da informação transmitida ou armazenada.

Para que o prestador de serviços seja penalmente responsável, impõe-se que o conhecimento da ilicitude dos conteúdos alojados ou armazenado – **art. 16º nº1** LCE – seja efectivo. Este conhecimento pode resultar de queixa dos interessados dignos de tutela[92], sendo que nestes casos o prestador analisa se a ilicitude é ou não manifesta[93] ao ponto de retirar o conteúdo, isto sem prejuízo da intervenção do mecanismo de resolução provisória do litígio[94].

O prestador de serviços que tenha conhecimento de conteúdos ilícitos deve deve comunicar às entidades competentes e posteriormente acatar com a decisão proferida – art. 12º LCE, seja ela de remoção ou restrição de acesso ao conteúdo – art. 15º nº3 e 16º nº1 LCE.

- ***Brasil***

No Brasil, o Marco Civil não estabeleceu nenhum dever para o utilizador de internet, apenas direitos como o da privacidade e neutralidade de rede, sendo os deveres apenas aplicados aos fornecedores de acesso, serviços e conteúdo. Ao tornar a guarda ou armazenamento dos logs (entradas de utilizadores) facultativa para os provedores, incluindo os e-mails no cloud computing (nuvem) e redes sociais, torna-se mais difícil a identificação de um criminoso. Para se solicitar informações a um provedor de acesso, que se encontra obrigado a guardar o log por um ano, é necessário primeiro identificar o IP usado na publicação do conteúdo.

A responsabilidade do provedor de acesso apenas surge quando este desobedeça a uma ordem de remoção de conteúdo.

No Brasil o art. 241, §1°, do ECA, prevê a possibilidade de responsabilização criminal dos administradores de fornecedores de acesso e de hospedagem de páginas, quando estes, dolosamente, assegurem os meios ou serviços para o acesso ou armazenamento na internet de fotografias, cenas ou imagens ilícitas. Depois de terem conhecimento de que

[92] Art. 18º LCE
[93] Art. 18 nº1 LCE; ilicitude manifesta – art. 16º nº2 LCE – ilicitude de natureza subjectiva (prestador deve ter consciência da ilicitude)
[94] Art. 18º nº2 e 39º LCE – intervenção da autoridade de supervisão

alojam conteúdos ilícitos, os fornecedores têm o dever de informar as autoridades judiciárias sobre o facto, sob pena de responderem pelo crime tipificado no art. 241º §1º, incisos 2 ou 3, do estatuto da criança e do Adolescente.

A legislação brasileira sobre a responsabilidade dos prestadores de serviços relativamente aos crimes cibernéticos é manifestamente deficiente, uma vez que não há, uma definição clara dos deveres das empresas que mantêm serviços de acesso e hospedagem de páginas, em matéria criminal.

A Lei Brasileira 10.764/03 previu explicitamente a responsabilidade criminal dos administradores e empregados de prestadores, quando estes:

a) Assegurem os meios ou serviços para o armazenamento das fotografias ou imagens de crianças ou adolescentes em cenas de sexo explícito;

b) Assegurem, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, de tais cenas ou imagens.

À parte das leis existentes e da falta de coerência de muitas delas, no Brasil, o Ministério Público, tem celebrado "termos de compromisso" com os prestadores locais, tendo como objectivo uma cooperação destes através de condutas por eles tomadas que:

a) Divulguem campanhas contra a pornografia infantil e contra os crimes de ódio;

b) Orientem o público sobre a utilização não criminosa de salas de chat, grupos e fóruns de discussão, blogs, páginas pessoais e outros serviços disponibilizados ao utilizador;

c) Insiram, nos instrumentos de adesão ao serviço, uma cláusula que preveja a rescisão contratual na hipótese do utilizador utilizar os serviços que detém com o prestador para publicar fotografias e imagens de pornografia infantil, ou ideias preconceituosas quanto à origem, raça, etnia, sexo, orientação sexual, cor, idade, crença religiosa ou outras formas de discriminação;

d) Mantenham "link" pelo qual os utilizadores possam informar ao prestador signatário as condutas referidas neste termo, quando praticadas em ambiente, página, grupo de discussão, álbum electrónico, ou outro serviço prestado pelo próprio prestador;

e) Informem imediatamente o MP federal, quando tomem conhecimento de que alojam pornografia infantil ou conteúdo manifestamente discriminatório;

f) Preservem e armazenem, pelo prazo mínimo de 6 meses, o registo de "logs" de acesso e quando possível também os "IP´s" originários dos utilizadores dos serviços de "Web page", salas de chat, fotologs, fóruns de discussão on-line e outros;

g) Solicitem e mantenham os dados pessoais ou de acesso informados pelos utilizadores;

h) Exijam que os novos utilizadores informem o número de algum documento válido de identificação.

Este protocolos de cooperação revelam extrema importância na medida em que muitas vezes os prestadores de serviços "ajudam" na divulgação e publicação de materiais ou condutas ilícitas realizadas pelos seus utilizadores. Esta cooperação permite combater o cibercrime e obrigar os prestadores a prestar informações que sejam solicitadas pelas autoridades e quando não o façam são responsáveis de acordo com a lei vigente, na medida em que se tornam cúmplices do criminoso.

Em países mais empenhados no combate a este tipo de crimes – Holanda, Suécia, Austrália e Canadá – a lei prevê que os prestadores de serviços informem as autoridades logo que tomem conhecimento de crimes cometidos no uso dos serviços de Internet e também preservem as provas necessárias à investigação criminal, por um prazo mínimo estabelecido por lei.

Na maioria dos casos a identificação de um cibercriminoso, passa pela identificação e localização do seu endereço "IP", que pode ser estático ou dinâmico, consoante os casos, mas em todos eles é atribuído por um prestador de serviços que gere milhares de "IPs"

Para que seja possível identificar qual o utilizador que estava ligado a determinado endereço "IP", num determinado dia e hora, os prestadores de acesso e de hospedagem devem manter uma base de dados electrónicos, uma lista de cada endereço "IP" utilizado, juntamente com a correspondente data, horário e local de conexão. A "International Association of Prosecutors" recomenda que os prestadores mantenham os "logs" de acesso pelo prazo mínimo de um ano, de forma que, quando forem formalmente requisitados, tenham disponível tal informação, cooperando com as entidades que investigam o crime, sejam eles nacionais ou internacionais.

6.6. Protocolos de cooperação

6.6.1. Despacho da PGR de 25 de Setembro de 2012

Número: 12/2012 - Proferido nos termos e para os efeitos do disposto no artigo 12º, n.º 2, alínea b), do Estatuto do Ministério Público, na redacção da Lei n.º 60/98, de 27 de Agosto.

A PGR assinou, a 9 de Julho de 2012, um protocolo de cooperação com operadores de comunicações, no âmbito da investigação da cibercriminalidade e da obtenção de prova digital. Este operadores, entidades de direito privado, produzem e guardam informação que se considera de especial importância no âmbito da obtenção de prova no decurso de um processo penal, de forma que se impõe uma estrita cooperação entre estes e o MP, titular da acção penal, diminuindo as possíveis divergências existentes no relacionamento processual entre estas duas entidades.

Para tal, criaram-se pontos de contacto permanente entre aquelas entidades, que dentro dos limites legais definidos, contribuem para o esclarecimento de dúvidas ou para soluções no seio de um processo de inquérito, quando tal não se mostre possível de outra forma. Foi definido pelo MP um conjunto de procedimentos para obrigações de cariz institucional e também no tratamento destes casos em sede de inquérito.

Assim, sempre que se mostre necessária a prestação de informação por parte de um operador e o MP solicitar elementos de prova, deve faze-lo através de uma plataforma informática, tendo sido disponibilizado o recurso ao SIMP (Sistema deInformação do Ministério Público), assegurando celeridade processual. Estas solicitações obedecem sempre a formulários pré-elaborados, o que facilita os pedidos, tornando-os simples e eficazes, sendo que nos casos em que não seja possível remete-los via electrónica, estão disponíveis em suporte papel e são remetidos pelas vias normais.

Os pedidos realizados pelo MP aos operadores de serviço, devem obedecer a um critério de necessidade, atendendo à descoberta da verdade, assim como de clareza quanto às formulações efectuadas, indicando com exactidão os dados que pretendem, pois só assim obterão respostas exactas.

Face ao exposto, a PGR, ao abrigo do disposto no artigo 12º, n.º 2, al. b), doEstatuto do Ministério Público, determina que os Magistrados e Agentes do Ministério Público obedecem a um conjunto de instruções:

- Os pedidos dirigidos aos operadores, em sede de inquérito, devem obedecer a um critério de necessidade;
- Cada pedido deve especificar o objectivo concreto de forma a permitir aos operadores responder com mais eficácia atendendo aos interesses da investigação.
- Os pedidos formulados à "Optimus – Comunicações, S.A.", à "PTComunicações, S.A.", à "TMN – Telecomunicações Móveis Nacionais, S.A.", àVodafone Portugal – Comunicações Pessoais, S.A." e à "ZON TV Cabo Portugal,S.A.", são realizados com a utilização de um dos formulários anexos ao despacho da PGR, consoante o caso.
- Enquanto não for possível utilizar a plataforma destinada e estas solicitações, as mesmas são efectuadas em impressos em papel e remetidos pelas vias normais.

6.6.2. PGR - Gabinete do cibercrime

- ***Nota prática nº1/2012***

O endereço IP e a identificação do seu utilizador

O Protocolo celebrado a 9 de Julho de 2012 entre a Procuradoria-Geral da República e os operadores de comunicações adoptou procedimentos eficazes nos pedidos formulados pelo MP, em sede de inquérito, de forma a facilitar o entendimento entre estas entidades. Entre os pedidos efectuados para prestação de informação, podemos enunciar a da identificação do endereço IP utilizado por um determinado cliente do operador e, no sentido oposto, a da identificação do utilizador de um determinado endereço IP, num momento temporal conhecido e determinado.

Esta informação deve obedecer a trâmites legais que de seguida se explicam.

O endereço de IP tem suscitado algumas dúvidas quanto à sua natureza, pois não se prevê em nenhuma norma jurídica a sua consideração ou não como "um dado de tráfego". O entendimento dos tribunais tem demonstrado ser de elevada importância no que respeita à possibilidade de se obter informações desta natureza em processo-crime.

Em sede de inquérito, a obtenção de dados de tráfego de comunicações electrónicas, encontra-se prevista no art. 18º da Lei do Cibercrime, que é também aplicável à obtenção de dados de conteúdo das comunicações (Art. 18º, nº 1 e nº 3). Como vimos em altura própria,

esta obtenção depende de autorização judicial e só é admissível em fase de inquérito, em casos idênticos aqueles em que é possível realizar intercepções telefónicas.

No que toca aos outros tipos de dados informáticos, fora do âmbito dos dados de tráfego ou de conteúdo, aqueles podem ser obtidos em todas as fases processuais, de acordo com o art.14º da Lei do Cibercrime, através da injunção. Compete ao MP e pode ser ordenada sempre que se julgue necessário à descoberta da verdade.

A qualificação do endereço IP como dado de tráfego implica que a sua solicitação se faça mediante autorização do juiz de instrução, e apenas em sede de inquérito, quanto aos crimes que se considerem mais graves, pois tais dados apenas são permitidos obter nos mesmos casos em que se realizam as intercepções telefónicas, como anteriormente referido, e que a LC remete no seu art.18º nº1 b) e nº4. Acresce que se fosse dada tal qualificação ao endereço IP, tornava-se muito difícil a investigação da cibercriminalidade.

O endereço IP quando identificado, assim como de quem o utilizou em dia e hora determinada, não nos fornece o percurso realizado por essa comunicação nem de outras que o sujeito possa ter feito, apenas nos prova que aquela comunicação foi efectuada por aquele endereço de IP que conecta à internet. Assim através deste procedimento podemos, apenas, identificar uma ligação entre determinada comunicação e a sua origem. Diferentemente acontece, numa investigação quando se pretende informação sobre um período longo de tempo ou sobre inúmeras comunicações do mesmo sujeito, implicando uma entrada no domínio do tráfego.

Desta forma, quando se trate apenas de obter a identificação do sujeito que usa um certo endereço IP ou vice-versa, em tempo determinado (dia e hora), não será de aplicar a doutrina constante no Parecer nº 21/2000 do Conselho Consultivo da PGR, pois não se está a aceder a informação privada ou confidencial. [95]

O art. 2º c) da LC define o que são dados de tráfego através de um conceito muito abrangente. Tendo em conta que o regime jurídico aplicável à obtenção de dados de tráfego, é mais restritivo que o da obtenção de todos os restantes dados (que não sejam de conteúdo), a jurisprudência tem insistido na discussão sobre a natureza do endereço IP. Contudo, não tem tido resultados quanto à definição do seu estatuto processual, pois o art. 14º da mesma lei prevê o regime aplicável ao pedido do endereço IP aos operadores de comunicações, através de um regime especial, na injunção. É possibilitado ao MP obter, o endereço IP, através da injunção, basta que solicite aos fornecedores de serviço os dados informáticos que tenham

[95]Cf. Ponto 3, pág. 2, da Nota Prática nº1/2012

armazenados, excluindo-se deste pedido os dados de tráfego sujeitos ao regime do art. 18º da LC.

A LC não enquadra o endereço IP numa categoria especifica de dados, mas o art. 14º nº4 b) prevê um regime especial[96] aplicável à solicitação daquele por via da injunção, independentemente de o incluir nos dados definidos por lei. Quando no art. se encontra a expressão "número de acesso" estamos perante o endereço IP, tendo sido propositada para fazer referência àquele.

O endereço IP pode ser atribuído a um utilizador a título permanente ou a diversos utilizadores quando for um endereço dinâmico, mas em ambos o endereço IP é o "número de acesso". Se através deste procedimento não se acede a informação pessoal ou íntima, a diferença reside na forma como o fornecedor obtêm a informação que lhe é solicitada. Nos casos de endereço IP dinâmico, para o fornecer ao MP, a entidade tem que consultar dados de tráfego, que contudo não podem ser os que estão conservados por imposição da Lei nº 32/2008 (em relação aos quais há específicas obrigações de confidencialidade e limitação de acesso – Art. 7º, nº 1, alínea d) e Art. 8º, nº 1) de resto não estão os fornecedores impedidos de aceder aos mesmos, não podendo revelar a terceiros. Não podemos esquecer que os fornecedores de serviços devem monitorizar o tráfego das suas redes, de acordo com art. 3º da Lei 41/2004, de forma a garantir a segurança dos serviços que prestam e a segurança da própria rede e ainda, quando necessário, aceder aos dados de tráfego, de modo a cobrar qualquer pagamento, por exemplo, no decorrer da sua actividade, art. 6º nº2 da mesma lei. Assim, os fornecedores, para responder ao pedido efectuado e dar a informação sobre determinado IP, podem consultar dados de tráfego.Mais uma vez, em nenhuma destas leis, assim como na Convenção sobre o Cibercrime, se atribuiu um estatuto ao endereço IP, apenas se consagrou uma norma jurídica com vista à sua obtenção no decurso de uma investigação.

Podemos concluir que o endereço IP (seja identificação do endereço IP utilizado por um determinado indivíduo ou a identificação do cliente que usou um determinado endereço IP com dia e hora) pode ser solicitado (art. 14º nº4 b)) por via da injunção a quem tenha disponibilidade ou controlo desses dados, devendo faculta-los (art. 14º nº1). Esta solicitação deverá ocorrer no decurso de uma investigação independentemente do tipo de crime que esteja em causa, desde que se torne necessário à descoberta da verdade, pela autoridade

[96]Art. 14º nº4 b) obtençao de dados "*relativos aos seus clientes ou assinantes, neles se incluindo qualquer informação diferente dos dados relativos ao tráfego ou ao conteúdo, contida sob a forma de dados informáticos (...) e que permita determinar qualquer número de acesso*".

judiciária competente - na fase de inquérito, o Ministério Público. Esta informação por ter regime próprio na lei, está subtraída às limitações do art. 18º da LC.

7. A investigação do cibercrime

7.1. Dificuldades

Entre os inúmeros problemas inerentes à investigação do cibercrime, podemos apontar como principais, a falta de metodologia no tratamento da especificidade deste crime, a antiguidade dos sistemas, e a difícil cooperação na partilha de informações entre as entidades. As características deste tipo de crime, assim como o elevado grau técnico que exigem, o elevado número de processos e falta de pessoal especializado leva a uma morosidade enorme no tratamento de casos associados aos crimes informáticos. A estas dificuldades junta-se o factor da extraterritorialidade do cibercrime.

A identificação do sujeito que cometeu o ilícito é uma das maiores dificuldades no seio de uma investigação criminal, acresce que esta aumenta sempre que aquele utilize terminais públicos ou sistemas pré-pagos. Face a esta situação muitos países passaram a exigir que nestes locais seja obrigatória a identificação do utilizador.

Por outro lado, o acesso e distribuição de conteúdos ilegais através da internet, dificultam de igual modo o papel das autoridades na identificação do infractor, pois no caso da utilização de valores monetários virtuais não é exigida identificação.

Podemos apontar como outra dificuldade enfrentada pelas autoridades, mas no domínio das violações dos direitos de propriedade intelectual, os casos de partilha de ficheiros existentes em todo o circuito da internet, sendo que nem todos aqueles que são partilhados constituem uma violação daqueles direitos. Não é possível analisar todos os ficheiros que são partilhados, até porque tal pode implicar uma violação da privacidade e confidencialidade destes ficheiros.

A conferência RSA[97] em São Francisco, E.U.A., que contou com mais de 20 mil participantes, teve como objectivo melhorar a protecção das empresas contra os ataques provenientes do cibercrime, tendo o director do FBI afirmado que existem dois tipos de empresas, as que já foram atacadas e as que vão ser atacadas. Face a esta realidade aconselhou a que aquelas apostem fortemente nos seus sistemas de segurança de rede e informação.

[97] Empresa dedicada à criptografia, que realiza anualmente uma conferencia dedicada à segurança de sistemas informáticos. O seu nome resulta da junção da primeira letra do apelido dos 3 fundadores – Ron Rivest, Adi Shamier e Len Adleman, integrando o Instituto MIP

Um programa de partilha de informação – InfraGard – derivado de uma parceria com o sector privado, tem melhorado a segurança informática com redução de custos.

O Director do FBI, Robert Mueller, salienta que as empresas alvos de ataques informáticos não devem ter receio de os reportar às autoridades, pois estas vão conduzir as investigações sempre com respeito pela privacidade das entidades e vítimas. Defende que uma das formas de combate ao cibercrime passa por uma partilha de conhecimento, informação e formação sobre as novas tecnologias, algo que foi instituído no seio da organização com a criação de salas de reuniões virtuais onde os investigadores analisam e partilham dados sobre os seus casos.

Como referido no capitulo dedicado ao impacto da cibercriminalidade, as pessoas alvo do cibercrime não denunciam muitas vezes o ocorrido pelo facto de acreditarem que o autor do ilícito não será identificado. Contudo existe outras causas para a omissão de denúncia. No caso das empresas, a publicidade negativa (clientes poderão questionar a fragilidade dos sistemas da empresa) que poderá advir do conhecimento publico de que foi alvo de um cibercrime, faz com que muitas não denunciem o ocorrido.

O responsável pela Serious Organised Crime Agency (Soca) - organização britânica afirma que uma das formas de combater o cibercrime é através das empresas responsáveis pelo registo de domínios de sites, que devem dotar os seus sistemas actuais de ferramentas capazes de identificar quem regista domínios Web que depois são utilizados nestas práticas ilícitas, afirmando que "o que estamos a tentar fazer é incentivar a indústria a introduzir sistemas mais seguros, para que eles [as empresas de registo de domínios] possam saber quem é que registou estes sites, tenham uma base de dados de clientes mais abrangente e façam mais para evitar que os criminosos comprem sites e os utilizem para fins criminosos".

No ano de 2012, durante um seminário organizado pelo Observatório de Segurança, Criminalidade Organizada e Terrorismo (OSCOT), denominado "O desafio da cibersegurança", a então directora do Departamento de Investigação e Acção Penal (DIAP) de Lisboa, Maria José Morgado, referiu "sete obstáculos que criam dificuldades na intervenção e investigação criminal", alertando que os "sistemas informáticos são frágeis", que existe um "enquadramento legal confuso e compensador do crime" e uma "dispersão e sobreposição de autoridades competentes e o esforço insuficiente a nível da prevenção e repressão", aliado à falta de recursos informáticos e "os meios desproporcionados às ameaças".

Numa entrevista ao Expresso, Maria José Morgado, Director do DIAP de Lisboa, revelou que nos últimos anos existiu uma intensificação nos ataques informáticos em

Portugal, que envolvem, nomeadamente, fraudes, pornografia infantil, ataques dirigidos por grupos organizados contra estruturas bancárias e infra-estruturas críticas, sendo que estes ataques na sua maioria são levados a cabo por grupos anónimos. A falta de estrutura policial e operacional, assim como a falta de técnicos especializados torna difícil a investigação destes crimes, aliado à falta de apoio financeiro torna-se quase impossível terminar as investigações com acusações.

Só no ano de 2012 decorreram 1661 investigações, sendo que 1554 diziam respeito a burlas informáticas, incluindo 102 casos de "phishing", que se traduz nos piratas informáticos a fazerem o papel dos bancos para enganar os clientes e convence-los a dar os números de cartões de crédito e códigos secretos.

Dos 1554 inquéritos sobre crimes de burlas informáticas, dois terços (1015) foram arquivados por falta de provas. E durante o ano inteiro o Ministério Publico só conseguiu prosseguir com acusações em 49 dos casos.

7.2. Algumas soluções

Um **estudo da Universidade de Cambridge** revela que o combate ao cibercrime terá uma melhor abordagem quando os montantes gastos em policiamento e justiça penal global forem reforçados, assim como os que são gastos em tecnologias de segurança imperfeitas forem alterados.

Outro estudo com o nome "**Measuring the Cost of Cybercrime**" revela que as organizações investiram demasiado na defesa e limpeza de sistemas, com prejuízo nas retribuições custo do cibercrime que resulta de três cálculos: "*o custo directo das próprias fraudes (relativamente pequeno); o dinheiro gasto na defesa contra essas fraudes (muito maior) e os custos de limpar e recuperar os sistemas quando as defesas falham (também relativamente alto)"*.[98]

Estes estudos apontam que o Reino Unido e os Estados Unidos, países com uma forte resposta ao cibercrime, aplicam poucos recursos nos seus orçamentos que nas forças policiais atingem 12,3 milhões no Reino Unido e 79 milhões de dólares nos Estados Unidos. Se consideramos à escala mundial estima-se que atinja os 316, 2 mil milhões de dólares. Face a estes resultados concluiu-se que os países devem apostar menos na antecipação do cibercrime,

[98] Cf. Study "Measuring the Cost of Cybercrime"

que já se considerou ser de feito difícil, e apostar mais na resposta àquele, através da identificação dos infractores e da sua respectiva punição.

A **Comissão Europeia** propõe um plano de acção, para combater o cibercrime, baseado em cinco princípios:

⇒ Preparação e prevenção, recorrendo às equipas de Resposta de Emergência (CERTs - *Computer Emergency Response Teams*[99]) com o apoio da ENISA[100]

⇒ Detecção e resposta, desenvolvendo a *European Information and Alert System* (EISAS)

⇒ Mitigação e recuperação, através de simulações e de uma forte cooperação entre CERTs;

⇒ Cooperação internacional;

⇒ Estabelecer critérios para *European Critical Infrastructures* no sector das TIC (Tecnologias da Informação e Comunicação).

Trata-se de incrementar a informação, a consciencialização e a preparação, aumentando a literacia informática. A preparação e prevenção devem ser feitas tanto pelas empresas através da tomada de consciência do problema e da imprescindibilidade das medidas de segurança, como pela informação às potenciais vítimas do cibercrime. Outro apoio deverá ser prestado a nível tecnológico e financeiro à investigação e desenvolvimento na área da segurança e em medidas de protecção.

As técnicas de investigação e perseguição criminal de crimes cibernéticos têm de se apoiar noutras ciências. É imperioso que o investigador digital tenha um acompanhamento de especialistas na área, que dominem as redes e as técnicas, pois só assim poderá interceptar, interpretar e conservar apropriadamente os dados.

As entidades competentes para a investigação e repressão do cibercrime devem ter formação especializada na área, ficando dotados de conhecimentos científicos, técnicos e forenses na área. O apoio financeiro a estas estruturas torna-se crucial ao seu bom desempenho e forma de investigação.

[99] A nível nacional a FCCN (Fundação para a Computação Científica Nacional), através do seu serviço CERT.PT

[100] Agência Europeia para a Segurança das Redes e da Informação visa o reforço das capacidades da EU, dos Estados-membros e do sector das empresas no que diz respeito à prevenção, resposta, assistência, aconselhamento e gestão de problemas ligados à segurança das redes e da informação.

Deve ser tirado proveito dos instrumentos legislativos internacionais existentes neste domínio, pois as legislações nacionais de cada Estado estão cada vez mais próximas, devendo a investigação passar sempre por uma opção que vá de encontro às disposições materiais e processuais do cibercrime, regendo-se por uma cooperação internacional que promova a troca de informação e conhecimento no seio de uma investigação, nomeadamente através de uma rede internacional que possibilite tais contactos.

Em **Portugal**, numa formação sobre cibercriminalidade, realizada em 2011, ministrada por serviços de informação americanos[101] para agentes portugueses[102], a Directora do DIAP, Maria José Morgado, defendeu que deve existir um reforço da segurança contra a criminalidade informática e que este matéria tem que ser uma prioridade política. Foi uma formação de extrema importância dada a desproporção existente no seio do nosso sistema entre os meios disponíveis e as verdadeiras ameaças derivadas da cibercriminalidade. Foi reafirmado o bom nível de preparação das autoridades portuguesas, contudo a atribuição de meios proporcionados a uma investigação criminal não se têm revelado suficientes, pelo que uma das formas de combater eficazmente esta realidade passa por uma maior aposta nos recursos. Mais uma vez a Directora do DIAP reforçou a ideia de que as autoridades portuguesas devem partilhar informação e experiencias com outras entidades que tenham tanto ou mais conhecimento e formação, pois só assim se pode estar em constante evolução e actualização. A cooperação internacional torna-se imprescindível para este tipo de criminalidade.

Ao dar prioridade a este tema, combate-se inúmeras formas de crimes que já se praticavam, mas que agora se praticam através de outros meios inseridos no cibercrime, como por exemplo o branqueamento de capitais, pornografia infantil e burlas informáticas.

Atendendo aos ataques de que o país foi alvo nos últimos 2/3 anos e pelo facto dos recursos disponibilizados para os combater e investigar serem escassos, concluiu-se que o combate tem que ser feito em tempo real e de forma eficaz e só com a nova perspectiva apresentada pode trazer resultados.

Foi criado pelo Governo em 2012 uma Comissão Instaladora do Centro Nacional de Cibersegurança com a missão de "definir as medidas e os instrumentos necessários à criação, instalação e operacionalização em Portugal" desse organismo.

A sua criação inseriu-se no âmbito da Estratégia Nacional de Segurança da Informação, e do Grupo de Projecto para as Tecnologias de Informação e Comunicação na

[101]ICE - ImmigrationCustomsEnforcement - HomelandSecurity,
[102] GNR, PSP, PJ, SEF, Magistrados do MP e elementos do DIAP

Administração Pública. Teve como principal objectivo criar um centro de Cibersegurança e uma estratégia nacional para combater o cribercrime.

No relatório anual de segurança interna, relativo a 2011, o Gabinete do Secretário-Geral do Sistema de Segurança Interna, aponta que nos crimes registados em 2011, nota-se entre as subidas mais significativas a burla informática e nas comunicações, com mais 580 casos registados (aumento de 27,4% relativamente a 2010). Com este relatório sentiu-se a necessidade de reforçar os dispositivos de segurança, designadamente através de um plano estratégico nacional e da criação do dito centro nacional de cibersegurança.

7.3. Gabinete do Cibercrime

O Gabinete do Cibercrime tem como principais objectivos a coordenação, formação de magistrados do MP, interacção entre os órgãos de polícia criminal e privados e acompanhamento de alguns processos.

O entendimento sobre a LC e da obtenção de prova em suporte digital, tem suscitado algumas divergências entre os magistrados do MP o que muitas vezes conduz a soluções diferentes. Face a esta realidade, o Gabinete do Cibercrime pretende harmonizar estes entendimentos e permitir que os mesmos factos considerados penalmente relevantes sejam enquadrados juridicamente da mesma forma pelo MP, assim como permitir que a obtenção de prova em suporte digital seja efectuada de modo coordenado.

A formação dos magistrados é, também, realizada pelo Centro de Estudos Judiciários (CEJ), contudo o Gabinete está mais vocacionado para os magistrados do MP com uma vertente mais técnica e prática.

Com a LC, no decurso de uma investigação criminal, é possível recorrer a obtenção de provas em suporte digital. Ora, estas diligências exigem uma cooperação efectiva por parte de entidades privadas, nomeadamente, dos fornecedores de serviço, pois são os portadores de informações importantes e imprescindíveis para a descoberta da verdade. Esta inovação trazida pela LC vem afastar as hipóteses em que anteriormente era proibido aceder a algumas destas informações por via do sigilo sobre as telecomunicações. Face a esta nova possibilidade trazida pela LC, sentiu-se a necessidade de criar um elo de ligação entre as autoridades e as entidades privadas, pelo que o Gabinete tem o intuito de estabelecer contactos entres estas, de forma a assegurar uma colaboração eficaz através de meios de

comunicação expeditos, para que sempre que seja necessário, existir uma rápida e pronta resposta às solicitações efectuadas pelas autoridades.

Até 2009, existia na PJ, uma unidade nacional onde se centralizava toda a investigação da cibercriminalidade, todavia hoje em dia este tipo de investigação está distribuída por diferentes departamentos da PJ, sendo que até em muitos casos e quando não seja da sua competência especifica, é delegada em outros órgãos de policia criminal.

Atendendo a estes novos mecanismos de interacção entre o MP e órgãos de polícia criminal e entre estes e entidades privadas, o Gabinete desenvolveu canais e rotinas específicas para os processos de cibercrime, promovendo o relacionamento de todos na realização das diligências de inquérito.

Conclusão

As evoluções constantes nas tecnologias de informação tiveram um impacto notável na sociedade. Hoje em dia, é raro o sector da sociedade que não está abrangido por estas, tendo vindo a conferir novas mudanças nas actividades desenvolvidas pelo Homem.

Uma das evoluções mais polémicas que operou nas tecnologias de informação foi sem dúvida na área da tecnologia das telecomunicações. Os modelos clássicos simples de comunicação, como os meios telefónicos, foram substituídos por outros que comportam inúmeras quantidades de dados, como a voz, imagem, som e texto. Para tal, basta que os dados sejam introduzidos numa rede com um endereço de destino ou que sejam disponibilizados a quem desejar aceder-lhes. Podemos tomar como exemplo o correio electrónico, fonte utilizada cada vez mais no mundo actual para a comunicação entre as pessoas, ou mesmo os inúmeros sites da Internet que disponibilizam grandes quantidades de informação, acessível a qualquer um. O aparecimento destes sistemas de telecomunicação permitiu, independentemente da distância, o armazenamento e a transmissão de todos os tipos de dados. Criou-se uma espécie de espaço comum, designado de ciberespaço.

É claro que estes desenvolvimentos originaram diversas mudanças a nível social, mas também a nível económico. Transformaram a sociedade em todas as suas vertentes, possibilitando, como se referiu a acessibilidade a informação do mais variado nível, permitindo, também alargar os horizontes do conhecimento.

Estas evoluções nas tecnologias da informação, não trouxeram apenas aspectos positivos. De notar que a comunicação, troca de informação e conhecimento de forma mais facilitada e simples, permitiu também que surgissem aspectos negativos associados a estas evoluções. O aparecimento de novos tipos de crime associados às novas tecnologias, como a prática de crimes clássicos através de novos meios trouxeram graves consequências. Os autores dos crimes encontram-se muitas vezes em locais diferentes onde estes produzem efeitos, dificultando a sua localização. O carácter transfronteiriço destas infracções entra em conflito com a territorialidade das autoridades nacionais competentes para a aplicação da lei. As legislações nacionais estão confinadas a um território delimitado, pelo que se torna cada vez mais importante que exista legislação internacional que posso tutelar estes crimes.

Tornou-se necessário aplicar medidas de carácter técnico conjuntamente com medidas jurídicas a fim de evitar e deter a prática de crimes.

Surgiram assim instrumentos legislativos internacionais com o objectivo de harmonizar as legislações nacionais para combater eficazmente o cibercrime. Ficou demonstrado que fazer face a este fenómeno não é fácil e apenas se consegue com uma cooperação internacional das entidades que investigam estes crimes, permitida pelas legislações nacionais, já harmonizadas e em consonância. Estas entidades devem ter formação nesta matéria e devem dispor de meios financeiros e técnicos que possibilitem um bom desenrolar da investigação. A nível interno tem que existir uma maior proximidade entre as entidades investigadoras e os prestadores de serviços, estabelecendo protocolos de cooperação de forma a facilitar a identificação do infractor. A prevenção do cibercrime deve, também, passar pela formação e instrução das pessoas no geral, alertando para as práticas ilícitas existentes na internet, assim como a existência de meios de defesa que podem possibilitar uma prevenção mais adequada.

O Cibercrime nunca irá desaparecer, mas pode ser prevenido e combatido se a sociedade for instruída neste sentido.

Bibliografia

Fontes:

Internacionais

- Convenção sobre o Cibercrime adoptada em Budapeste em 23 de Novembro de 2001

- Decisão-Quadro2005/222/JAI do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação

- Protocolo adicional à Convenção sobre o Cibercrime relativo à incriminação de actos de natureza racista e xenófoba praticados através de sistemas informáticos, adoptada em Estrasburgo em 28 de Janeiro de 2003

Nacionais

- Lei nº 109/2009 de 15 de setembro
- Lei nº 32/2008, de 17 de julho
- Lei nº 5/2004, de 10 de fevereiro
- Decreto-Lei nº 176/2007, de 8 de maio
- Lei nº 7/2004, de 7 de Janeiro
- Lei nº 41/2004,de 18 de Agosto
- Lei nº 67/98,de 26 de outubro
- Lei nº 38/2009; 2009-2011 - lei quadro da policia criminal
- Parecer nº 11/2011 da PGR
- Estatuto do MP Art. 12 nº2 b) e art. 42 nº1
- Resolução da AR 88/2009
- Decreto do PR nº 91/2009 de 15 de Setembro
- Resolução AR 91/2009
- Despacho da PGR de 7 de Dezembro de 2011
- Despacho nº12/2012 PGR, 25 de Setembro de 2012

Livros e artigos

I Curso Pós-Graduação de Aperfeiçoamento em Direito da Investigação Criminal e da Prova – A Problemática da Investigação do Cibercrime, Faculdade de Direito, Universidade de Lisboa

CEJ – Jornadas sobre Código Penal, Conferência 27.09.07, Responsabilidade das Pessoas Colectivas, Germano Marques da Silva

Ascensão, José Oliveira, Direito da Internet e Sociedade de Informação, Editora Forense, 2002

Casabona, Carlos, El Cibercrimen Nuevos Retos J-P, Nuevas Resprestas Politico-Criminales, Editorial Camares

Costa, Luciana Oliveira, Internet, Privacidade e Dados Pessoais, Universidade de Lisboa, Faculdade de Direito, 2006

Colóquio "A partilha de ficheiros na internet e o direito de autor", PGR 18 de Janeiro de 2013, Gabinete do Cibercrime

Courrier Internacional, "A Hora do Hacktivismo", Janeiro de 2012

De Melo Bandeira, Gonçalo Serpa, Responsabilidade Penal Económica e Fiscal dos Entes Colectivos

Dias, Figueiredo, Direito Penal, Universidade de Coimbra, 1977

Fachana João, Responsabilidade Civil pelos conteúdos ilícitos colocados e difundidos na Internet, Almedina, 2012

Garcia Marques e Lourenço Martins, Direito da Informática, 2ª Ed. Refundida e Actualizada, Almedina, 2006

Gomes, Paulo Jorge, A Partilha de Ficheiros na Internet e o Direito de Autor, Instituto Açoriano da Cultura, 2011

Instituto Jurídico da Comunicação, As Telecomunicações e o Direito na Sociedade de Informação, Faculdade de Direito, Universidade de Coimbra, 1999

Jornal Expresso, de 9 de Fevereiro de 2013, rubrica "Sociedade Justiça"

Mendes, Paulo Sousa, A Responsabilidade das Pessoas Colectivas no âmbito da Criminalidade Informática em Portugal

Ministério Público Federal e Comité Gestor da internet no Brasil, Crimes Cibernéticos, manual prático de investigação, partilha segurança para a internet, 2006

Neves, Rita Castanheira, As Ingerencias nas Comunicações Electrónicas em Processo Penal; Natureza e Respectivo Regime Jurídico do Correio Electrónico enquanto Meio de Obtenção de Prova, Coimbra, 2011

Nota Prática nº1/2012, "O endereço de IP e a identificação do seu utilizador", Gabinete do Cibercrime

Oliveira, Marcel Lionardi, Responsabilidade Civil dos Provedores de Serviços de Internet, Editora Juarez, 2005

Paulo Pinto de Albuquerque e José Branco, Comentário das Leis Penais Extravagantes, Volume I, Universidade Católica Editora

Pereira, Alexandre Libório Dias, Comércio Electrónico na Sociedade da Informação: Da Segurança Técnica à Confiança Jurídica, Almedina, 1999

Pedro Verdelho, Rogério Bravo e Manuel Rocha, Leis do Cibercrime, Volume I, Centro Atlântico, 2003

Quelhas, Filipe, O advento da Responsabilidade Penal das Pessoas Colectivas no Direito Penal de Justiça à Luz da Reforma do Artigo 11 do CP em Portugal, Faculdade de Direito, Universidade de Lisboa, 2008

Rodrigues, Benjamim Silva, Direito Penal, Parte Especial, Tomo I, Direito Penal Informático Digital, Coimbra Editora, 2009

Teixeira, Filipe Canaberro, Da Responsabilidade Civil dos Provedores de Serviços de Internet, Faculdade de Direito, Universidade de Lisboa, 2007

Venâncio, Pedro Dias, Lei do Cibercrime Anotada e Comentada, Coimbra Editora, 1ªed., 2011

Links internet:

- http:// cibercrime.pgr.pt / outroslinks/ outroslinks.html (Gabinete cibercrime pt)
- www. coe. int/t /dghl /cooperation /economiccrime/ cybercrime/ tcy/ default_tcy_en.asp (Comité Convenção Cibercrime do Conselho da Europa)
- http:// www. coe. int/t/dghl /cooperation /economiccrime/ cybercrime/ tcy/ default_tcy_en.asp (Plano Global sobre Cibercrime Conselho Europa
- eurojust. europa.eu/ pages/ home. aspx

- www.mp.mg.gov.br / portal/ public / interno / index / id/ 10 (MP Brasil (Minas Gerais))
- www. prsp.mpt.gov.br / noticias-prsp / crimes-ciberneticos (MP Brasil (São Paulo))
- www. justice. gov/ criminal / cybercrime/ (USA Department of Justice)
- www. fiscal. es /as (Espanha MP)
- *www. portaltic. com/ 84- alcyon-junior/ 200-cibercrime-o-que-deve-vir-primeiro-lei civil-ou-lei-penal.html*
- *www. quantanoticia.com.br/ site / index. php/ en / template / tecnologia/ item/ 2111-lei-do-cibercrime-texto-não-contempla-doud-computing-diz-especialista*
- *itweb.com.br*
- *www. advocatus.pt/ opiniao/ 4060-os-efeitos-do-cibercrime*
- www. computerworld. com. pt
- gavgavka.co
- http:// tek. sapo.pt / noticias/ computadores/ centro_europeu_contra_o_cibercrime_comeca_a_f_1292608.html.
- http://tek.sapo.pt/notticias/internet/mais_de_metade_dos_portugueses_tem_ medo_de_us_1255842 html
- http:// segurancaecienciasforenses. wordpress.com/ 2012/11/13/dados-de-trafego cibercrime
- http:// www.gddc.pt/siii/im.asp?id=2083 (Gabinete de documentação e direito comparado)
- http://cibercrime.pgr.pt/
- http://sol.sapo.pt/inicio/Tecnologia/Interior.aspx?content_id=43001
- http://www.verbojuridico.com/doutrina/penal/0.html
- http://www.dgsi.pt