I – INTRODUÇÃO

Na constante evolução técnica da sociedade hodierna amplamente dominada pelas tecnologias da informação e da comunicação (TIC), encontram-se a informática, em geral, e a internet, em particular, onde têm vindo a ocupar, progressivamente, um espaço cada vez mais importante na vida do Homem. As TIC encontram-se em todo o lado, desde o controlo de abastecimento de redes elétricas e hídricas aos transportes aéreos, sendo até utilizadas pelos serviços de identificação civil. É indiscutível que os computadores e a Internet fazem parte integrante da vida do homem, estando o seu dia-a-dia cada vez mais dependente desta tecnologia e da sua correta utilização e funcionamento.

A informática e a internet, quando utilizadas em simultâneo são, presentemente, meios que permitem viajar sem nos deslocarmos do mesmo local físico, pois de uma forma sem precedentes, e em conjugação com os avanços tecnológicos, ao nível das redes de comunicação, eliminam, ainda que de uma forma virtual, todas as fronteiras transnacionais, concedendo também a grande parte da população mundial que as utilizam, a possibilidade de estar informada, em tempo real, sobre praticamente tudo o que acontece no planeta. Sobre isso, citemos Castells quando refere que os "novos usos da tecnologia, assim como as modificações efectuadas nessa tecnologia, são transmitidos de regresso ao mundo inteiro, em tempo real" (Castells, 2007, p.46).

Esta corrida, ao conhecimento e à informação, é, atualmente, mais do que um lazer, é encarada como fundamental na atual sociedade, na medida em que a competitividade comercial assim o exige, sendo que as tecnologias de informação fazem parte integrante de um mundo cada vez mais globalizado, pelo que não se pode ignorar que "estruturam as economias mundiais tornando-as cada vez mais comunicantes, convergentes, interdependentes e competitivas" (Santos, Bessa & Pimentel, 2008, p.1). Pierre Levy refere que, em termos evolutivos, os "meios de comunicação interactivos, as comunidades virtuais sem território e a explosão da liberdade de expressão, permitida pela

Internet, abrem um novo espaço de comunicação, transparente e universal (…)" (Levy, 2002, p. 11). A Internet acrescentou uma nova forma de comunicar, pois doravante, esta ferramenta confere a qualquer cidadão a possibilidade de interagir de uma forma sem precedente.

No entanto, o surgimento e a utilização das novas tecnologias, não trouxe só vantagens. Venâncio (2011) refere que "as práticas e capacidades da informática, e em particular da Internet, potenciam exponencialmente a internacionalização da criminalidade" (Venâncio, 2011, p.15). Também em França, o Decano Jean Carbonnier afirmou, em tempos que, "*L'évolution des mœurs et des techniques donne matière à de nouvelles forme de délinquance*[1]" (Pansier e Jez, 2000, p. 6). Na prática, essa criminalidade é quase sempre cometida no ciberespaço[2] e só consegue ser praticada através da utilização das redes de comunicação, a partir de computadores, ou ainda contra estes. Venâncio salienta que, "as especificidades da criminalidade informática colocam-se, não só na transferência de comportamentos ilícitos para o ambiente digital, como na tipificação de novos crimes com elementos caracterizadores de natura digital" (Venâncio, 2011, p. 15).

Com o crescimento universal desta ameaça, tem sido visível o esforço dos responsáveis europeus para a consolidação de uma legislação comum a todos os países, que se quer capaz de travar a evolução do cibercrime. Perante um tipo de criminalidade, cada vez mais mediatizado, e face a "uma sociedade em que grande parte das trocas de informação ocorre por meios eletrónicos deverá preocupar-se com a implementação de técnicas e meios de transmissão seguros dessa mesma informação" (Martins, 2004, p. 69).

A elaboração deste estudo pretende afastar-se de quaisquer outros que, apesar de toda a sua importância e pertinência, diferem daquilo a que nos

(1) *"A evolução das condutas sociais e da técnica dão forma a novos tipos de delinquência".*
(2) A palavra ciberespaço foi introduzida pela primeira vez na obra de ficção científica Neuromencer, pelo autor William Gibson e destinava-se a descrever o ambiente onde os *hackers* operavam (Chawki, 2005).

propusemos estudar, ou seja, o de caracterizar, de uma forma global, as trajetórias do cibercrime em Portugal, e no final poder perspetivar o futuro deste fenómeno criminal, sem para isso aspirar a qualquer tipo de futurologia. Para atingir os objetivos fixados para a realização deste trabalho, desenvolveu-se um estudo, essencialmente, de caráter reflexivo, sendo que a pesquisa a realizar deve revelar informações "que não tenham já sido ditas ou rever com uma óptica diferente coisas que já foram ditas" (Eco, 1997, p. 53). Tornou-se assim, pertinente abordar, mesmo que de uma forma superficial, a legislação existente sobre a matéria, dando-se mais ênfase àquela que se encontrava na data, em vigor, sem contudo ter sido posta de parte a que outrora vigeu, e que direta ou indiretamente contribuiu para a evolução no combate ao cibercrime. Apesar de não se considerar este trabalho como sendo uma análise, à luz do direito penal, não podem ser excluídas, as legislações criadas, e que penalizam este fenómeno criminal.

II – ENQUADRAMENTO GERAL

Tema e Objetivos da Investigação

A utilização da Internet e da informática aumenta diariamente, e a "rede informática mundial apresenta-se como o instrumento indispensável para o controlo das acções necessárias à mundialização. Com a criação da *World Wide Web*, existem hoje mais de 800 milhões de consumidores de Internet" (Fontanel, 2008, p.41). Este aumento referido por Fontanel deve-se à facilidade de acesso às tecnologias da informação e comunicação que segundo Santos, Bessa e Pimentel (2008) se encontra associada a uma redução de preços dos equipamentos informáticos e dos custos do acesso à rede internet. Tudo isto faz com que o número de utilizadores do computador bem como dos acessos domésticos à Internet aumente, permitindo aos particulares aceder a esse serviço. Em consequência, verifica-se um aumento significativo do tráfego no ciberespaço e ainda a probabilidade dos cibernautas se tornarem potenciais

vítimas do cibercrime. Santos, Bessa e Pimentel, referem que o ciberespaço é um mundo virtual, onde a presença física é desnecessária para a realização de qualquer ação criminal (2008), tratando-se de um ambiente cada vez mais utilizado nas atividades das organizações do crime organizado.

As ações cometidas através da Internet são, muitas vezes, noticiadas nos meios de comunicação social, levando a que a imagem transmitida à opinião pública seja a de que a Internet e a informática não possam oferecer garantias de segurança. Essas convicções apoiam-se também no crescente número de incidências criminais que se têm verificado no ciberespaço. Prevalece a ideia de que é um local desprovido de segurança, onde a privacidade de cada indivíduo está, permanentemente, em risco de ser violada. É importante relembrar que a máquina, por si só, não representa nenhuma ameaça real, sendo sempre necessária a intervenção do homem para pôr em prática qualquer forma de ilícito criminal. Como muitas outras invenções do Homem, as novas tecnologias não trazem somente benefícios aos seus utilizadores, pois o risco de as utilizarem em práticas criminais estará sempre presente.

Não existe consenso entre os estudiosos quando se trata de definir o cibercrime. Em 2003, não havia em Portugal "nenhum texto legal que consagre a expressão cibercrime (…)", nem existia nessa altura "nenhum dispositivo legal que use, refira ou defina esta expressão" (Verdelho, 2003, p. 347 *in* Direito da Sociedade de Informação Volume IV). Não há um conceito definido para o termo cibercrime, todavia quando se fala em criminalidade informática, a mesma tem sido encarada como sendo "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 do crime" (Venâncio citando, Garcia Marques & Lourenço Martins, 2011, p.16). Com a entrada em vigor da LC, essa consagração encontra-se, presentemente, mencionada na legislação portuguesa. Contudo, a expressão cibercrime continua sem definição concreta, não tendo sido encontrada qualquer referência específica na lei portuguesa que a defina. Ora, é da opinião de Majid

Yar que "*a major problem for the study of cybercrime is the absence of a consistent current definition (…)*" (Yar, 2006, p. 9). Porém, verificou-se a existência de uma definição amplamente aceite na Europa sobre o termo cibercrime, e que partiu de uma comunicação da Comissão Europeia "*Toward a General Policy on the Fight Against Cybercrime*". Essa definição qualifica o cibercrime como quaisquer "violações criminais cometidas por meio de redes de comunicação eletrónica e sistemas de informações ou contra tais redes e sistemas[3]", fazendo ainda uma categorização do cibercrime em três categorias criminais:

- a primeira que abrange as formas tradicionais de criminalidade, como por exemplo a fraude e a falsificação; a segunda onde se encontra inserida a publicação de conteúdos ilícitos em meios de comunicação electrónicos, tais como a pornografia infantil ou o incitamento ao ódio racial e a terceira categoria que diz respeito aos crimes eletrónicos propriamente ditos, tais como os ataques aos sistemas de informação, bloqueios de serviços ou até pirataria. Esta especificidade própria do cibercrime requer que os investigadores criminais possuam uma formação cada vez mais especializada nesta área criminal.

Um outro fator importante e a ter em consideração no cibercrime é o "facto das comunicações se processarem a nível planetário entre uma rede infindável de computadores, em que se considera faltar o elemento territorialidade para se poder impor o direito nacional" (Santos *et al.*, 2008, p. 5). A falta desse elemento, tem sido encarada como uma problemática no sentido em que a investigação criminal deste fenómeno torna-se mais difícil, ou até impossível, devido a essa limitação.

Costa Andrade & Figueiredo Dias (1997) referem que, para se classificar um determinado comportamento como crime, é necessário a presença de dois critérios que os possa classificar como tal. O primeiro, que o ato seja

([3])Disponível na WWW:
<URL: http://www.mcafee.com/br/resources/white-papers/wp-cybercrime-hactivism.pdf >.

socialmente danoso, e o segundo, que as suas sanções já se encontrem previstas. Não há duvida de que o cibercrime é um ato socialmente danoso cujas sanções já se encontram previstas. Como tal, e conforme a delimitação legal de todos os comportamentos ilícitos, o cibercrime foi alvo da aplicabilidade do direito penal material, e do direito processual, estando tipificado na atual Lei do Cibercrime (LC).

A amplitude globalizada alcançada pelo cibercrime e os estragos que este pode provocar, a nível económico, securitário e privado, faz com que esse combate não dependa, somente, dos atores judiciários, devendo contemplar também os atores não judiciários. Nesse sentido, Mata e Martín referem que "*La lucha frente a la criminalidade informática desborda naturalmente el campo exclusivo del Derecho penal, pues se trata de un fenómeno cuyo control reclama además otros instrumentos más amplios y complejos (de tipo jurídico – no penal -, de tipo técnico, formativo, así como educativo)*" (Mata & Martín, 2004, p. 199).

Na verdade, o cibercrime confere nos delatores um constante sentimento de impunidade, e as normas e regulamentações criadas para reprimir esses comportamentos, não parecem impedi-los de os praticar. Para além, de se sentirem protegidos pela facilidade com que os meios informáticos lhes podem potenciar a faculdade em ocultarem a sua identidade no ciberespaço, os atos ilícitos praticados dessa forma, permitem que os seus alvos sejam quase instantaneamente atingidos, a partir de um determinado lugar e para qualquer parte do mundo. Aliás, é talvez por isso, que "o internauta sente uma ausência de controlo ao nível social, da acção reguladora das instâncias formais e informais de combate ao crime, bem como uma inexistência dos complexos sociais de rotulação e de estigmatização" (Santos, *et al*., 2008, p. 5). Já Guedes Valente referiu que, o "actor do crime sente-se seguro e, não sendo investigado, descoberto e punido, não desiste de uma prática que lhe permite usufruir de bens avultados (…)" (Valente, 2009, p.499).

É frequente o facto das próprias vítimas do cibercrime não tomarem consciência de que já o foram, ao invés da criminalidade praticada fora do ciberespaço, como por exemplo, os roubos ou as agressões, onde as vítimas têm contacto com o criminoso. Ali El Azzouzi (2009) refere que "no mundo real, determinadas situações externas podem fazer com que a prática de um crime possa ser abortada pelo seu autor. O fator psicológico pode desencorajar o criminoso, e obrigá-lo a desistir dos seus intentos. Pelo contrário, a particularidade do mundo virtual permite agir sem o contato direto com a vítima e o meio que a rodeia, tornando-se por isso uma grande vantagem para os cibercriminosos" (Azzouzi, 2010, p. 20). A possibilidade das vítimas de cibercrime não atribuírem grande importância à cibercriminalidade ou ainda por acreditarem ser impossível identificar e punir os seus autores, pode ser um dos motivos pelo qual não apresentem queixa junto das autoridades. Pedro Verdelho refere que a "polícia e os tribunais nunca chegam a saber da sua existência. Os danos e os prejuízos sofridos pelas vítimas ficam por reparar e os respectivos responsáveis ficam por castigar. Supõe-se que os cibercrimes sejam uma grande fatia no conjunto dos crimes ocultos. Não há estatísticas nem estimativas rigorosas para as *cifras negras* no cibercrime" (Verdelho, 2003, p. 351 *in* Direito da Sociedade de Informação Volume IV).

Chegados aqui, importa referir novamente, que este estudo seguiu a evolução do cibercrime em Portugal, pelo que julgou-se relevante ir ao encontro da opinião de alguns especialistas nesta matéria. Todos eles oriundos de áreas científicas distintas, e cuja intenção é a de, junto dos mesmos, recolher determinadas informações relacionadas com a atual LC. Esperamos pois, que a informação obtida possa contribuir para uma melhor compreensão do fenómeno em estudo, e a forma como essa lei tem ou não contribuído para a luta contra o cibercrime. Este é um dos fatores que acreditou-se ser primordial para a realização deste estudo. Realça-se contudo, o facto, das opiniões transmitidas não serem consideradas representativas da generalidade da classe científica ou profissional, onde se encontram inseridos os três

entrevistados. Esperemos porém, que a arte recolhida possa servir de base de apoio nas reflexões que se pretendem fazer, ao longo da investigação.

Como focado anteriormente, é neste contexto exploratório e reflexivo que pretendemos levar a cabo este nosso estudo, de forma a abordar o cibercrime em Portugal, seguir as suas trajetórias, e poder traçar as perspetivas de futuro para o fenómeno em questão.

Estrutura da Investigação

A repartição estrutural do presente estudo efetua-se em cinco capítulos distintos:

- O **capítulo I**, que corresponde à introdução, onde é realizada uma descrição da natureza e do âmbito do estudo a realizar;

- O **capítulo II**, que trata de todo o enquadramento geral do estudo, focando-se neste, a caracterização do tema e os objetivos da investigação, bem como uma abordagem ao Estado da Arte;

O **capítulo III**, que aborda a metodologia de investigação utilizada para a elaboração do presente estudo, bem como os procedimentos encetados na preparação e execução das entrevistas e dos inquéritos, contemplando ainda o tratamento de todos os dados recolhidos;

- O **capítulo IV**, que caracteriza-se pela análise empírica, não só no que concerne às trajetórias do objeto de estudo, mas também pela importância que a Internet representa, como palco principal para a prática dos ilícitos e, que por consequente, se encontra interligada ao fenómeno do cibercrime em Portugal;

- O **capítulo V** que caracteriza-se, pela análise das questões de investigação, pela exposição fundamentada das perspetivas de futuro para o cibercrime em

Portugal e, finalmente, pela formulação das considerações finais do estudo efetuado.

O Estado da Arte

Antes de podermos apontar as trajetórias do cibercrime em Portugal, considerou-se importante debruçarmo-nos sobre a obra até aqui realizada, e como era de esperar, verificou-se a existência de uma vasta riqueza científica, que gira em torno do fenómeno do cibercrime. Nessa medida, achou-se essencial realizar uma seleção rigorosa de alguma arte já existente, para nos podermos focar naquela que, mais particularmente, vai ao encontro, do que se pretende alcançar com a realização deste estudo. Feita essa seleção, pretendemos abranger, de uma forma sucinta, sem que para tal se ponha de parte o rigor necessário, o fenómeno a que nos propusemos estudar. Faremos, inicialmente, uma breve alusão à noção de crime e ao papel da criminologia, antes de abordarmos o cibercrime propriamente dito.

A criminologia é, pois, uma ciência que "pretende conhecer a realidade criminal, através da observação e da experimentação. Propõe-se descrever e explicar os comportamentos dos actores sociais (…)". O criminólogo "não despreza nenhum método, nenhum instrumento das ciências sociais: questionário, inquérito, análises de estatísticas administrativas, censos, etc. (Cusson, 2002, p. 27). A noção de crime diverge na sua perspetiva, consoante a definição que lhe é dada, seja ela feita por juristas, psicólogos, sociólogos ou criminólogos. A título de exemplo, os criminólogos "utilizam mais ou menos indistintamente os termos crime, delito, delinquência e infracção embora prefiram o primeiro para designar factos graves (Cusson, 2002, p. 14)". Já Émile Durkheim (1895) definiu o crime "como aquilo que é sancionado por uma pena" (Robert, 2005, p.25). Quanto à definição jurídico-legal de crime, Machado "define-o como todo o comportamento – e só esse – que a lei tipifica como tal (…)". Machado faz alusão à possibilidade de identificar três elementos básicos na definição de crime: "(1) os danos que remetem para a natureza,

dimensão e severidade dos prejuízos e males causados, e que tipo de vítimas foram atingidas; (2) o consenso social sobre os impactos criados pela ocorrência do crime; (3) as respostas oficiais, que implicam a existência de legislação criminal que especifica as circunstâncias em que um acto danoso pode ser classificado como crime e quais as sanções a dirigir a quem o cometeu" (Machado, 2008, p. 29). Já Verdelho (2003) refere que a realidade legal e socio criminal permitem dividir as diferentes formas de cibercrime em três grupos distintos: o primeiro onde estão englobados os crimes que recorrem a meios informáticos; o segundo relacionado com os crimes referentes à proteção de dados pessoais e o terceiro que inclui os crimes informáticos propriamente ditos.

O cibercrime encontra-se associado à utilização de novas tecnologias, pelo que a forma como é cometido, difere em modo e lugar, da restante criminalidade convencional. Nesta perspetiva, um estudo realizado sobre a cibercriminalidade concluiu que o cibercrime "*differ from terrestrial crimes in four ways: They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal* [4]*".* Acredita-se que, o facto de nem sempre serem claramente ilegais, prende-se com a falta de territorialidade anteriormente referida.

Apesar de todos falarem nesta nova forma de criminalidade, o criminólogo francês Alain Bauer afirma que não há cibercrime. Na sua opinião, o que se verifica é uma associação "da velha escroqueria e da nova tecnologia. Roubar números de cartão de crédito ou papéis de identificação, tudo isto é tão velho como o crime. O que temos aqui é, portanto, o bom velho crime mais a nova tecnologia, (…) o cibercrime ainda está para vir, ainda está à nossa frente[5]".

([4]) *In Cyber crime…and Punishment? Archaic laws Threaten Global Information,* December 2000, McConnell Internacional, p.1.
([5]) Bauer, A. (2012). *O cibercrime ainda está para vir.*
Disponível na WWW:
<URL:http://inteligenciaeconomica.com.pt/?p=11431>.

Para Xavier Raufer (2009), a informática alcançou uma dimensão planetária, atingindo milhares de seres humanos. Raufer utiliza dois termos como forma de descrever o mundo da informática e apelida-os de "*maladies de la société dite de l´information*: a *monochromie* et *flux-tendu*[6]" (Raufer, 2009, p. 79). Segundo o autor, esta forma de patologias apelidadas também de defeitos estruturais, ameaçam toda uma infraestrutura tecnológica, da qual faz parte integrante a informática, pelo que esses defeitos devem ser identificados e corrigidos antes que contaminem, por sua vez, toda a sociedade.

A cibercriminalidade tornou-se "uma atividade onde a rentabilidade é elevada, organizada, fácil de pôr em prática e com riscos muito reduzidos" (Azouzzi, 2009, p41). Cada vez mais, são detetadas no mundo, atividades criminosas praticadas através das novas tecnologias, por *gangs* ou grupos organizados de indivíduos, associados entre si, para praticarem todo o tipo de delitos. Desde o tráfico de droga, ao branqueamento de capitais, esta nova forma utilizada para praticar crimes faz com que o crime organizado[7] procure recrutar cibercriminosos com grandes conhecimentos técnicos (Le Doran & Rosé, 1998). Braz (2010) refere também que "o crime organizado transnacionalizou-se, aproveitando com sagacidade as facilidades de comunicação existentes no mundo informacional (comunicação electrónica instantânea e rápida deslocação de pessoas entre países e continentes), (…) com auxílio de estruturas opacas, fechadas, servidas por sofisticados meios tecnológicos que favorecem a rapidez, a eficácia e o anonimato" (Braz, 2010, p. 331). Santos,

(6) "***Monochromie***. A sociedade da informação converge em direção a um mundo mais interligado e uniformizado. Em informática e comunicações a impermeabilidade e heterogeneidade dos sistemas desempenharão um papel cada vez menos protetor. Este mundo plano e monocromático torna-se vulnerável a cada agressão fortuita ou premeditada, com possíveis efeitos de dominós a caírem em cascata, atendendo a que as infraestruturas funcionam cada vez mais em simbiose".
"***Flux tendu***. A evolução introduz mudanças técnicas, comportamentais e organizacionais (até psicológicas, como evidenciado pela nossa dependência crescente nas tecnologias da comunicação). A nossa civilização torna-se a da espontaneidade e do contacto. As empresas querem-se ágeis com ciclos decisórios curtos, repetitivos e que se aprovisionam a *flux-tendu*. Mas a segurança a *flux-tendu* (atualização de software, antivírus…) face às crescentes ameaças será sempre mais aleatória*".(Flux tendu:* Encaminhamento regular, em tempo útil, de produtos destinados a serem vendidos de imediato, sem que haja armazenamento)
(7) Crime organizado: qualquer associação ou qualquer grupo de indivíduos que se entregam a uma atividade ilícita contínua, onde o objetivo primeiro é obter benefícios, esquecendo as fronteiras nacionais. (Interpol)

Bessa e Pimentel referem que "nos últimos anos houve um aumento significativo da sofisticação por parte das organizações colombianas no tráfico de droga (…). Estas organizações contratam, cada vez mais, especialistas com conhecimentos na área financeira e na área das redes informáticas, tendo em vista conduzir, através da Internet, transacções de lavagem de dinheiro, explorando as vulnerabilidades dos vários tipos de sistemas de informação (…)" (Santos, *et al*, 2008, p. 6).

A tecnologia militar está, também ela, cada vez mais dependente do fluxo de informações veiculadas através da Internet. Luís Sousa Cardoso refere que "as consequências dos ataques no ciberespaço podem ser muito grandes, tais como a falta de energia em áreas vitais, falhas nas comunicações criando áreas isoladas, invasão de redes militares, espionagem, e podem afectar um maior número de pessoas do que o terrorismo convencional. A NATO apontou cinco razões pelas quais os ataques do ciberespaço podem ser uma maneira viável de serem usados pelo terrorismo ou até mesmo como arma de guerra:

- São mais baratos que o terrorismo tradicional;
- Possibilitam um maior anonimato, sendo mais difícil identificar os atacantes;
- Podem afectar um conjunto de alvos, muito maior;
- Podem ser realizados de maneira remota[8]".

Nos Estados Unidos da América, a definição legal dos atos ilícitos que compõem o cibercrime foram especificamente categorizados. Um grupo de trabalho composto, entre outros, por especialistas do FBI, refere no artigo "*Future Challenge of Cybercrime"* que "*the United States Code proscribes a range of conduct related to the use of computers in criminal behavior, including conduct relating to the obtaining and communicating of restricted information; the unauthorized accessing of information from financial institutions, the United*

([8]) Cardoso, S.L., (2007). *A resposta à emergência – n.º 19.*
Disponível na WWW:
<URL: www.cnpce.gov.pt/archive/doc/revista19.pdf >.

States government, and ´protected computers`; the unauthorized accessing of a government computer; fraud; the damaging of a protected computer resulting in certain types of specified harm; trafficking in passwords; and extortionate threats to cause damage to a "protected computer". Este estudo refere ainda que "*the legal definition of cybercrime tends to read like a grocery list and fails to anticipate future criminal variations in cyber offending"*. Os comportamentos cibercriminais são tão diversificados que podem ir desde a invasão de computadores, à fraude, ao roubo de propriedade intelectual, ao assédio sexual, etc. Majid Yar (2006) refere que "*cybercrime refers not so much to a single, distinctive kind of criminal activity, but more to a diverse range of illegal and illicit activities (…)*" (Yar, 2006, p.5).

Para além do que já foi referido, outra das dificuldades inerentes a esta forma de criminalidade, é a sua dificuldade em ser investigada pelas autoridades competentes. Para Santos, Bessa e Pimentel, no ambiente digital "a prova tem uma natureza instável e iminentemente fungível comparativamente às provas tradicionais do meio forense, como por exemplo a testemunha ocular, a impressão digital ou o ADN" (Santos, *et al*, 2008, p. 7). Contudo, tal como na criminalidade tradicional onde no momento em que é feita a análise ao local da prática do crime se deve ter em linha de conta os fundamentos da teoria de Locard, o mesmo deve acontecer também no ambiente digital.
Como Casey afirma:

> "De acordo com o Principio de Troca de Locard, o contacto entre dois itens resultarão numa troca. Este princípio aplica-se a qualquer contacto numa cena de crime, inclusive entre um criminoso e uma vítima, entre uma pessoa com uma arma, e entre as pessoas e a própria cena do crime. Em suma haverá sempre uma evidência de interação, embora nalguns casos possa não ser detetada facilmente (note que a ausência de evidência não é a evidência de ausência). Esta transferência ocorre quer nos reinos físicos quer nos digitais e pode fornecer ligações entre eles como descrito (…). A prova digital pode revelar comunicações entre suspeitos e vítima, atividades *on-line* em momentos-chave, e outras informações que fornecem uma dimensão digital para a investigação. Em invasões de computador, os atacantes vão deixar vários vestígios da sua presença por todo o lado, incluindo nos ficheiros do sistema, registos, *logs* de sistema e *logs* a nível da rede. Além disso, os atacantes poderiam levar elementos da cena do crime com eles, como senhas

> de usuários roubados ou Informações de Identificação Pessoal num ficheiro ou base de dados. Tal evidência pode ser útil para relacionar um indivíduo a uma intrusão. Num caso de assédio via *e-mail*, o ato de enviar mensagens ameaçadoras via um serviço de *e-mail* baseado na *web*, como o Hotmail, pode deixar uma série de vestígios. O navegador da *web* usado para enviar mensagens irá armazenar ficheiros, ligações e outras informações contidas no disco rígido do remetente, juntos com informações relacionadas com a data e a hora. Por isso, os analistas forenses podem encontrar um vasto leque de informações relacionadas com a mensagem enviada no disco rígido do ofensor, incluindo o conteúdo da mensagem original. Além disso, os investigadores podem ser capazes de obter informações relacionadas a partir do Hotmail, incluídos *logs* do servidor *web* de acesso, endereços IP e, possivelmente a mensagem completa na pasta dos *e-mails* enviados da conta de correio eletrónico do infractor".
>
> Casey, 2011, p.16 e 17

Casey e Schatz, (2011) referem ainda que, uma eficaz e completa investigação digital deve dividir-se em cinco etapas[9]: a preparação; a identificação; a preservação; a examinação e análise, e por fim a apresentação dos resultados (Casey e Schatz, 2011, p.189).

Em Portugal, Vera Dias realizou um trabalho onde abordou a problemática da investigação do cibercrime[10] e neste fez alusão a um estudo levado a cabo pela Europol, onde, resumidamente, são apontados os vários problemas com que se deparam os investigadores na investigação do cibercrime, e os quais passamos a citar:

([9]) **Preparação:** Traçando um plano de ação para realizar uma investigação digital eficaz para obter recursos de apoio e materiais.
Identificação: Encontrar potenciais fontes de evidência digital (por exemplo, na cena do crime, dentro de uma organização, ou na Internet). Porque o termo identificação tem um significado mais preciso na ciência forense respeitante à análise de um item de provas.
Preservação: Prevenindo mudanças nas evidências digitais, incluindo o isolamento do sistema na rede, protegendo os arquivos de *logs* relevantes, e recolhendo dados voláteis que estariam perdidos quando o sistema estivesse desligado. Esta etapa inclui a recolha subsequente ou a aquisição.
Examinação e análise: Em busca de pistas evidentes.
Alguns modelos de processo utilizam o termo examinação e análise indistintamente neste capítulo, uma pequena distinção é feita entre estas duas etapas numa investigação digital, onde a examinação forense é o processo de extrair e visualizar informações através da prova, e torna-la disponível para análise. Em contrapartida, a análise forense é a aplicação do método científico e do pensamento crítico para abordar as questões fundamentais numa investigação: quem, o quê, onde, quando, como e porquê.
Apresentação: Comunicar descobertas de modo a satisfazer o contexto da investigação, seja ela, jurídica, empresarial, militar, ou qualquer outra.

([10]) DIAS, V., (2010) -*A Problemática da Investigação do Cibercrime – I Curso Pós Graduação de aperfeiçoamento em Direito da Investigação criminal e da prova – Universidade de Lisboa – Faculdade de Direito.*
Disponível na WWW
<URL:http://www.verbojuridico.com/doutrina/2011/veradias_investigacaocibercrime.pdf>.

- A falta de legislação adequada;
- A falta de metodologia no tratamento da especificidade deste crime;
- A interoperatividade dos sistemas;
- A lentidão da cooperação e a falta de partilha de informações (quer entre entidades nacionais quer a nível internacional).

Pedro Verdelho referiu que existem "investigações científicas e policiais sobre os crimes cometidos no ciberespaço e as instâncias internacionais manifestam, cada vez mais, preocupação pelas consequências dos actos ilícitos cometidos nas redes, ou através das redes de computadores" (Verdelho, 2003, p.347 *in* Direito da Sociedade de Informação Volume IV). Nesse sentido, a Convenção sobre Cibercrime do Conselho da Europa foi um sinal claro de vontade de mudança, tendo sido alargada a possibilidade de adesão a países fora da Europa. Portugal adaptou a Convenção do cibercrime do Conselho de Europa (Cciber) retificando a sua própria lei com a entrada em vigor a 15 de Setembro, da Lei n.º 109/2009, Lei do Cibercrime (LC) a qual "veio introduzir novos meios de investigação e produção de prova específicos para o combate à criminalidade informática" (Venâncio, 2011, p. 23).

Para além da LC, continua a vigorar outra legislação, já existente, e que a pode completar. Nesse sentido, referirmo-nos à Lei n.º 7/2004, de 7 de Janeiro e à Lei n.º 32/2008, de 17 de Julho, bem como ao Decreto-lei n.º 41/2004, de 18 de Agosto.

III – METODOLOGIA DE INVESTIGAÇÃO

Enquadramento metodológico geral

Qualquer que seja o caminho enveredado na elaboração de um estudo científico, a explanação dos métodos e dos procedimentos utilizados para

alcançar o objetivo pretendido é fundamental. Podemos questionar o que são métodos e procedimentos. Quivy e Campenhoudt (2008) referem que, um "procedimento é uma forma de progredir em direcção a um objectivo (…). Os métodos não são mais do que formalizações particulares do procedimento, percursos diferentes concebidos para estarem mais adaptados aos fenómenos ou domínios estudados (…)". Citando a obra *Le métier de sociologue*[11], Quivy e Campenhoudt descrevem o procedimento como "um processo em três actos cuja ordem deve ser respeitada. É aquilo a que chamam «hierarquia dos actos epistemológicos». Estes três actos são a ruptura, a construção e a verificação (ou experimentação)" (Quivy & Campenhoudt, 2008, p. 25). Nesse caso, devemos ter em atenção quais os métodos e os procedimentos a levar em consideração na elaboração de um estudo científico.

Torna-se, portanto, essencial, assinalarmos quais os métodos e procedimentos utilizados na elaboração deste estudo, sendo legítimo questionarmo-nos acerca dos princípios fundamentais que esta investigação deve contemplar. Como tal, não devemos esquecer que "estabelecer com precisão o estado da questão que se estuda, também é, geralmente, um procedimento central de investigação" (Albarello, Digneffe, Hiernaux, Maroy, Ruquoy, Saint-Georges, 2005, p. 15). Quivy e Campenhoudt consideram que "ainda que a sua preocupação não seja fazer uma investigação científica em sentido estrito, mas sim apresentar um estudo honesto sobre uma questão particular, continua a ser indispensável tomar conhecimento de um mínimo de trabalhos de referência sobre o mesmo tema ou, de um modo mais geral, sobre problemáticas que lhe estão ligadas" (Quivy & Campenhoudt, 2008, p. 51).

No campo da pesquisa deste tema deparamo-nos com a difícil tarefa de escolher entre a realização de uma pesquisa qualitativa ou quantitativa, ou ainda optar por uma que permitisse abranger ambas as técnicas. Bell refere que a "abordagem adoptada e os métodos de recolha de informação

([11]) *Le métier de sociologue* (1968) de Pierre Bourdieu, Jean-Claude Chamboredon et Jean-Claude Passeron.

selecionados dependerão da natureza do estudo e do tipo de informação que se pretenda obter" (Bell, 2007, p. 20). Nesse sentido, consideramos de toda a importância, abordar o tema deste estudo através da utilização de mais do que um método de recolha de dados, recorrendo-se, para o efeito, a uma técnica de investigação qualitativa e quantitativa.

A investigação qualitativa é uma técnica "que exige o contacto face a face com um indivíduo, com um grupo, ou a observação do comportamento em contexto natural, o que permite desenvolver uma ideia aprofundada do modo como as pessoas pensam, sentem, interpretam, experimentam os acontecimentos em estudo. É um método, especialmente, apropriado quando o investigador pretende ter uma compreensão aprofundada do fenómeno em estudo (…)" (Ribeiro, 2008, p.66). Já a utilização da investigação quantitativa, leva a que seja necessário conduzir "uma análise focalizada na procura de padrões de relacionamento em variáveis, ou relações de causalidade entre variável dependente e (diversas) independentes" (Silvestre & Araújo, 2012, p. 172). Nessa medida, aplicamos como técnica, para a recolha de dados, a pesquisa bibliográfica e documental, a entrevista semi-estruturada e o inquérito. "Este método de aproximação múltipla é conhecido como triangulação (…)" (Bell, 2007, p. 96). Desta forma, será possível medir a amplitude do cibercrime, ou seja, ficar a par da dimensão do fenómeno e das necessidades que requer o seu combate.

Na pesquisa bibliográfica e documental, foram realizadas diversas leituras, sobre decisões legislativas europeias, diretamente relacionadas com o cibercrime, artigos de imprensa presentes na internet, bibliografia nacional e internacional, teses de doutoramento e matérias que se considerou muito enriquecedoras para o estudo a realizar. Ademais, à consulta deste vasto leque documental escrito, foram igualmente ouvidas algumas entrevistas, as quais se encontram disponíveis, para consulta pública, na internet, muitas das quais foram concedidas a órgãos de comunicação social portugueses, quer por especialistas na área da informática, quer por juristas ou por peritos em

investigação criminal. Adverte-se, porém, os mais renitentes quanto à utilização de informação radiofónica que "o conceito de documento ultrapassa a ideia de textos escritos e/ou impressos. O documento, como fonte de pesquisa, pode ser escrito e não escrito, tais como filmes, vídeos, slides, fotografias ou pósteres. Esses documentos são utilizados como fontes de informação, indicações e esclarecimentos que trazem o seu conteúdo para elucidar determinadas questões e servir de prova para outras, de acordo com o interesse do pesquisador[12]" (Figueiredo, citado por Sá Silva, Almeida & Guidani, 2009, p. 5). Nesse sentido, também Bell refere que "«documento» é um termo geral que designa uma impressão deixada num objeto físico por um ser humano. A investigação pode envolver a análise de fotografias, de filmes, de vídeos, de diapositivos e de outras fontes não escritas, todas elas classificáveis como documentos (…)" (Bell, 2010, p. 103). Em relação à entrevista, Bell refere que "a grande vantagem da entrevista é a sua adaptabilidade (…), a forma como determinada resposta é dada (o tom de voz, a expressão facial, a hesitação, etc.) pode transmitir informações que uma resposta escrita nunca revelaria" (Bell, 2010, p. 137).

Como já havíamos referido, recorremos à entrevista semi-estruturada. Semi-estruturada, no sentido em que "não é inteiramente aberta nem encaminhada por um grande número de perguntas precisas" (Quivy & Campenhoudt, 2008, p. 192). Neste tipo de entrevistas predominam "perguntas que estimulam o entrevistado a apresentar o seu ponto de vista, exprimir a sua opinião (…). O entrevistador pode conduzir a entrevista de forma a obter os dados que pretende, orientando-a através da sequência em que coloca as perguntas e/ou colocando perguntas que considera mais convenientes numa determinada fase da entrevista" (Silvestre & Araújo, 2012, p. 151). Sabendo-se que os dados investigados são também eles qualitativos, a utilização da entrevista semi-estruturada permite que "o próprio entrevistado estruture o seu pensamento em

([12]) Silva, Almeida, Guidani (2009). *Pesquisa Documental: pistas teóricas e metodológicas* Revista Brasileira de História & Ciências Sociais, *p.5*. Disponível na WWW**:**
<URL: http://www.rbhcs.com/index_arquivos/Artigo.Pesquisa%20documental.pdf >.

torno do objecto perspectivado" (Albarello et al., 2005 p. 87). Porém, um dos limites à sua aplicação demarca-se pelo "facto de a flexibilidade do método poder levar a acreditar numa completa espontaneidade do entrevistado (…)" (Quivy & Campenhoudt, 2008 p. 194). Com a realização da entrevista semi-estuturada, pretendeu-se que os entrevistados contribuíssem com todo o seu conhecimento e experiência, o que, tal como esperado, acabou por acontecer, uma vez que foram concedidas três entrevistas por especialistas oriundos de áreas de trabalho distintas, todos eles especializados na área do cibercrime.

Segundo alguns autores, as entrevistas podem ainda ter "cariz exploratório ou confirmatório" (Silva & Araújo, 2012, p. 150). Atendendo ao que se pretendia alcançar com este estudo, optamos pela entrevista exploratória, tendo em atenção que esta forma de realizar entrevistas "não tem como função verificar hipóteses nem recolher ou analisar dados específicos, mas sim abrir pistas de reflexão, alargar e precisar os horizontes de leitura, tomar consciência das dimensões e dos aspectos de um dado problema, nos quais o investigador não teria decerto pensado espontaneamente" (Quivy & Campenhoudt, 2008, p. 79).

Seguimos, mais uma vez, a ideia de Quivy e Campenhoudt quando defendem que há "três categorias de pessoas que podem ser interlocutores válidos. (…) *docentes*, *investigadores especializados* e *peritos* no domínio de investigação implicado pela pergunta de partida" (Quivy & Campenhoudt, 2008, p. 71). Seguindo essa ideia, pretendeu-se obter uma diversidade de opiniões. Esta diversidade, segundo Guerra "relaciona-se com a garantia de que a utilização das entrevistas se faz tendo em conta a heterogeneidade dos sujeitos (ou fenómenos) que estamos a estudar. De facto, na pesquisa qualitativa, procura-se a diversidade e não a homogeneidade, e, para garantir que a investigação aborde a realidade considerando as variações necessárias, é preciso assegurar a presença da diversidade dos sujeitos ou das situações em estudo" (Guerra, 2010, p. 40).

De seguida, mencionar-se-á as especializações académicas dos entrevistados, bem como as funções profissionais desempenhadas pelos mesmos. Desta forma, e sem violar o acordo firmado com os mesmos, ou seja, o de preservar as suas identidades, e por conseguinte, mantê-los em anonimato, caracterizamo-los da seguinte forma:

- Entrevistado número 1 [E01], Engenheiro Informático, exerce funções de investigador criminal numa secção da Polícia Judiciária, especializada na investigação de crimes ligados à criminalidade informática;

- Entrevistado número 2 [E02], Engenheiro Informático, docente do ensino superior e coordenador de serviços de tecnologia e informação, na especialidade da informática;

- Entrevistado número 3 [E03] Licenciado em Direito, docente do ensino superior e especialista na área do direito informático.

Ao longo do estudo, julgou-se, de igual modo, pertinente, avaliar qual o conhecimento e a perceção que alguns utilizadores domésticos da informática e da Internet pudessem demonstrar sobre o fenómeno do cibercrime. Tal avaliação foi aferida de uma forma quantitativa, através da aplicação de um inquérito. Atendendo que o tema do presente trabalho aborda o tema do cibercrime em Portugal, as suas trajetórias e perspetivas de futuro, considerou-se pertinente tentarmos, desta forma, obter a opinião pessoal de cada inquirido sobre o que acreditam ser o cibercrime, se alguma vez o praticaram ou se conhecem alguém que o tenha praticado e, ainda de uma forma genérica, se já foram vítimas deste fenómeno e se o denunciaram às autoridades policiais.

Procedimentos na preparação e execução das entrevistas

Moser e Kalton (1971) citados por Bell descrevem a entrevista como sendo "uma conversa entre um entrevistador e um entrevistado que tem o objectivo de extrair determinada informação do entrevistado" (Bell, 2010, p. 137). Porém, essa conversa deve assentar na confiança, pelo que o "sucesso da entrevista está associado à capacidade do entrevistador para estabelecer um relacionamento com o entrevistado" (Bryman, citado por Silva & Araújo, 2012, p. 149).

Devido à grande distância geográfica que separa o local de residência do entrevistador da dos entrevistados, e pelo facto de que os mesmos acederam a ser entrevistados e pelo qual merecem toda a consideração, todas as entrevistas desenrolaram-se nos locais de trabalho dos entrevistados, num horário previamente acordado.

Antes de se iniciar as entrevistas, solicitou-se, previamente, a cada entrevistado autorização para se proceder ao registo das mesmas, através de gravador de áudio. Tal autorização foi concedida com a condição de que as gravações não fossem divulgadas publicamente, vontade que será seguramente respeitada. Nesse sentido, procedeu-se então à gravação áudio de todas as entrevistas realizadas. O recurso a registos áudio prende-se com o facto de poderem, segundo Bell ser "úteis para verificar as palavras de uma afirmação que pretenda citar e para verificar a exactidão das suas notas. Podem igualmente ser úteis se pretender empreender uma análise de conteúdo" (Bell, 2010,p. 143). Assim, e seguindo as regras normais da boa educação, como não poderia deixar de o ser, iniciou-se cada uma das entrevistas após uma breve apresentação do entrevistador, onde foi indicado o nome da instituição de ensino superior onde se realiza o estudo, bem como uma explanação sucinta do objetivo pretendido com a investigação em curso. Importa referir que elaborou-se, previamente, um guião personalizado para

cada entrevista, pois achou-se necessário, devido à especialização de cada entrevistado, adequar as questões colocadas.

No decorrer das entrevistas, decidiu-se não seguir a ordem pela qual as questões estavam redigidas no guião, moldando-as e, até mesmo, modificando-as, à medida que as opiniões dos entrevistados eram transmitidas. E, nessa direção, seguimos mais uma vez a opinião de Quivy e Campenhoudt quando referem que "o investigador dispõe de uma série de perguntas-guias, relativamente abertas, a propósito das quais é imperativo receber uma informação da parte do entrevistado. Mas não serão colocadas necessariamente todas as perguntas pela ordem em que as anotou e sob a formulação prevista. Tanto quanto possível, «deixará andar» o entrevistado para que este possa falar abertamente, com as palavras que desejar e pela ordem lhe convier" (Quivy & Campenhoudt, 2008, p. 192). Estes dois autores referem ainda que durante as entrevistas "trata-se, de facto, de fazer aparecer o máximo possível de elementos de informação e de reflexão, que servirão de materiais para uma análise sistemática de conteúdo que corresponda, por seu lado, às exigências de explicitação, de estabilidade e de intersubjectividade dos processos" (Quivy & Campenhoudt, 2008, p. 195).

Com a elaboração do guião de entrevistas, esperamos conseguir abordar alguns dos pontos considerados essenciais na LC, desde as disposições penais, passando pelas disposições processuais e pelas necessidades evolutivas no combate ao fenómeno. Segundo Lalanda (1998), a "condução da entrevista é, em geral, orientada por um guião que se construiu, mas que se procurou interiorizar (decorar) nas suas grandes linhas[13]" (Lalanda, 1998, p. 880). Nesse sentido, optou-se por perguntas-guias, relativamente abertas, cujo conteúdo foi adaptado à especialização de cada um dos entrevistados, uma vez que não podemos esquecer que cada um tem uma área de especialização

([13]) Disponível na WWW:
<URL www.apis.ics.ul.pt/SendDoc.aspx?d=1072&q=9365>.

distinta. Quanto ao número de questões, cada entrevista é composta por 7 a 8 questões, e todas elas visam, diretamente, a LC *(ver anexo p. 85).*

Procedimentos na preparação e execução dos inquéritos por questionário

Na elaboração das questões que compõem o inquérito, teve-se em atenção a não colocação de questões ambíguas e imprecisas, ou ainda que a especificidade do tema requeresse, dos inquiridos, determinado tipo de informação técnica que pudessem desconhecer (Bell, 2010). Quanto à forma como seriam colocadas, seguiu-se a ideia de que, as perguntas que integram um inquérito por questionário podem ser perguntas fechadas. Silvestre e Araújo (2012) dizem-nos que "existem também questões, que preveem um conjunto de categorias de resposta e acrescentam uma categoria para contemplar uma possível resposta não prevista pelo pesquisador (sendo normalmente usada a categoria <outras> para esta categoria de resposta deixada em aberto). As vantagens desta forma de pergunta (por vezes identificada como <mista>) são o facto de permitir ampliar o quadro de resposta (…)" (Silvestre & Araújo 2012, p. 159).

Importa agora falar da conceção do inquérito. Silvestre e Araújo dizem que "as perguntas devem ser claras e concisas. A linguagem utilizada nas perguntas e nas categorias de resposta deve ser simples, para estar ao alcance das capacidades de interpretação e dos conhecimentos dos sujeitos (…) devem evitar interpretações dúbias e não podem incitar a resposta. Quanto à apresentação, as perguntas devem estar ordenadas, contribuído para a coerência interna do inquérito" (Silvestre & Araújo 2012, p. 160).

No que diz respeito aos instrumentos de recolha de informação, os mesmos devem "ser testados para saber quanto tempo demoram os receptores a realizá-los; por outro lado, isto permite eliminar questões que não conduzam a dados relevantes" (Bell, 2008, p. 128). No seguimento desta indicação e, antes

de distribuirmos os questionários, decidimos testar a clareza das perguntas colocadas pelo que, foi aplicado um pré-teste ou exercício piloto, cujo objetivo segundo Bell "consiste em descobrir problemas apresentados pelo instrumento de recolha de informação que escolher, de modo que os indivíduos no seu estudo real não encontrem dificuldades em responder" (Bell, 2010, p. 129).

Formato do inquérito por questionário

Para a elaboração do inquérito por questionário, seguiu-se a ideia de que não "há regras definidas sobre o formato de um questionário, mas algumas linhas de orientação dilatadas pelo senso comum contribuirão para uma boa apresentação" (Bell, 2010, p. 126). Portanto, realizou-se um questionário composto por 13 questões *(ver anexo p.87)*, as quais foram espaçadas entre si, com vista a ajudar o inquirido na parte da leitura, e também no momento em que se procede à análise das respostas (Bell, 2010). Quivy e Campenhoudt referem que "essa forma de questionário é de «administração directa» quando é o próprio inquirido que o preenche. O questionário é-lhe então entregue em mão por um inquiridor encarregado de dar todas as explicações úteis (…)"(Quivy & Campenhoudt, 2008, p. 188). A principal vantagem apontada para a utilização deste método prende-se com a possibilidade em "quantificar uma multiplicidade de dados e de proceder por conseguinte, a numerosas análises de correlação, o facto de a exigência, por vezes essencial, de representatividade do conjunto dos entrevistados poder ser satisfeita através deste método" (Quivy & Campenhoudt, 2008, p. 189). É preciso sublinhar, no entanto, que "esta representatividade nunca é absoluta, está sempre limitada por uma margem de erro e, só tem sentido em relação a um certo tipo de perguntas – as que têm sentido para a totalidade da população em questão. (…) Um dos limites ou problemas que retemos na utilização deste tipo que inquérito, e aquele em que referem que umas das limitações, prende-se com o facto de os resultados apresentarem-se muitas vezes como simples descrições, desprovidas de elementos de compreensão penetrantes" (Quivy & Campenhoudt, 2008, p.189 e 190).

Caracterização dos inquiridos

É importante mencionarmos que, a forma como o inquérito foi aplicado, não obedeceu, no que diz respeito à população alvo, a uma regra previamente determinada. O pouco tempo disponível para a elaboração do presente estudo tornou-se um obstáculo incontornável, pelo que optou-se por entrevistar pessoas ao acaso, questionando a sua disponibilidade e disposição a colaborar nesse momento (Bell, 2010). Diz-nos ainda Bell, que "as amostras de oportunidade deste tipo são geralmente aceitáveis, desde que se explique claramente a forma como se chegou a elas e se esteja ciente das limitações que tais dados implicam. No entanto, mesmo num estudo pequeno há que tentar seleccionar a amostra mais representativa possível" (Bell, 2010, p. 127) Nesse sentido, distribuiu-se, os 65 inquéritos de forma aleatória, a 65 funcionários de duas empresas, uma ligada ao ramo da hotelaria, e outra ligada à área da saúde, tratando-se todos os inquiridos de pessoas que, diariamente devido às suas funções laborais, utilizam os computadores e a Internet, no trabalho ou no conforto do seu lar.

Como podemos constatar no quadro que se segue, a amostra é composta por um universo de 65 pessoas, 69,2 por cento do sexo masculino e 30,8 por cento do sexo feminino.

Quadro n.º 1 - Género dos inquiridos

	Frequência	%
Masculino	45	69,2
Feminino	20	30,8
Total	65	100,0

Fonte: Recolha de dados - Inquéritos 2012

No quadro seguinte, verifica-se que a idade mínima dos inquiridos situa-se nos 18 anos, e a máxima nos 59 anos. A média de idade situa-se perto dos 35 anos, com um desvio padrão de, aproximadamente 8.

Quadro n.º 2 - Média de idade dos inquiridos

	N	Idade mínima	Idade máxima	Média de idade dos inquiridos	Desvio padrão
Idade	65	18	59	35,42	8,305
Valido	65				

Fonte: Recolha de dados - Inquéritos 2012

Tratamento dos dados

Ao atingir esta etapa do estudo, torna-se fundamental analisar e avaliar todos os dados recolhidos durante a investigação. E, para se proceder a essa análise, utilizou-se a análise de conteúdo. A utilização deste método na análise das entrevistas, "oferece a possibilidade de tratar, de forma metódica, as informações e testemunhos que apresentam um certo grau de profundidade e de complexidade, como por exemplo, os relatórios de entrevistas pouco directivas (…)" (Quivy & Campenhoudt, 2008, p. 227), e também pelo facto de em investigação social, "o método das entrevistas está sempre associado a um método de análise de conteúdo" (Quivy & Campenhoudt, 2008, p. 195). No que diz respeito à análise dos dados obtidos através dos inquéritos por questionários, foi também utilizado o mesmo método. De facto, "se nos tentarmos distanciar dos métodos de análise de conteúdo e do domínio em que estes podem ser explorados, apercebemo-nos de que o campo de aplicação é extremamente vasto. Numa última análise, qualquer comunicação, isto é, qualquer veículo de significados de um emissor para um receptor controlado ou não por este, deveria poder ser escrito, decifrado pelas técnicas de análise de conteúdo" (Bardin, 2009, p. 34).

Relativamente aos inquéritos por questionário, efetuou-se uma análise dos resultados obtidos, após a contagem de todas as respostas, estando a sua interpretação orientada para a frequência de ocorrência de cada questão abordada. Tratando-se de uma parte do estudo onde se pretende alcançar resultados, os que foram obtidos permitiram aferir, ainda que de uma forma

pouco aprofundada, a perceção que os inquiridos têm do cibercrime e do perigo que o mesmo representa.

Quanto ao tratamento das entrevistas utilizou-se a análise da avaliação como tipo de análise de conteúdo para cada uma. A avaliação "mede as atitudes do entrevistado face ao objecto de estudo e a direcção e a intensidade da opinião: desmembra-se o texto em unidades de significação (…) e analisa-se a carga avaliativa" (Guerra, 2010, p. 63). Antes de mais, convém referir que as transcrições não foram anexadas ao presente estudo, para que a confidencialidade seja assegurada. Contudo, convém referir que as mesmas se encontram na posse do investigador, bem como todos os ficheiros áudio armazenados em suporte digital. Não obstante, será entregue conjuntamente com a dissertação, uma cópia, em suporte digital, das referidas gravações.

Para se iniciar a análise das entrevistas, procedeu-se, na íntegra, à sua transcrição. Debruçamo-nos, para isso, sobre a ideia de Guerra (2010), que enumera algumas propostas que consideramos interessantes e as quais tivemos em consideração. Relacionado com a celeridade dessa mesma transcrição, e segundo o próprio, devemos:

- "Numa primeira fase, transcrever (de preferência logo no computador) o que se ouve na audição, deixando espaços em branco nas passagens em que a audição não é clara;
- Numa segunda fase, rever a gravação e preencher manualmente as «brancas»;
- Numa terceira fase, redigir um discurso inteligível, com pontuação, supressão e com supressão de elementos inúteis" (Guerra, 2010, p. 69).

IV – ANÁLISE EMPÍRICA

Trajetórias do objeto de estudo

Para consolidar o objeto de estudo, considerou-se, fundamental, destacar, de entre todas as respostas obtidas no decorrer das entrevistas, as que se considerou conterem informação mais enriquecedora, nomeadamente, as que permitissem identificar as potencialidades da LC e também apontar os pontos fracos que a mesma possa ter. Contudo, "em primeiro lugar é preciso «ler». Mas não basta ler e compreender «normalmente». É possível usar perguntas como auxílio: «O que está esta pessoa a dizer realmente? Como isso é dito? Que poderia ela ter dito de diferente? O que não diz ela? Que diz sem dizer? Como é que as palavras, as frases e as sequências se encadeiam entre si? Qual a lógica discursiva do conjunto? Será que posso resumir a temática de base e a lógica interna específica da entrevista? etc.». (Após a decifração de várias respostas ou entrevistas, outras perguntas se acrescentarão por comparação: «Esta pessoa manifesta em tal sítio tal tema, onde é que já o vi noutra entrevista?(…)" (Bardin, 2009, p. 94). Como tal, selecionou-se, criteriosamente, de entre a totalidade da informação recolhida, a que nos pareceu corresponder ao objeto da pesquisa. Em seguida, organizamo-la numa grelha, classificando cada uma das respostas por entrevistas e pelas diferentes informações pretendidas. Esta classificação permite uma leitura rápida dessa mesma informação, conferindo uma fácil comparação entre toda a informação-chave, extraída de cada uma das questões colocadas aos entrevistados. Posteriormente, far-se-á uma decifração estrutural desse mesmo conteúdo. A grelha em questão encontra-se representada nas páginas seguintes e, como já foi referido, contém a informação selecionada e retirada das três entrevistas realizadas, as quais relembra-se, são de cariz exploratório. Espera-se que o objetivo primo das mesmas seja alcançado e, que com a informação recolhida, seja possível identificar os pontos mais relevantes, e assim compreender as trajetórias do cibercrime em Portugal. Assim sendo, passamos nas páginas seguintes, à análise dessas questões.

Quadro n.º 3 – Análise das entrevistas

INFORMAÇÃO PRETENDIDA	ENTREVISTA 1	ENTREVISTA 2	ENTREVISTA 3
Opinião sobre a qualidade da atual lei do Cibercrime	É a lei que temos, é com ela que trabalhamos [Q2] Tem mecanismos de cooperação Internacional [Q2] Esta lei veio acrescentar algumas coisas, nada de significativo a nível da tipificação dos crimes [Q3]	Uma mais-valia (…) pela componente de atualização que esta lei traz relativamente à anterior (…) [Q2]	Havia a possibilidade da lei ser mais compacta [Q1] É uma lei equilibrada [Q2]
Opinião sobre uma diminuição da criminalidade informática desde a entrada em vigor da LC	"De maneira nenhuma esta lei foi um seguimento de uma lei anterior que já existia desde 1991, em que os comportamentos ilícitos já estavam balizados nessa lei anterior, esta lei veio acrescentar algumas coisas, nada de significativo a nível da tipificação dos crimes (…)" [Q3]	Acho que sim (…) não só pela perspetiva da prevenção mas por aquilo que permite em termos de atuação (…) resta ver é ao longo do tempo (…) [Q4]	*(Ainda não há feed back judicial visto a lei ser muito recente)*
Potencialidades da atual lei do cibercrime	Ponto de contacto 24h/7 [Q4] Troca de informação a nível internacional (Q4)	Atualização de uma série de conceitos que, até agora, existiam do ponto de vista tecnológico dada à evolução, mas que não estavam tipificados [Q6] Cooperação internacional [Q6]	Uma lei que tenta salvaguardar ao máximo os direitos fundamentais dos não delinquentes [Q3] É uma lei que está na linha do princípio da proporcionalidade [Q5]

(Continua na página seguinte)

Pontos fracos da lei do cibercrime	A conflitualidade com a lei de retenção dos dados [Q4] Há uma série de coisas que necessitariam de ser revistas [Q2]	Poderá limitar a componente de investigação, a componente académica e, mesmo quem trabalha nestas áreas, acaba por estar limitado. A lei não contempla a possibilidade dessas áreas poderem investigar e desenvolver [Q2]	Nalguns aspetos é obscura [Q1] Não será a mais eficaz para o combate ao crime, mas isso é algo que é da própria natureza [Q3]
Perspetiva de futuro para a lei do cibercrime	Obrigar os ISP, em determinadas situações mais gravosas, a responder rapidamente aos pedidos das autoridades, por exemplo em 48 horas [Q8] Devia de haver uma revisão séria da lei [Q9] Limitar algumas interpretações extensivas que estão a ser feitas [Q9]	Provavelmente, terá de passar por nova atualização ou adaptar-se de forma mais concreta às tecnologias [Q4] Contemplar a existência de indivíduos que atuem nesta área de forma legítima Criar mecanismos para atualizar-se, em termos do ponto de vista tecnológico porque em termos tecnológicos a evolução é extremamente rápida A evolução vai ser a lei tornar-se um pouco mais generalista no que diz respeito aos conceitos (Q7)	Gostaria que deixassem esta lei ficar tal como está, o tempo suficiente até conseguirmos, com objetividade, determinar se foi ou não eficaz [Q8]

Fonte: Recolha de dados - Entrevistas 2012

A primeira informação recolhida está relacionada com a opinião dos entrevistados sobre a qualidade da atual LC:

- Do primeiro entrevistado, (investigador criminal) destaca-se a seguinte observação: "(…) é a lei que temos, é com ela que trabalhamos (…)" [E1,Q2] – esta resposta evidencia, segundo a nossa opinião, um certo conformismo por parte do entrevistado. É sabido que as leis existem e são para se cumprir, sejam consideradas boas ou más. Krech,

Crutchfield e Ballachey (1962) dizem "que para existir conformismo tem de haver conflito" (Noronha & Noronha, 2003, p. 49). Ora, o conflito parece estar presente nesta observação, pois a LC pode já ter demonstrado ao entrevistado que esta não é, conforme está atualmente redigida, a mais eficaz no combate ao cibercrime. Esta opinião é, provavelmente, fruto da experiência profissional do entrevistado e das funções que desempenha, que o obrigam a reger-se pela lei em vigor, apesar de não estar convicto de que esta seja a mais eficaz para fazer frente ao cibercrime.

- O segundo entrevistado (especialista informático) pelo contrário defende que a LC é "uma mais-valia pela componente de atualização que traz relativamente à anterior" [E2,Q2]. Esta opinião corrobora com a nossa ideia de que uma lei criada para o combate ao cibercrime não deve ficar aquém da evolução tecnológica, devendo ser atualizada a par dessa evolução, pois acredita-se que só assim poderá manter a sua eficácia.

- A opinião do terceiro entrevistado (especialista em direito do cibercrime) direciona-se para a redação da LC. É da sua opinião o facto da *"*(…) possibilidade da lei ser mais compacta" [E3,Q1], pois, conforme refere é possível encontrar, na mesma, diversas camadas de sentido. Apesar destes reparos, no que diz respeito à qualidade da LC, acredita mesmo assim que esta "é uma lei equilibrada" [E3,Q2]. Nesse sentido, julga-se que o equilíbrio evocado pelo entrevistado está relacionado com os direitos, liberdades e garantias de todos, inclusive dos suspeitos.

A segunda informação recolhida visa a opinião, de uma eventual diminuição da criminalidade informática, desde a entrada em vigor da LC:

- O primeiro entrevistado refere que "de maneira nenhuma (…) esta lei foi um seguimento de uma lei anterior, que já existia desde 1991, em que sensivelmente os comportamentos ilícitos já estavam balizados nessa lei

anterior, esta lei veio acrescentar algumas coisas, nada de significativo a nível da tipificação dos crimes (…)" [E1, Q3].

- Sobre esse assunto, o segundo entrevistado respondeu "acho que sim (…) não só pela perspetiva da prevenção mas por aquilo que permite em termos de atuação (…) resta ver é ao longo do tempo (…) [E2,Q4].

Sobre esta informação-chave, o terceiro entrevistado foi mais cauteloso, e não quis responder a esta questão, deixando apenas a ideia de que a LC é muito recente, e não há, ainda, qualquer *feedback* judicial.

A terceira informação recolhida junto dos entrevistados prende-se com as potencialidades da LC:

- Recorrendo à resposta dada pelo primeiro entrevistado, verifica-se que é dada importância à parte processual da LC, nomeadamente no que diz respeito à cooperação internacional e na possibilidade conferida pela "troca de informação a nível internacional" e também pela existência de um ponto de contacto 24h/7 dias [E1,Q4] que permite que as autoridades estejam permanentemente em contacto. De facto, uma das novidades trazidas pela LC encontra-se prevista no seu artigo 20.º, que confere às autoridades portuguesas a possibilidade de "cooperarem com as autoridades estrangeiras competentes para efeitos de investigações ou procedimentos respeitantes a crimes relacionados com sistemas ou dados informáticos (…)" (Venâncio, 2011, p.124).

- O segundo entrevistado realça a parte penal da LC, quando refere que contempla uma "série de conceitos, até agora existentes do ponto de vista tecnológico dada à evolução, mas que não estavam tipificados" [E2,Q6]. Neste caso, os mesmos encontram-se previstos no artigo 2.º da LC, e dizem respeito à introdução de novos termos que não eram contemplados na revogada LCI. Termos tais como "dados informáticos,

dados de tráfego, fornecedor de serviço", que agora, estão definidos na lei.

- Já o terceiro entrevistado aponta como potencialidade o facto da LC ser "uma lei que tenta salvaguardar ao máximo os direitos fundamentais dos não delinquentes" [E3,Q3], referindo ainda que se trata de "uma lei que está na linha do princípio da proporcionalidade" [E3,Q5]. Nesse sentido, segundo a opinião do entrevistado, depreende-se que é uma lei que pauta pelo respeito dos direitos fundamentais dos cidadãos, sem que haja uma diminuição da função repressiva.

A quarta informação recolhida relaciona-se com os pontos fracos da LC:

- A fragilidade apontada pelo primeiro entrevistado diz respeito à conflitualidade existente com a lei de retenção dos dados. Essa conflitualidade, estará, provavelmente, relacionada com o que está preceituado na Lei n.º 32/2008 de 17 de Julho, e que se refere à *conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações,* mais precisamente no artigo 2.º alínea *g),* onde é definido o que se consideram crimes graves para o efeito desta lei, e no artigo 3.º n.º 1 onde está previsto que a conservação dos dados só será efetuada aquando da deteção e posterior repressão dos crimes graves. Ora, a criminalidade informática não se encontra prevista nesses crimes. Contudo, o artigo 12.º da LC preceitua que, caso seja necessário para a produção de prova, os dados de tráfego poderão ser preservados. Convém mencionar uma nota de opinião do Ministério da Administração Interna, datada do dia 2 de Outubro de 2009, referente a essa matéria e que diz o seguinte: "*A realização de interceções de comunicações eletrónicas e, sobretudo, a obtenção de dados de tráfego, são ferramentas processuais essenciais em processo-crime em que se investiguem crimes cometidos por via das redes de comunicações,*

tendo essa preocupação ficado espelhada no diploma que obriga os operadores de comunicações a guardarem os dados de tráfego dos seus clientes, tendo em vista a sua eventual necessidade em investigação criminal – Lei n.º 32/2008, de 17 de Julho, que regula a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas. A Lei n.º 109/2009 veio fornecer ao sistema processual penal normas que permitam a obtenção de dados de tráfego e a realização de interceções de comunicações em investigações de crimes praticados no ambiente virtual. O novo diploma condensa todas as normas respeitantes à cibercriminalidade. Optou-se por não se proceder à alteração das várias fontes legislativas sobre a matéria (…)[14]*".* Ora, neste caso a interpretação que se faz, é a de que a Lei 109/2009 de 15 de Setembro, veio complementar a Lei n. 32/2008 de 17 de Julho, no que diz respeito à possibilidade de requerer a preservação de dados de ambientes informáticos.

- O segundo entrevistado sublinha que, na parte que diz respeito ao ensino e à educação, a LC é algo limitada – ao analisar as razões implícitas nesta última opinião, pode-se depreender que a limitação apontada, se encontra relacionada com a forma como a lei está redigida, por não possibilitar a componente investigatória, relativamente à pesquisa informática numa vertente educativa e preventiva. Na opinião do entrevistado, a atual LC "(…) poderá limitar a componente de investigação, a componente académica e até mesmo quem trabalha nesta área acaba por estar limitado. A lei não observa a possibilidade dessas áreas poderem investigar e desenvolver" [E2,Q2]. Nesse sentido, também Rui Seabra, presidente da Associação Nacional para o Software Livre (ANSOL), referiu publicamente, ainda antes da entrada em vigor da LC, que a lei terá "um impacto negativo ao colocar em risco o

([14]) Disponível na WWW:
<URL: http://opiniao.mai-gov.info/2009/10/02/a-nova-lei-do-cibercrime/ >.

desenvolvimento de ferramentas de segurança, e colocará em causa o ecossistema, que permite a melhoria da segurança dos sistemas operativos e outros programas de computador[15]". Volvidos, praticamente três anos desde a entrada em vigor da LC, a opinião do entrevistado vai de encontro à opinião tornada pública pelo presidente da ANSOL antes da entrada em vigor da nova LC. Sobre este ponto, o terceiro entrevistado refere que, este assunto foi debatido na altura da elaboração do projeto de lei e, que este debate só faz sentido por parte de quem não tenha nenhum ou quase nenhum conhecimento em direito penal, pois segundo referiu, neste caso preciso entra a noção de dolo específico, dando como exemplo o facto de alguém desenvolver um *software* espião, e que se não houver ou não se demonstrar nenhuma relação causal entre esse desenvolvimento e a tentativa de, pelo menos, introduzir esse software num sistema, não se preenche o dolo específico, previsto no tipo [E3,Q7], ou seja, segundo este, não existindo a intenção de prejudicar, não haverá lugar à prática de crime.

- Sobre os pontos fracos da LC, o terceiro entrevistado refere que a mesma "nalguns aspetos é obscura" [E3,Q1]. Tudo terá a ver com a forma como o diploma se encontra redigido, no que diz respeito à sua essência, o que, segundo o próprio, pode suscitar dúvidas quanto à sua interpretação.

Por último, apontar-se-á algumas perspetivas de futuro para a LC referidas pelos três entrevistados:

- O primeiro entrevistado indica duas prioridades para o futuro, pelo que, segundo suas palavras, deve "haver uma revisão séria da lei". As prioridades passam por "limitar algumas interpretações extensivas que estão a ser feitas" [E1,Q9], e "obrigar os ISP, em situações mais

([15]) Disponível na WWW:
<URL:http://tek.sapo.pt/opiniao/entrevista_lei_do_cibercrime_seguranca_nacion_1005695.html>.

gravosas, a responder rapidamente aos pedidos das autoridades, por exemplo em 48 horas" [E1,Q8]. Segundo referiu, um dos problemas na celeridade das investigações prende-se com a inexistência de um tempo estipulado, para que os responsáveis pela retenção dos dados respondam aos pedidos que, por vezes, são essenciais para o eficaz desenrolar de uma investigação no âmbito criminal. Sobre este assunto, foi assinado, a 9 de julho de 2012, um protocolo de cooperação entre a Procuradoria-Geral da República e os operadores de comunicações eletrónicas enquadrando a cooperação funcional entre estes operadores e o Ministério Público, no âmbito da atividade de investigação criminal deste último. Este protocolo visa incrementar a cooperação mútua e alcançar uma maior eficácia no combate ao cibercrime e na obtenção de prova digital[16]".

- O segundo entrevistado acredita que o futuro passará por uma nova atualização ou adaptação da lei, de uma maneira mais concreta às novas tecnologias [E2,Q4], defendendo uma LC que contemple a existência de indivíduos, que atuem nesta área de forma legítima e crie mecanismos para se atualizar do ponto de vista tecnológico, uma vez que nesses termos, a evolução é extremamente rápida [E2,Q7].

- O terceiro entrevistado gostava que deixassem esta lei ficar tal como está, o tempo suficiente até conseguir, determinar, com objetividade, se a mesma foi ou não eficaz. [E3,Q8]

Em suma, e como seria de esperar, é notória a riqueza de informação fornecida pelos entrevistados. Em certas questões, verifica-se que as opiniões divergem. Também é verdade, que essas divergências variam consoante as áreas profissionais de cada um. O cibercrime requer eficácia no seu combate. A LC

([16]) Disponível na WWW:
<URL: http://www.pgr.pt/Protocolos/PROTOCOLO-comunicacoes.pdf. >

oferece essa potencialidade. Como tal, justifica amplamente a sua existência. Esta questão nunca foi posta em causa pelos entrevistados. No entanto, não deixaram de referir que existem alguns pormenores passíveis de serem revistos ou até mesmo alterados.

Análise do estudo quantitativo

No seguimento do estudo quantitativo realizado, passa-se a descrever todos os resultados obtidos através da aplicação dos inquéritos por questionário, onde se tentou obter dos inquiridos, entre outras questões, a forma como protegem os seus computadores ou ainda o que acreditam ser o cibercrime, de entre alguns exemplos apresentados no inquérito. Considerou-se importante aferir a forma como encaram o referido fenómeno e também os seus atores. Perante isto, apresentar-se-á nas próximas páginas, o resultado estatístico de cada resposta, calculado através do programa estatístico SPSS 15.0 (*Statistical Package for the Social Sciences*). Num processo de análise estatístico, "o investigador depara-se sempre com ´algo` que precisa medir, controlar ou manipular durante o processo de investigação. Este `algo´ designa-se por `variável´. Neste estudo a variável é quantitativa, " *i.e.* variáveis cuja escala de medida permite a ordenação e quantificação de diferenças entre elas" (Maroco, 2007, p.27).

Quadro n.º 4 - Protege o computador

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	sim	63	96,9	96,9	96,9
	não	2	3,1	3,1	100,0
	Total	65	100,0	100,0	

Fonte: Recolha de dados - Inquéritos 2012

- À questão "protege o seu computador?", cujos resultados constam do quadro acima representado, 96,9 por cento responde que sim, o que corresponde à quase totalidade dos inquiridos. Apenas 2 inquiridos respondem que não protegem o seu computador. Os utilizadores devem

interiorizar que o antivírus protege o computador de ataques maliciosos, verificando os programas que instalam no computador, as páginas da Internet que consultam e os *emails* que recebem na caixa de correio eletrónico. O facto de não ter antivírus instalado e navegar na Internet, torna o computador vulnerável às ameaças existentes no ciberespaço.

- No quadro seguinte, é visível que essa proteção é feita, maioritariamente, através da utilização de programas antivírus, descarregados gratuitamente através da Internet, o que corresponde a 69,2 por cento dos inquiridos. Já 27,7 por cento compra programas para os mesmos fins numa loja ou na Internet. Dos 65 inquiridos, 2 não utilizam um programa antivírus. O seu preço de aquisição destes programas é ainda um pouco elevado, podendo ser uma condicionante no momento de os comprar.

Quadro n.º 5 - Como protege o computador

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Descarga gratuita de antivírus através da Internet	45	69,2	69,2	69,2
	Adquire antivírus numa loja ou via Internet	18	27,7	27,7	96,9
	Não utiliza antivírus	2	3,1	3,1	100,0
	Total	65	100,0	100,0	

Fonte: Recolha de dados - Inquéritos 2012

- No quadro a seguir representado, podemos verificar que 41,5 por cento dos inquiridos já teve problemas no computador, e 55,4 por cento diz não ter encontrado qualquer problema. Da totalidade dos inquiridos, 3,1 por cento respondeu não saber.

Quadro n.º 6 - Já teve problemas no computador

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	sim	27	41,5	41,5	41,5
	não	36	55,4	55,4	96,9
	não sabe	2	3,1	3,1	100,0
	Total	65	100,0	100,0	

Fonte: Recolha de dados - Inquéritos 2012

Os resultados verificados anteriormente vão de encontro a um estudo realizado em Portugal, promovido pelo portal de conteúdos *Microsoft System Network*[17], "sendo atribuído aos portugueses 44 pontos num total de 100 na Microsoft *Computing Safety Índex*, o mesmo valor que é conseguido pela média dos países europeus. Segundo este índice, os portugueses ainda têm muito que aprender para se protegerem das ameaças *online*, uma vez que os cibercriminosos estão cada vez mais sofisticados. Em comunicado, a empresa adianta que o estudo revela que 78 por cento dos cibernautas portugueses inquiridos possuem proteção de segurança *online* básica, mas estão mal informados sobre o que devem fazer para se proteger contra ameaças de cibercrime que assentam na fraude, tais como o *phishing*[18], roubo de identidade e ligações fraudulentas".

Quadro n.º 7 - Tipos de Problemas encontrados

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Trojan/Spyware	10	15,4	37,0	37,0
	Sistema operativo com problemas	4	6,2	14,8	51,9
	Bloqueio total do PC	3	4,6	11,1	63,0
	Perda de dados	2	3,1	7,4	70,4
	Dificuldades em aceder á Internet	2	3,1	7,4	77,8
	Phishing	3	4,6	11,1	88,9
	Diversos	2	3,1	7,4	96,3
	Não se recorda	1	1,5	3,7	100,0
	Total	27	41,5	100,0	
	Dados em falta	38	58,5		
Total		65	100,0		

Fonte: Recolha de dados - Inquéritos 2012

- Perante a questão do quadro anterior, a leitura dos dados indica que 15,4 por cento dos inquiridos detetou a presença de *trojan/spyware*[19] no

([17]) Disponível na WWW:
<URL: http://sol.sapo.pt/inicio/Tecnologia/Interior.aspx?content_id=40747>
([18]) Fraude informática na qual o criminoso se faz passar por uma instituição ou empresa para tentar persuadir (através de um mail), uma vítima a divulgar informação pessoal. Deste modo, o autor da fraude fica na posse das suas palavras-passe e números de contas bancárias.
([19]) São programas informáticos maliciosos - como os vírus ou os "cavalos de troia"- cujo objetivo é infiltrarem-se no sistema de um computador de qualquer pessoa para causar algum tipo de dano. Em

seu computador, 6,2 por cento encontrou problemas com o funcionamento do sistema operativo, 4,6 por cento diz ter sido vítima de *phishing* e 1 inquirido referiu não se recordar qual o tipo de problema encontrado.

- No quadro seguinte, verificam-se os dados resultantes da questão "Já foi vítima de cibercrime?", 72,3 por cento responde que não, enquanto 7,7 por cento responde que sim.

Quadro n.º 8 - Já foi vítima do cibercrime

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Sim	5	7,7	7,7	7,7
	Não	47	72,3	72,3	80,0
	Não sabe	13	20,0	20,0	100,0
	Total	65	100,0	100,0	

Fonte: Recolha de dados - Inquéritos 2012

- Como se pode verificar no quadro seguinte, dos 5 inquiridos, que dizem ter sido vítimas de cibercrime, nenhum apresentou queixa junto das autoridades. A descrença de que as autoridades possam vir a identificar os suspeitos de cibercrime, ou então pelo facto do cibercrime não ser valorizado, pode fazer com que não formalizem a respetiva queixa.

Quadro n.º 9 - Apresentou queixa junto das autoridades

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Não	5	100,0	100,0	100,0

Fonte: Recolha de dados - Inquéritos 2012

- Na questão, "o que é o cibercrime?", visível no quadro seguinte, o maior resultado evidencia-se na resposta "todos os exemplos mencionados" com, 53,8 por cento. Já 33,8 por cento diz tratar-se, apenas, de

ataques de '*phishing*', os '*malware*' termo geral para os identificar, destinam-se ao roubo de informações confidenciais da vítima. *Spyware* é um termo genérico para software escrito com a intenção de extração de dados.

subtração de códigos de acesso (passwords) e intrusão em sistemas alheios, enquanto 1 inquirido responde nenhum e outro não sabe.

Quadro n.º 10 - O que é o Cibercrime

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Descarga/Partilha de música/filmes/programas com direitos de autor da Internet	5	7,7	7,7	7,7
	Subtração de códigos de acesso (passwords) e intrusão em sistemas informáticos alheios	22	33,8	33,8	41,5
	Aceder através do computador e da Internet a canais de televisão (que carecem do pagamento de uma assinatura paga)	1	1,5	1,5	43,1
	Todos os exemplos referidos	35	53,8	53,8	96,9
	Nenhum	1	1,5	1,5	98,5
	Não sabe	1	1,5	1,5	100,0

Fonte: Recolha de dados - Inquéritos 2012

- À questão, "conhece alguém que já tenha praticado, de qualquer forma, algum cibercrime?", 72,3 por cento dos inquiridos respondeu que não, contra 27,7 por cento que dizem conhecer quem já tenha praticado.

Quadro n.º 11 - Conhece alguém que já tenha praticado, de qualquer forma algum cibercrime

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Sim	18	27,7	27,7	27,7
	Não	47	72,3	72,3	100,0
	Total	65	100,0	100,0	

Fonte: Recolha de dados - Inquéritos 2012

- Relativamente ao grau de perigosidade percecionado pelos inquiridos acerca dos cibercriminosos, constata-se que, 72,3 por cento acredita que a perigosidade é grande, e 4,6 por cento que os cibercriminosos não representam qualquer perigo.

Quadro n.º 12 - Grau de perigosidade dos cibercriminosos

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Fraco	3	4,6	4,6	4,6
	Médio	12	18,5	18,5	23,1
	Grande	47	72,3	72,3	95,4
	Nenhum	3	4,6	4,6	100,0
	Total	65	100,0	100,0	

Fonte: Recolha de dados - Inquéritos 2012

- No quadro n.º 13 constam os resultados obtidos com a questão " Já praticou algum ato que se possa enquadrar nas práticas cibercriminosas?", 78,5 por cento dos inquiridos diz nunca ter praticado qualquer ato que se possa enquadrar nas práticas cibercriminosas, enquanto 21,5 por cento respondeu que sim.

Quadro n. 13 - Já praticou algum ato que se possa enquadrar nas práticas cibercriminosas

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Sim	14	21,5	21,5	21,5
	Não	51	78,5	78,5	100,0
	Total	65	100,0	100,0	

Fonte: Recolha de dados - Inquéritos 2012

- Quanto ao tipo de cibercrime praticado, sobressai no quadro que se segue, a descarga de filmes/música/programas com 78,6 por cento. Os resultados obtidos neste quadro refletem, amplamente, aquilo que foi referido no início deste estudo, quanto à ausência de controlo ao nível social que o internauta sente, e que o pode levar à prática de comportamentos ilícitos. Verifica-se ainda que, um dos inquiridos afirma ter-se introduzido em rede *wireless* protegida. Este acesso ilegítimo é um

tipo de crime que segundo Santos, Bessa e Pimentel "levanta algumas questões, pelo facto de muitas vezes o cibercriminoso apenas se sentir motivado em ter acesso a um sistema informático, para testar a sua segurança (…) não actuando com intenção de alcançar para si ou para outrem, um benefício ou vantagem ilegítimos" (Santos, *et* al, 2008, p. 15 e 16).

Quadro n.º 14 - Tipos de Cibercrime praticados

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Descarga filmes/musicas/ programas	11	78,6	78,6	78,6
	Intrusão em rede *wireless* protegida	1	7,1	7,1	85,7
	Acesso a tv paga	2	14,3	14,3	100,0
	Total	14	100,0	100,0	

Fonte: Recolha de dados - Inquéritos 2012

- À questão correspondente ao quadro n.º 15, 61,5 por cento dos inquiridos refere não estar devidamente informado acerca do cibercrime, e 38,5 por cento acreditam que estão.

Quadro n. º 15 - Crê estar devidamente informado acerca do cibercrime

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Sim	25	38,5	38,5	38,5
	Não	40	61,5	61,5	100,0
	Total	65	100,0	100,0	

Fonte: Recolha de dados - Inquéritos 2012

- Por último, podem ser observados no quadro seguinte, os resultados à questão "Sabia da existência da LC em Portugal?", onde 52,3 por cento respondeu que sabia, e 47,7 por cento respondeu que desconhecia.

Quadro n.º 16 - Sabia da existência da LC

		Frequência	Percentagem	Percentual Válido	Percentagem cumulativa
Válido	Sim	34	52,3	52,3	52,3
	Não	31	47,7	47,7	100,0
	Total	65	100,0	100,0	

Fonte: Recolha de dados - Inquéritos 2012

A informação fornecida pelos 65 inquiridos revelou-se essencial para se ter uma noção acerca da imagem social do cibercrime e, da forma como cada utilizador protege os seus computadores, verificando-se neste último caso que apesar dos problemas que possam vir a provocar, ainda existe quem não o faça. O facto de descarregar/partilhar na Internet conteúdos protegidos pelos direitos de autor não é considerado, para alguns inquiridos, uma prática criminosa. Já outros acreditam que o cibercrime só engloba a subtração de códigos de acesso e a intrusão em sistemas informáticos alheios. Estes resultados indiciam uma falta de conhecimento real sobre o que é o cibercrime verificando-se que 61,5 por cento dos inquiridos referem estar mal informado acerca deste fenómeno. Tivemos ainda a possibilidade de verificar, com este inquérito, que os inquiridos que revelaram ter sido vítimas deste fenómeno, não o denunciaram às autoridades.

Internet: um novo palco para a prática de crimes

Inicialmente era denominada ARPANET, e foi desenvolvida pela agência ARPA (*Advanced Research Projects Agency*). Os seus pressupostos embrionários, foram criados em 1969, fundados pelo Departamento de Defesa dos EUA. A sua construção justificou-se, na época, "como um meio de repartir o tempo de trabalho *on-line* dos computadores entre os vários centros de informática interativa e grupos de investigação" da ARPA (Castells, 2007, p.26). Alguns autores defendem que o principal objetivo da existência da ARPANET era "a sobrevivência de um meio de comunicação, mesmo após a ocorrência de uma guerra nuclear" (Sousa, 1999, p. 1). Outros afirmavam que as suas aplicações militares foram secundárias no seu projeto tecnológico porém, Castells não tem dúvidas que "o projeto tinha uma orientação claramente militar" (Castells, 2007, p.34). Em 1990, Tim Berners-Lee[20], criou em colaboração com Robert Cailliau[21], uma aplicação para a partilha de informação que chamaram *world*

([20]) Físico britânico, cientista da computação e professor do MIT. É o criador da *World Wide Web*, tendo feito a primeira proposta para sua criação em Março de 1989.
([21]) Informático belga foi um dos pesquisadores do CERN que desenvolveu o conceito da *World Wide Web.*

wide web. O objetivo era de ligar entre si, diversas fontes de informação através de um sistema interativo de computação (Castells, 2007). “Apesar da Internet estar na mente dos informáticos desde os princípios dos anos 60, e de se ter estabelecido em 1969, uma rede de comunicações entre computadores e, desde final dos anos 70, se terem formado várias comunidades interativas de cientistas e *hackers*, quer para as pessoas, quer para as empresas e sociedade em geral, a Internet viria a nascer em 1995” (Castells, 2007, p. 33). Vinton Cerf foi, conjuntamente com Robert Kanh, um dos seus fundadores. Ambos são responsáveis pela criação do protocolo TCP/IP[22], que sustenta a conexão em rede. A Internet expandiu-se de tal forma que até 1999, o número de países ligados à rede aumentou de 83 para 226. A maioria, cerca de 95 por cento, era repartida entre os Estados Unidos, Canadá, Europa, Austrália e Japão (Yar, 2006). Portugal não fugiu a essa tendência ascendente.

Na figura n.º 1, visível na página seguinte, verifica-se que o número de utilizadores de Internet em Portugal, quase que duplicou entre o ano de 2003 e 2008, registando um aumento anual de utilizadores na ordem dos 10,9 por cento. Os números publicados apontam ainda que, por cada 100 habitantes, Portugal transpôs a média de 25,65 utilizadores verificados em 2003 para os 41,92 utilizadores em 2008. Apesar da tendência ascendente do número de utilizadores da Internet, um estudo publicado pelo Observatório das Desigualdades (cfr. figura n.º 2, p. 47), indica que Portugal permanecia ainda, em 2008, abaixo da média da União Europeia. Um estudo da Comissão Europeia (CE), divulgado em Junho de 2012, revela que cerca de metade da população portuguesa acede à Internet com regularidade. A análise, que faz parte da avaliação anual do *Digital Agenda Scoreboard*, relatório que apresenta o desempenho dos países da CE no uso das tecnologias de informação e comunicação, revela que, no ano de 2011, 51 por cento dos portugueses utilizaram com frequência a Internet. Portugal registou um aumento de 4 por cento em relação a 2010, contudo, o país encontra-se ainda abaixo da média

([22]) TCP *(Transmission Control Protocol)* e IP *(Inter-net-work Protocol)* são o standard sobre o qual opera a Internet.

europeia, a qual se situa, atualmente, nos 68 por cento[23]. Para se verificar um aumento da taxa de utilização da Internet em Portugal, os preços praticados pelos operadores devem continuar a baixar.

Figura n. º 1 – Utilizadores de Internet na Europa, e número de utilizadores para cada 100 habitantes entre o ano de 2003 e 2008

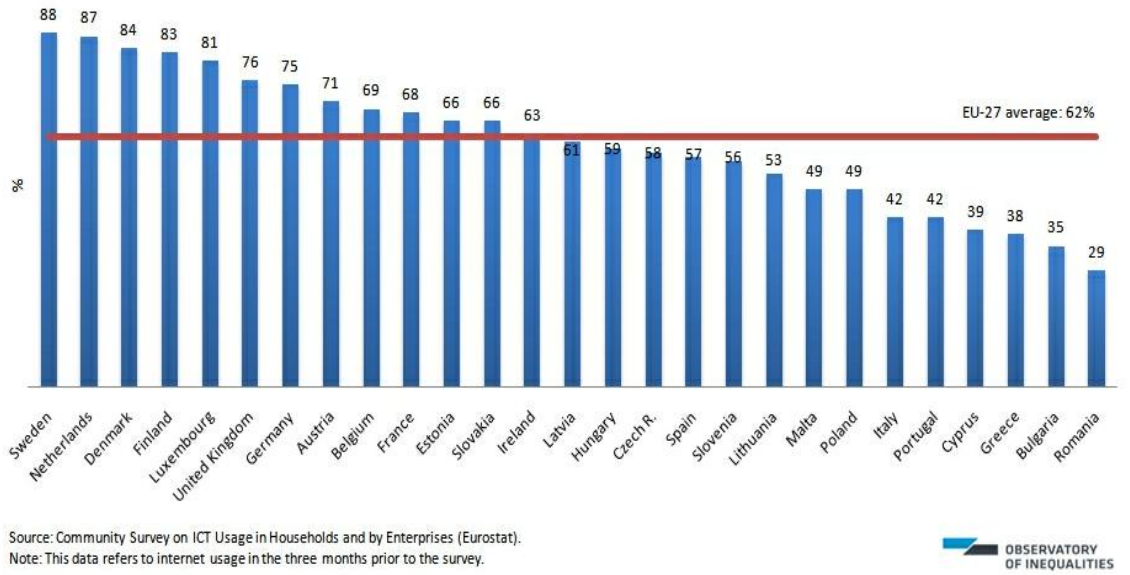
		Internet users (000s)		CAGR (%)	Internet users per 100 inhabitants		CAGR (%)
		2003	2008	2003-2008	2003	2008	2003-2008
1	Albania	30	750	90.4	0.97	23.86	89.7
2	Andorra	10	59.1	42.5	13.55	70.04	38.9
3	Austria	3'337.30	5'936.70	12.2	41.02	71.21	11.7
4	Belgium	5'153.00	7'292.30	7.2	49.97	68.86	6.6
5	Bosnia and Herze-govina	150	1'307.60	54.2	3.97	34.66	54.3
6	Bulgaria	944.3	2'647.10	22.9	12.04	34.86	23.7
7	Croatia	1'014.00	1'879.60	13.1	22.75	42.5	13.3
8	Cyprus	245.8	334.4	6.3	30.09	38.78	5.2
9	Czech Republic	2'849.30	6'027.70	16.2	27.99	58.41	15.9
10	Denmark	3'822.00	4'578.60	3.7	70.94	83.89	3.4
11	Estonia	613.1	888.1	7.7	45.32	66.21	7.9
12	Finland	3'436.50	4'382.70	5	65.93	82.62	4.6
13	France	21'765.00	42'315.40	14.2	36.14	68.21	13.5
14	Germany	44'191.20	61'973.10	7	53.68	75.33	7
15	Greece	1'791.40	4'253.40	18.9	16.25	38.19	18.6
16	Hungary	2'190.70	5'873.10	21.8	21.63	58.66	22.1
17	Iceland	233.9	285.7	4.1	81.19	90.56	2.2
18	Ireland	1'229.20	2'774.90	17.7	30.57	62.54	15.4
19	Israel	1'264.50	3'500.00	22.6	19.59	49.64	20.4
20	Italy	16'524.80	24'991.50	8.6	28.53	41.93	8
21	Latvia	626.2	1'369.60	16.9	26.98	60.63	17.6
22	Liechtenstein	20	23	2.8	58.81	64.55	1.9
23	Lithuania	844.4	1'761.90	15.8	24.45	53.05	16.8
24	Luxembourg	239.3	387	10.1	52.8	80.53	8.8
25	Malta	125.7	198.8	9.6	31.64	48.79	9
26	Monaco	16	22	6.6	49.49	67.25	6.3
27	Montenegro	-	294	...	...	47.24	...
28	Netherlands	10'400.70	14'304.60	6.6	64.35	86.55	6.1
29	Norway	3'411.60	4'235.80	4.4	74.7	88.86	3.5
30	Poland	9'522.00	18'679.10	14.4	24.87	49.02	14.5
31	Portugal	2'673.20	4'475.70	10.9	25.65	41.92	10.3
32	Romania	1'941.90	6'132.20	25.9	8.9	28.71	26.4
33	San Marino	14.5	17	3.3	50	54.52	1.7
34	Serbia	-	3'300.00	...	...	33.54	...
35	Slovak Republic	2'316.60	3'566.50	9	43.04	66.05	8.9
36	Slovenia	635.2	1'125.70	12.1	31.85	55.86	11.9
37	Spain	15'338.40	25'240.00	10.5	36.63	56.74	9.1
38	Sweden	6'890.70	8'085.50	3.2	76.82	87.84	2.7
39	Switzerland	4'696.80	5'739.30	4.1	64	76.1	3.5
40	TFYR Macedonia	386.8	847.9	17	19.07	41.54	16.8
41	Turkey	8'550.30	25'405.40	24.3	12.33	34.37	22.8
42	United Kingdom	36'291.80	46'683.90	5.2	60.82	76.24	4.6
	Europe	215'738.20	353'946.00	10.2	36.72	57.8	9.7

** (CAGR) Compounded Annual Growth rate*

Fonte: ITU World Telecommunication/ICT Indicators Database <URL: http://www.itu.int/ >

([23]) Disponível na WWW:
<URL: http://www.jornaldigital.com/noticias.php?noticia=31188 .>

Figura n.º 2 – Utilização da Internet em Portugal e média dos 27 países da União Europeia no ano de 2008



Fonte: Observatório das desigualdades URL:<[*http://observatorio-das-desigualdades.cies.iscte.pt/index.jsp?page=indicators&id=186&lang=en*](http://observatorio-das-desigualdades.cies.iscte.pt/index.jsp?page=indicators&id=186&lang=en)

A Internet expandiu-se por todo o mundo, sendo hoje "uma rede internacional/global de computadores interligados que permite às pessoas de todo o Mundo comunicarem entre si no ambiente cibernético, na qual circulam grandes quantidades de informações provenientes de todo o mundo e às quais acedem milhões de pessoas, desde que se liguem à rede[24]". "Criada como um meio para a liberdade, nos primeiros anos da sua existência global, a Internet parecia pressagiar uma nova era de libertação (…). A liberdade de expressão podia estender-se por todo o planeta sem depender dos meios de comunicação de massas, já que a internet permitia a comunicação de muitos para muitos sem entraves. A propriedade intelectual (da música, das publicações, das ideias, da tecnologia e do software) devia ser partilhada já que, quando estas criações estavam na Rede, não havia maneira de limitar a sua difusão. A

([24]) *In* Subjudice/índex 35, Documento de trabalho de 21 de Novembro de 2000 " Privacidade na Internet – Uma Abordagem Integrada na U.E. no domínio da proteção de dados em linha, emanado do Órgão Consultivo Independente da União Europeia, no domínio da Proteção de Dados Pessoais, criado pelo artigo 29.º da Diretiva 95/46/CE, do Parlamento e do Conselho, de 26 de Outubro de 1995, *cit.* CAMPOS, Eduardo, 2003.

privacidade estava protegida pelo anonimato da comunicação na Internet (…)" (Castells, 2007, p. 201).

Apesar dos benefícios conferidos a toda uma sociedade, a Internet não escapou às atividades criminais. Castells referiu que "os governos de todo o mundo levaram a sério a ameaça a que os mesmos chamaram `cibercrime´. Tornara-se claro que a infraestrutura de comunicações informáticas da qual dependiam a riqueza, a informação e o poder no nosso mundo era muito vulnerável à intrusão, à interferência e à disrupção" (Castells, 2007, p. 210). Segundo Wall, "*the Internet can be seen to have impacted upon human activities in three main ways. First, it has acted as a vehicle for the further facilitation of existing criminal activities. Second, it has created new opportunities for existing types of crimes; and third, it has facilitated the creation of entirely new types of activity which are largely free of traditional and terrestrial constraints"* (Wall, 2000, p.168). Indo de encontro à opinião de Castells quando refere que "a Internet é o tecido das nossas vidas", não podemos olvidar que existe um lado obscuro inerente à sua utilização, e Sousa (1999) refere que a Internet é "crescentemente palco de atividades criminais. As suas potencialidades são facas de dois gumes. Elas tanto podem ser utilizadas para fins legais, como ilegais" (Sousa, 1999, p.75).

Para Santos, Bessa e Pimentel, "a internet (…) permite veicular todo o género de situações existentes na sociedade real, mas com diferenças significativas ao nível da velocidade, tempo, diversidade e quantidade de acontecimentos (…)", referem ainda que a internet "é extremamente propiciadora a todo o género de práticas delitivas" (Santos, *et al*., 2008, p. 5). Refira-se, que a este propósito, Wall, refere-se aos crimes veiculados pela Internet e que suportam a criminalidade tradicional tais como o tráfico de estupefacientes ou o *stalking*[25], referindo também, que "*the internet has created a transnational environment that provides new opportunities for harmful activities that are currently the*

([25]) Comportamentos persistentes que instauram apreensão e medo (Santos, Bessa e Pimentel, 2008, p. 18)

subject of existing criminal or civil law. Examples would include paedophile activity, and also fraud" (Wall, 2000, p. 3).

Castells indica também que a Internet está cheia de "implacáveis ondas de vírus e *worms*, os *crackers* atravessam *firewall* e roubam números de cartões de crédito, os ativistas políticos desativam e alteram os sítios web, os arquivos de alguns computadores militares circulam por todo o mundo e conseguiu-se extrair software confidencial da própria rede interna da Microsoft" (Castells, 2007, p. 210). Sem a existência da Internet, os crimes que hoje são cometidos na rede não existiriam tal como são conhecidos. Nesse sentido, Yar refere que "*whether the internet plays a merely `contingent ´ role in the crime (it could be done without it, using other means), or if is it absolutely `necessary´ (without the Internet, no such crime could exist)"* (Yar, 2006, p. 10).

O presidente da Google, Eric Schmidt, alertou para o facto da Internet ter sido concebida, sem que tivessem em mente que a criminalidade a poderia afetar, e em consequência, deverá estar altamente vulnerável durante pelo menos os próximos dez anos. Acrescentou ainda que, o "cibercrime, especialmente aquele desenvolvido em países que não o controlam ou o promovam, representa um dos maiores perigos atuais para a Internet[26]".A opinião de Schmidt acerca da vulnerabilidade da Internet vai de encontro à opinião de dois especialistas portugueses, um da área da investigação criminal e o outro da esfera do direito. Ambos referem que "o cidadão médio português utilizador da Internet não está preparado para se proteger, nem a utilização que faz daquela rede é norteada por cuidados e princípios de segurança informática. Este tipo de utilizador não salvaguarda os seus dados pessoais, tem tendência a acreditar no que lê publicado na Internet e assume uma atitude passiva e resignada mesmo quando constata que a sua esfera de intimidade foi invadida (…) " (Costa e Bravo, 2005, p. 22).

([26]) Disponível na WWW:
<URL: http://expresso.sapo.pt/google-alerta-para-o-cibercrime-e-a-censura=f728282>

Ainda assim, apesar de todas as contrariedades que a Internet possa fomentar, recorre-se mais uma vez à opinião de Castells, quando o próprio refuta a ideia de que as redes informáticas possam ser consideradas inseguras, o que Castells assegura é que falta dominar a Internet. “A ideia de que as redes possam ser inseguras é literalmente insustentável para os poderes de facto, reais, do nosso mundo: tudo depende destas redes e o controlo das ditas redes é um princípio essencial para conseguir manter o domínio” (Castells, 2007, p. 211).

Todos os ilícitos praticados na Internet têm um único objetivo - o benefício financeiro que conferem. Em Janeiro de 2011, a EUROPOL, apresentou em Hague, uma avaliação da ameaça na utilização da Internet - *Internet Facilitated Organised Crime.* Nesse relatório, entre outros assuntos relacionados com o cibercrime, é focada a dimensão da *digital underground economy* que o cibercrime fornece. Todos os dados pessoais obtidos ilicitamente, quer sejam informações relativas a dados bancários ou a dados de identificação das vítimas, alcançam um valor de venda elevado no mercado paralelo. O mesmo estudo revela que, o valor da economia que envolve o mundo do cibercrime não é conhecido, porém uma recente estimativa da empresa McAfee aponta o valor de 1 trilião de dólares por ano, como quantia indicativa relacionada com as perdas globais das empresas em todo o mundo[27].

A Conferência do Conselho da Europa - *Cooperation against Cybercrime*[28] - decorrida entre os dias 6 e 8 de Junho de 2012 em Strasbourg, França, apontou em jeito de resumo inicial, a existência atual de mais de 2,3 mil milhões de utilizadores de Internet em todo o mundo, a deteção diária de duas mil páginas de Internet onde são dissimulados *malware* ou programas que

([27]) Disponível na WWW:
<URL: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf >.
([28]) Disponível na WWW:
<URL:http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus2012/Interface2012_en.asp >.

possibilitam esquemas de *phishing*. Existe uma contaminação diária de 3 milhões de computadores, devido aos comportamentos ilícitos.

Perante isto, "é hoje claro que a Internet é um meio fácil para cometer alguns tipos de crimes. Sob o signo do duplo anonimato decorrente, por um lado, da possibilidade garantida pela Internet e, por outro, da falta de controlo dos locais de acesso livre às redes de comunicação (a título de exemplo: cyber-cafés), é hoje possível efetuar um vastíssimo conjunto de atos ilícitos com uma enorme potenciação danosa" (Lopes & Cabreiro, 2006, *in* Sub Judice Internet, Direito e Tribunais n.º 35, p. 79).

O Cibercrime em Portugal

Como tem vindo a ser referido ao longo do presente estudo, também Portugal, a par dos restantes países mundiais, não tem escapado à onda crescente do cibercrime. A informação fornecida, publicamente, por Baltazar Rodrigues, do grupo técnico de informática forense da Polícia Judiciária[29], aponta para um aumento sucessivo das queixas de cibercrime. Verifica-se no RASI de 2009, uma variação positiva do crime de burla informática e nas comunicações, quando comparado com os dados de 2008, o que equivale a mais de 650 incidências criminais ou seja um aumento percentual de 70,3 por cento. A tendência ascendente deste tipo de criminalidade é, mais uma vez, confirmada pelos RASI de 2010 e de 2011, onde se volta a constatar uma variação positiva de mais 540 incidências criminais no ano de 2009 e mais 580 em 2010, correspondendo neste último ano, a um aumento percentual de 27,4 por cento, comparativamente ao ano anterior.

([29]) Disponível na WWW:
<URL: http://www.computerworld.com.pt/2010/03/15/decorrem-1227-investigacoes-de-cibercrime-na-policia-judiciaria/>.

Os ataques cibercriminosos ocorridos em território português são classificados por John Austen[30] como relativamente simples, apesar de não deverem ser subestimados. Austen refere a importância das autoridades nacionais darem especial atenção a este fenómeno e, a necessidade de terem meios e recursos que permitem enfrentar o problema. Numa entrevista concedida em Dezembro de 2011, o especialista em combate ao cibercrime mencionou a novidade dos ataques acontecidos em Portugal, contudo frisou que não o são nos restantes países do mundo, daí a importância de serem adotadas, nestes casos, todas as medidas preventivas necessárias, com a finalidade de evitá-los. Essas medidas, passam, por exemplo, pela atualização dos *softwares* informáticos, nomeadamente a atualização dos pacotes de segurança, logo que sejam disponibilizados e, também pela importância de se efetuarem vigilâncias às bases de dados constantes nos sistemas informatizados. Destaca-se dessa entrevista, a constante focagem à importância dos recursos disponíveis para este tipo de investigações. O especialista em combate ao cibercrime, enaltece aliás, as competências da unidade existente em Portugal especializada no combate ao crime informático e reafirma no seu discurso que "tudo depende dos recursos e de quanto tempo lhes são dados para poderem fazer o seu trabalho". Refere nesse sentido que "o fator número um não é saber se podemos apanhar ou não os piratas informáticos[31]".

Relativamente aos meios colocados ao dispor das autoridades portuguesas no combate ao cibercrime, a Diretora do Departamento de Investigação Ação Penal (DIAP) de Lisboa, Maria José Morgado, realçou, após a sessão de apresentação de uma formação sobre cibercriminalidade para investigadores portugueses[32], que o nível de preparação das autoridades portuguesas é bom,

([30]) AUSTEN, Jonh, fundador da Unidade de Combate ao Crime Informático na Scotland Yard. Especialista em combate ao cibercrime, em técnicas de investigação, legislação internacional e em segurança organizacional. Foi responsável pelas detenções de hackers e de grupos de crime informático organizado.
([31]) Disponível na WWW:
<URL:http://www.público.pt/Sociedade/ataques-de-piratas-informáticos-portugal-sao-simples-mas-alertam-para-o-problema-diz-especialista-1525401>.
([32]) Formação ministrada pela norte-americana *ICE – Immigration Customs Enforcement – Homeland Security.*

porém, a questão é sempre política na atribuição dos meios proporcionais, sendo da sua opinião uma maior atribuição de meios à investigação criminal, referindo ainda que Portugal tem "algum equipamento e alguns meios, embora haja desproporção entre os meios e as ameaças[33]".

As ações levadas a cabo pelos cibercriminosos em Portugal concentram-se, essencialmente, em tornar indisponíveis, de forma temporária, determinadas páginas da Internet[34]. Porém, a forma de cibercrime mais comum em Portugal é o *phishing*. Já em 2010, durante uma apresentação do relatório anual da empresa de segurança Symantec sobre o cibercrime, o Inspetor-Chefe da Polícia Judiciária, Rogério Bravo, partilhou a mesma informação, referindo-se também à pornografia infantil que surge em segundo lugar na lista dos crimes mais cometidos em Portugal e ao *hacking,* que surge em terceiro[35]. No que diz respeito à pornografia infantil através da Internet, acaba de ser adotada a Diretiva 2011/92/EU de 13 de Dezembro de 2011, que veio substituir a Decisão-Quadro 2004/68/JAI no que diz respeito aos Estados-Membros que participam na adoção da referida diretiva.

Existem centenas de esquemas que permitem aos cibercriminosos obter os dados das suas vítimas através da Internet. Numa conferência onde fora apresentado o Relatório Norton de Cibercrime de 2011, o Inspetor Francisco Luís, investigador da secção de Investigação de Criminalidade Informática e Tecnológica da Policia Judiciária[36], referiu que uma das técnicas utilizadas para obter esses dados, passa pelo envio de mensagens de correio eletrónico falso com o objetivo de obter dados bancários secretos. O *modus operandi* atualmente mais utilizado, é a criação de páginas em tudo semelhantes às

(33) Disponível na WWW:
<URL:http://www.publico.pt/Tecnologia/maria-jose-morgado-diz-que-cibercrime-tem-de-ser-prioridade-politica-1524736>.
(34) Disponível na WWW:
<URL:http://www.ionline.pt/portugal/crimes-informáticos-so-5-dos-inquerios-resultaram-acusacao>.
(35) Disponível na WWW:
<URL:http://www1.ionline.pt/conteudo/83163-processos-crime-informatico-quase-duplicam-em-2010>.
(36) Disponível na WWW:
<URL:http://www.cmjornal.xl.pt/detalhe/noticias/nacional/economia/phishing-e-o-crime-informatico-mais-comum-em-portugal >.

páginas dos bancos, ou de sistemas de pagamento em linha como as contas de *Pay-Pal*. Segundo o investigador Francisco Luís, os ataques são, atualmente, ao contrário do que se verificava há uns anos, dirigidos a mais pessoas, e os valores envolvidos são menores. Realçou ainda, que a realidade portuguesa é vítima de ataques oriundos do Brasil e dos países do leste Europeu, sobretudo da Rússia. Da totalidade dos casos de cibercrime identificados em Portugal, 75 por cento dizem respeito ao *phishing*. Seguem-se, por ordem, os casos de acesso ilegítimo, dano informático, pornografia de crianças, *software* ilegal e sabotagem. Em 2010, o *phishing* causou, em Portugal, dois milhões de euros de prejuízos, sendo que 20% dos queixosos eram pessoas coletivas[37].

Os resultados apresentados pelas diversas empresas privadas (McAfee, Symantec) e também pelos RASI demonstram que a regulamentação e as normas criadas em Portugal para enfrentar o cibercrime não têm, até ao momento, contribuído para a diminuição deste fenómeno. Opinião contrária tem o terceiro entrevistado que, sobre este assunto, referiu que é ainda muito cedo para tirar conclusões nesse ponto particular [E3, Q8].

No primeiro semestre de 2012, a Polícia de Segurança Pública (PSP) tem vindo a registar diversas tentativas de burla através do esquema de *phishing*. Para o efeito, é utilizado o logótipo da instituição em mensagens fraudulentas, que, posteriormente são enviadas para as caixas de correio eletrónico dos cibernautas ou então disseminadas através de um vírus informático. Todas essas notificações fictícias, qualquer que seja a forma de disseminação, contêm instruções para o pagamento de multas, por suposta violação da lei de "direitos de autor e direitos adjacentes" e/ou por divulgação de "conteúdos pornográficos proibidos", impedindo, nalguns casos, a continuação da utilização do computador devido a um bloqueio que impede de utilizar corretamente o sistema operativo da máquina. Nos comunicados de imprensa

(37) Disponível na WWW:
<URL:http://www1.ionline.pt/conteudo/76414-mafias-actuam-em-portugal-branquear-dinheiro>.

efetuados pela PSP, a instituição alerta para a especial atenção dos cidadãos nestes casos, pois "para além de conterem uma identificação gráfica mais credível e cuidada, possuem ainda indicadores que induzem os utilizadores em erro, levando-os a acreditar no conteúdo da mensagem. Para além de acederem a esta informação, os utilizadores são ainda intimados a procederem a um pagamento de cerca de 100€ por NIB para evitarem o bloqueio do computador[38]" *(ver anexo p. 92)*.

Esta forma de informar os utilizadores, para os riscos passíveis de serem encontrados, por quem navega na Internet, vai de encontro a uma das soluções apresentadas pelo Procurador da República Pedro Verdelho, que numa entrevista concedida publicamente, explica que as respostas para combater o problema do cibercrime passam "pela informação dos utilizadores" e pela "formação contínua dos profissionais que investigam nesta área". Segundo refere, os chamados crimes convencionais, não requerem dos profissionais a mesma necessidade de atualização de que necessitam aqueles que são responsáveis pela investigação do cibercrime[39].

Em jeito de resposta à falta de meios evocados pela magistrada Maria José Morgado, o Ministério da Justiça Português divulgou que irá avançar com a criação de uma nova estrutura para o combate ao cibercrime. Esta notícia foi avançada pelo Jornal de Notícias em Abril de 2012 e, segundo fonte judicial, indica que essa nova estrutura irá funcionar de uma forma semelhante às unidades de Combate ao Terrorismo ou ao Combate ao Tráfico de Estupefacientes da Polícia Judiciária, e que irá contar com mais inspetores, mais meios e maior capacidade para combater o crime informático[40].
Com a entrada em vigor da LC, as comunidades educativas e científicas viram-se impossibilitadas, de forma legal, de poder desenvolver programas

([38]) Disponível na WWW:
<URL:http://www.psp.pt/Pages/Noticias/MostraNoticia.aspx?NoticiasID=728>.
([39]) Disponível na WWW:
<URL:http://www1.ionline.pt/conteudo/76414-mafias-actuam-em-portugal-branquear-dinheiro>.
([40]) Disponível na WWW:
<URL:http://www.asjp.pt/2012/04/03/judiciaria-cria-unidade-especial-para-investigar-cibercrime/>.

informáticos no campo da segurança. O UbiNET, Laboratório de Segurança Informática e Cibercrime do Instituto Politécnico de Beja, desenvolveu um laboratório de *hacking* virtual desenvolvido para instituições e empresas. Como explica José Caeiro do Laboratório UbiNET, "o HackLab é uma plataforma onde se pode estudar o ataque a sistemas num ambiente controlado sem as restrições legais que existem em ambientes reais[41]". Este laboratório encontra-se acessível a partir de qualquer parte do mundo e, após aceder à plataforma, o utilizador poderá assistir a vídeos que explicam a estrutura da aplicação e criar um cenário real num ambiente virtual.

Em 7 de Fevereiro de 2012, a Resolução do Conselho de Ministros n.º 12/2012, de 7 de Fevereiro[42], aprovou a constituição da Comissão Instaladora do Centro Nacional de Cibersegurança para que sejam definidas as medidas e os instrumentos necessários à criação, instalação e operacionalização de um Centro Nacional de Cibersegurança, em Portugal. Segundo Rui Miguel Silva, do laboratório UbiNET, a criação do referido Centro "poderá ter algum impacto na preparação de Portugal para os ataques vindo do exterior[43]".

Ainda como forma de resposta ao cibercrime foi criado, por Despacho do Procurador-Geral da República de 7 de Dezembro de 2011, o Gabinete de Coordenação da Atividade do Ministério Público na área da Cibercriminalidade (Gabinete do Cibercrime). A sua coordenação está a cargo do Procurador da República, Pedro Verdelho, coadjuvado pela Procuradora-Adjunta Patrícia Naré Agostinho. O referido Gabinete tem como propósitos "a coordenação, a formação específica de magistrados do Ministério Público, a interação com o sector privado e os órgãos de polícia criminal e, residualmente, o acompanhamento de processos concretos (…) é propósito do Gabinete Cibercrime estabelecer contactos com entidades terceiras que permitam

([41]) Disponível na WWW:
<URL http://sicnoticias.sapo.pt/programas/falarglobal/article1363300.ece
([42]) Disponível na WWW:
<URL http://www.inst-informatica.pt/documentos/rcm-12-2012
([43]) Disponível na WWW:
<URL http://sicnoticias.sapo.pt/programas/falarglobal/article1363300.ece

assegurar uma colaboração funcional rápida e eficaz com a investigação criminal, bem como criar canais expeditos de comunicação com entidades responsáveis pela segurança informática, de modo a assegurar pronta capacidade de resposta quando forem solicitadas a cumprir as suas legais atribuições". A proposta do Gabinete Cibercrime é "desenvolver canais específicos ou rotinas específicas para processos envolvendo o cibercrime, de modo a tornar mais eficaz e expedita a ação nesta área e promover o relacionamento dos órgãos de polícia criminal com entidades terceiras, no âmbito de diligências de inquérito[44]".

É frequente ouvir falar em Hacktivismo. O termo foi criado em 1996 pelo *Cult of the Dead Cow*. Tem sido, sem dúvida, uma das atividades com maior impacto mediático. O Hacktivismo, é a junção da palavra *hack* e ativismo e tem como finalidade a promoção de ideais políticos através da utilização das capacidades informáticas dos seus membros. Em Portugal, esta forma de criminalidade é praticada pelos LulzSec, grupo que define os seus membros de autodidatas descontentes com as medidas do Governo e com a corrupção em geral e ainda pelos Anonymous Portugal. Ambos os grupos partilham dos mesmos ideais. Os ataques efetuados por estes visam sítios web governamentais ou de empresas privadas, impossibilitando o acesso aos mesmos por períodos de tempo indeterminado, costumando, também, substituir as páginas web de origem por mensagens que consideram ideológicas. De forma resumida, podemos referir que no hacktivismo são "fundamentalmente utilizados quatro tipos de ações de *hacking*, sendo eles: Virtual *sit-ins e Blockades*[45], *Mail Bomb*[46], Ataques *web*, Vírus Informáticos e *worms*" (Santos *et* al. 2008, p. 81) *(ver anexo p.93)*.

([44]) Disponível na WWW:
<URL http://cibercrime.pgr.pt/>.
([45]) "É a transposição das formas de bloqueio existentes no mundo físico para o ciberespaço" *in* Santos *et* al. 2008, p. 81
([46]) "Mail Bom consiste no envio massivo de e-mails, com a intenção de ocupar toda a capacidade de armazenamento e de distribuição de uma simples caixa de correio, ou até mesmo de um servidor de *e-mail*, de modo a torna-los disfuncionais" *in* Santos *et* al. 2008, p. 81.

As Botnets, como define a *European Network and Information Security Agency*, são "*a concept of advanced malicious software that incorporates usually one or more aspects of the aforementioned techniques introduced by viruses, worms, Trojan horses and rootkits for propagation and hostile integration into a foreign system, providing the functionality of the compromises system to the attacker*[47]" Também apelidada de rede zombie, os botnet são uma rede composta por "computadores infectados por software malicioso que permite aos cibercriminosos controlar as máquinas infectadas remotamente sem o conhecimento dos utilizadores. Os computadores infectados são controlados através do centro de controlo e comando da botnet, que se une aos bots via canais IRC, conexões web ou qualquer outro meio disponível. Para que uma botnet comece a fazer dinheiro para o seu criador, é suficiente organizar algumas dúzias de máquinas em rede. A receita gerada por uma botnet é directamente proporcional à sua estabilidade e à sua taxa de crescimento (…) Novos sites de phishing são agora produzidos em massa pelos cibercriminosos, com botnets a protegerem os sites contra o encerramento. As redes zombi fornecem tecnologia de fluxo rápido, que permite aos cibercriminosos modificarem os endereços IP do website a cada minuto sem afectar o nome de domínio. Isto prolonga a vida de sites phishing, tornando muito difícil descobri-los e pô-los offline. A tecnologia implica a utilização de computadores domésticos de terceiros que se tornam parte de uma botnet como servidores web com conteúdo phishing. O rendimento do phishing é comparável com o de roubo de dados confidenciais usando programas maliciosos, e chega a milhões de dólares por ano.[48]". Como se pode constatar, trata-se de uma das grandes problemáticas cibercriminais atuais, refletindo a evolução constante das técnicas utilizadas no cibercrime com vista a obter maiores ganhos financeiros.

([47]) Disponível na WWW:
<URL www.enisa.europa.eu/act/res/.../fullReport >.
([48]) Disponível na WWW:
<URL http://www.kaspersky.com/pt/botnet_economy>.

Abordagem jurídica do Cibercrime

O sistema legislativo português, tem previsto, desde muito cedo, alguns comportamentos ilícitos no uso das TIC. O CP Português de 1982, já previa na sua redação, o crime *de devassa por meio de informática*, pelo que, a proteção criminal e, por consequente, a penalização de atos com recurso à informática eram já contemplados na legislação portuguesa. A evolução tecnológica criou a necessidade de serem adotadas outras medidas consideradas necessárias para enfrentar as novas formas de atuação criminal, que vinham pondo em causa a segurança dos equipamentos informáticos e os interesses dos seus utilizadores. O impulso para a criação de uma legislação específica nessa matéria deu-se com a Recomendação n.º (89) 9 do Comité de Ministros aos Estados-Membros de 13 de Setembro de 1989, que recomendava aos Estados a inclusão de uma série de abusos nas suas próprias legislações penais[49]. A referida recomendação e a entrada em vigor da Lei n.º 109/91, de 17 de Agosto, fizeram com que Portugal introduzisse, na sua ordem jurídica, aquilo a que chamou criminalidade informática. (Verdelho, 2003, p. 364). Perante uma lei que, doravante, iria delimitar e regular a utilização da informática, o fenómeno da criminalidade informática encontrava-se, então, definido em diploma próprio, cujos crimes nele previstos eram subsidiariamente aplicáveis às disposições do CP[50]. A referida lei veio a ser, posteriormente, alterada pelo Decreto-lei nº 323/2001, de 17 de Dezembro.

A LCI englobava um determinado tipo de ilícitos, entre os quais o crime de falsidade informática, de sabotagem informática, de acesso ilegítimo ou ainda de interceção ilegítima, todos constantes como ilícitos integrantes da lista mínima referida na Recomendação n.º (89) 9 e que são parte integrante de qualquer lei de criminalidade informática (Verdelho *et al,* 2003). A LCI contemplava também no artigo n.º 2º., um conjunto de definições ao nível de

(49) Cfr. MARTINS Lourenço, *in Criminalidade Informática – Direito da Sociedade de Informação Volume IV* -2003 pp17.
(50) LCI 109/91 de 17 de Agosto, revogada pela Lei n.º109/2009, 15 de Setembro

hardware e de *software*, uma particularidade, não muito vulgar neste género de diplomas. Pedro Verdelho, Rogério Bravo e Manuel Lopes Rocha referem que a "principal crítica que se pode fazer a uma prática definitória é, por um lado, o seu natural carácter redutor, por outro, a dificuldade de definir o que quer que seja com a precisão mínima nesta área específica" (Verdelho *et al*, 2003, p. 249). Contudo, segundo os mesmos autores, e realçando uma das razões por eles apontadas para a inclusão de definições num diploma legislativo, merece-nos especial atenção, aquela onde referem que "(…) evita que a mesma palavra ou expressão tenham diversas significações consoante o local em que são utilizadas" (Verdelho *et al* , 2003, p. 249).

Atendendo à evolução registada na internacionalização do combate ao cibercrime, a Convenção do Cibercrime de Budapeste em Novembro de 2001 (Cciber) é "o primeiro trabalho de fundo sobre crime no ciberespaço" (Verdelho *et al*, 2003, p. 10). A referida Convenção dedica uma parte ao direito penal material, com a inclusão de novos tipos de crimes, mas na globalidade muitos já estavam previstos na legislação portuguesa. A Cciber inclui também medidas processuais e regras referentes à cooperação internacional. A referida convenção visa a intensificação e a cooperação entre todos os estados membros signatários na luta contra a cibercriminalidade e a adequação das legislações nacionais, em termos penais com vista a uma eficaz cooperação no campo internacional. Um dos mecanismos inovadores da Convenção está previsto no artigo 16.º e refere-se à conservação expedita de dados informáticos armazenados, conferindo aos estados signatários a possibilidade de adotar medidas legislativas, para que estas prevejam a conservação de dados informáticos específicos, nos quais se incluem os dados de tráfego por um período máximo de 90 dias, permitindo às autoridades competentes a sua obtenção, caso o solicitem para efeitos de investigação.

A criação de uma Rede 24/7 prevista na Cciber, mais precisamente no seu artigo 35.º, prevê, entre outras medidas, a criação de um ponto de contacto permanente, o qual deverá estar disponível vinte e quatro horas por dia, sete

dias por semana. Com a evolução do cibercrime, tornou-se crucial assegurar, de imediato, a prestação de auxílio internacional em determinadas investigações. Sem dúvida que, esta medida permite lutar contra as práticas recorrentes dos cibercriminosos, ou seja, a ação de praticá-lo "lá a partir de cá" extrapolando as suas ações por diversos países. Através de um mecanismo previsto no artigo 29.º da Cciber, a preservação expedita de dados informáticos armazenados, pode ser solicitado noutro território, e por qualquer dos membros signatários da Convenção, salvo as exceções constantes no n.º 5 do mencionado artigo.

A Decisão-Quadro (DQ) 2005/222/JAI, relativa a ataques contra os sistemas de informação, resultou da proposta de DQ 2002/0086 e tem por objetivo a cooperação entre as autoridades judiciárias e outras autoridades competentes, nomeadamente as autoridades policiais e outros serviços especializados, responsáveis pela aplicação da lei nos Estados-Membros, mediante uma aproximação das suas disposições de direito penal, em matéria de ataques contra sistemas de informação, e garantir que esses ataques sejam puníveis em todos os Estados-Membros, com sanções penais efetivas, proporcionadas e dissuasivas. Para o efeito, esta DQ encontra-se direcionada para a alteração significativa do regime da criminalidade informática, previsto na LCI.

Apesar da celeridade requerida aos membros signatários da Cciber e da importância na luta contra o cibercrime, Portugal só veio a aprovar a Convenção após a Resolução da Assembleia da República n. 88/2009 de 15 de Setembro, com a reserva constante no artigo 2.º da resolução sobre as condicionantes para a não extradição de pessoas por parte de Portugal, ou seja, a LC entrou em vigor com pelo menos dois anos e meio de atraso. A Transposição do disposto na DQ deveria ter sido adotada pelo direito nacional, conforme mencionado no art.º 12 n.º 1, até ao dia 16 de Março de 2007. Com a sua entrada em vigor, transpôs-se para a ordem jurídica interna a DQ n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro relativa a ataques contra

sistemas de informação e adaptou-se o direito interno à Cciber do Conselho da Europa.

A LC cumpre, na generalidade, as obrigações constantes da DQ, no que diz respeito à qualificação de uma série de crimes, cometidos através e contra os sistemas informáticos. Encontram-se previstas no referido diploma as disposições processuais, consideradas essenciais para a aplicação da lei e, ainda as disposições relativas à cooperação internacional criadas na Cciber. A LC vem substituir a LCI, no entanto nem tudo é novo na nova legislação.

Acreditamos que existem alguns conflitos entre a LC e a Lei 32/2008 de 17 de Julho, relativamente à finalidade do tratamento dos dados. Se na LC encontra-se previsto a preservação expedita de dados para crimes informáticos, o artigo 3.º n.º 1 da Lei 32/2008 diz-nos que a conservação e a transmissão dos dados têm como única finalidade a investigação, deteção e repressão de crimes graves. Na definição de crimes graves, prevista no artigo 2.º n.º 1 al.*g)*, não está prevista a criminalidade informática. Na prática, e numa primeira análise, nada impede a preservação dos dados, de acordo com o artigo 12.º da LC, para a prática de crimes informáticos, todavia não podemos excluir uma eventual recusa dessa preservação, pois bastará fundamentar a recusa com o que está preceituado no artigo 11.º n.º 2 da LC e, que faz referência à Lei 32/2008, ou seja, que as disposições da LC não prejudicam o regime da Lei n.º 32/2008, de 17 de Julho.

A Diretiva 2011/92/EU do Parlamento Europeu e do Conselho de 13 de Dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil e, que substitui a DQ 2004/68/JAI do Conselho, traz para o ordenamento jurídico europeu novos tipos de conteúdo, nomeadamente, e tomando a título de exemplo, o aliciamento de crianças para fins sexuais, feito por intermédio das tecnologias da informação e comunicação (artigo 6.º) ou ainda novas medidas contra endereços da Internet que contenham ou divulguem pornografia infantil (artigo 25.º).

V – CONSIDERAÇÕES FINAIS

Análise das Questões de Investigação

Há que ter em consideração que a matéria recolhida, ao longo deste estudo, só se revelará útil se for alvo de uma análise pormenorizada, para que, daqui em diante, possamos delinear conclusões sobre o tema a que nos propusemos estudar. Atendendo, que parte deste estudo é aferir as trajetórias do cibercrime em Portugal, crê-se que o conjunto de leituras efetuadas, as entrevistas e os inquéritos aplicados contribuíram, de uma forma concreta, para aferir a dimensão do cibercrime, sobressaindo, sobretudo, que se trata de uma das grandes problemáticas criminais do século XXI e que põe em risco o funcionamento de toda a estrutura funcional moderna.

A análise das questões de investigação é feita a partir da informação recolhida. Sem querer entrar em interpretações próprias à área do direito, explorou-se a matéria jurídica e também algumas das características legais constantes na LC. Abordou-se, mais uma vez, o tema do cibercrime como fenómeno criminal *latu sensu*, a partir de todos os dados recolhidos durante a elaboração deste estudo.

O ordenamento jurídico português tem vindo a ser contemplado, há mais de duas décadas, por leis e legislação avulsa, especificamente criadas para o combate à criminalidade informática. A LCI foi o primeiro diploma dedicado exclusivamente a esta problemática tendo sido substituída, em Setembro de 2009 pela LC. A LC é uma lei que acrescentou algumas novidades quanto à definição de termos já existentes, vindo ainda tipificar novas formas de ilícitos ligados à criminalidade informática.

A LCI foi revogada, não apenas por se encontrar substancialmente desatualizada mas, porque as resoluções tomadas com a Cciber de Budapeste, da qual Portugal aderiu e foi signatário, impunham que fossem

honrados os compromissos firmados entre todos os países aderentes. Essas alterações levaram a que Portugal tivesse de adaptar a sua legislação interna às novas disposições. No decorrer das entrevistas, o segundo entrevistado (engenheiro informático) abordou a questão da necessidade de, no futuro, se procederem a atualizações da LC, adaptando a lei consoante a evolução tecnológica. Segundo referiu, a forma como se pensa e procede à atualização das leis nesta área criminal deve ser revista, pois o que se tem vindo a verificar é uma atualização penal e processual muito lenta quando comparada à atualização tecnológica sempre muito rápida [E2, Q4].

A transnacionalização do cibercrime tem sido uma das maiores dificuldades com que os Estados se têm deparado ao longo dos anos. Com a Cciber, os Estados signatários comprometeram-se a adotar medidas legislativas comuns, que se revelassem necessárias, para adaptar o seu direito interno, às normas da referida convenção. Esta última teve, segundo Verdelho (2003), como objetivo formal, "a harmonização legislativa com vista a um quadro comum de repressão da criminalidade relacionada com tecnologias de informação e comunicação, extravasando o espaço comunitário europeu como campo de ação" (Verdelho, Bravo & Rocha, 2003, p. 97). Só com a entrada em vigor da LC é que Portugal adaptou o direito nacional interno aos pressupostos previstos na Cciber, revogando a então LCI. No que diz respeito à harmonização internacional da legislação sobre cibercrime, verifica-se ainda que, ao nível Europeu, têm sido desenvolvidos esforços na partilha de experiencias entre Estados sobre tudo o que está relacionado com o cibercrime. Na data em que se realiza este estudo, a Cciber já foi ratificada por 34 países membros do Conselho da Europa, dos quais apenas 2 países não fazem parte do Conselho.

Como já foi referido, a LC entrou em vigor em 15 de Setembro de 2009 e as novidades mais visíveis desta lei estão presentes nas medidas processuais adotadas das quais sobressai os mecanismos respeitantes à cooperação internacional. Estes vieram conferir às autoridades judiciárias dos países

signatários da convenção, uma cooperação mútua no âmbito da investigação criminal e ainda no que concerne à preservação e recolha de prova, em suporte eletrónico, de um crime. Relembra-se que esta cooperação não se sobrepõe às normas legais existentes em cada Estado. Segundo o primeiro entrevistado (Investigador Criminal), a cooperação internacional "é um potencial sério" [E1, Q4] e um mecanismo possível, do qual é sempre possível recorrer, contudo apresenta as suas limitações, derivadas das legislações locais previstas em cada país. O entrevistado indicou, a título de exemplo, o facto de em determinados países como a Alemanha, os dados de tráfego, serem preservados durante 7 dias, o que é um prazo bastante mais reduzido daquele que está previsto em Portugal [E2, Q5].

As disposições processuais conferidas pela LC introduziram "significativas novidades no ordenamento interno português" (Venâncio, 2009, p. 24). Porém, determinados aspetos desta lei têm vindo a ser contestados. No decorrer deste estudo, verificou-se que, uma dessas disposições tem sido veemente contestada, estando a mesma prevista no artigo 16.º n.º 4 da LC, e que se refere ao prazo máximo para a validação de apreensões de dados informáticos. O prazo mencionado na lei é de 72 horas, o que, para alguns casos específicos, é considerado insuficiente. A chamada de atenção para este ponto específico foi feita por chefias da Polícia Judiciária, e pela Associação Sindical dos Juízes Portugueses, que neste último caso, refutou publicamente, na pessoa de António Martins, a viabilidade prática desta norma. O mesmo indicou, a título de exemplo, uma situação prática, referindo-se a uma "operação em que estejam envolvidos cinco computadores de arguidos, o juiz tem um prazo de 72 horas para abrir e validar todos os *e-mails* trocados, sublinhando que esse período não chega para aceder a, por vezes, 15 a 20 mil mensagens de correio eletrónico[51]". A este respeito, verificou-se que na proposta inicial de alteração à LCI, nomeadamente no artigo dedicado à

([51]) Disponível na WWW:
<URL: http://www.tsf.pt/PaginaInicial/Portugal/Interior.aspx?content_id=1425860&page=1>.

apreensão de dados informáticos (artigo 17.º da proposta de Lei da Criminalidade informática), que não estava proposto qualquer prazo para a validação de apreensões, ao contrário do que está previsto no artigo 178.º n.º 5 do CPP para a criminalidade tradicional. Esta omissão na proposta de alteração à LCI indicia que houve uma preocupação inicial em diferenciar a recolha de prova em suporte eletrónico, da recolha de prova em locais onde se praticaram os chamados crimes tradicionais. Foi um dos pontos abordados no decorrer das entrevistas, obtendo-se do primeiro entrevistado que "o prazo das 72 horas é uma limitação dificilmente aplicável a todas as operações policiais perante a impossibilidade técnica e humana que configura [E1, Q6].

Sobre a prevenção da criminalidade, Pinto de Albuquerque referiu que o "pilar preventivo é hoje totalmente descurado (…)[52]". A esse respeito, a Comissão das Comunidades Europeias, através da Comunicação 200/786, de 29 de Novembro de 2000 definiu a prevenção da criminalidade como "todas as actividades que contribuem para fazer cessar ou reduzir a criminalidade enquanto fenómeno social, tanto quantitativamente como qualitativamente, quer através de medidas de cooperação permanente e estruturada, quer através de iniciativas *ad hoc*. Estas actividades dizem respeito a todos os agentes susceptíveis de desempenhar um papel preventivo (…) bem como ao público em geral (…)[53]".

O cibercrime, como qualquer outra forma de criminalidade tradicional, precisa de ser antecipado ainda antes de se manifestar. Nesse sentido, julgamos que os aspetos preventivos têm uma importância relevante nesse processo.

O estudo do cibercrime tem sido seriamente encarado por alguns técnicos e investigadores especializados, na área da informática. Essas comunidades científicas dedicam-se ao estudo deste fenómeno criminal e orientam as suas

([52]) Disponível na WWW
<URL: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185CM=1&DF=&CL=ENG >.
([53]) Disponível na WWW
<URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0786:PT:HTML >.

pesquisas no sentido de estarem um passo à frente dos cibercriminosos, para assim poderem prevenir-se e até dar resposta às ações que põem em risco o funcionamento de toda a estrutura informática. Os investigadores responsáveis pelo desenvolvimento da já referida plataforma HackLab, do Laboratório Ubinet do Instituto Politécnico de Beja são, como já o frisamos, um exemplo da perseverança dessas comunidades científicas na investigação do cibercrime.

Perspetivas de futuro para o cibercrime em Portugal

Durante a preparação deste estudo, ousou-se referir que no final, iriam ser traçadas perspetivas de futuro para o cibercrime em Portugal. Ora, desde o início, sabíamos das dificuldades em atingir esse objetivo. Contudo, chegados a esta fase do estudo acredita-se já podermos, identificar o que se considera essencial encetar no futuro, para melhorar o combate ao cibercrime. As perspetivas em questão, não passam pela formulação daquilo que irá advir, mas antes por uma apresentação de algumas propostas, que acreditamos serem fundamentais para ajudar a solucionar um fenómeno que tem vindo a aumentar, consideravelmente, em Portugal e no mundo.

Guedes Valente, citando Gomes Canotilho e Vital Moreira, indica que "a prevenção criminal[54] comporta a função de vigilância (…)" (Valente, 2004, p.28). Nesse sentido, segue-se a ótica de Grabosky e Smith quando referem que "*much digital crimes takes place simply because of the absence of a capable guardian"* (2001, p. 36 *in* Crime and the Internet), pois torna-se urgente a adoção de medidas, que solucionam uma eventual falta de vigilância na Internet.

([54]) "A prevenção da criminalidade abrange todas as medidas destinadas a reduzir ou a contribuir para a redução da criminalidade e do sentimento de insegurança dos cidadãos, tanto quantitativa como qualitativamente, quer através de medidas diretas de dissuasão de atividades criminosas, quer através de políticas e intervenções destinadas a reduzir as potencialidades do crime e as suas causas. Inclui o contributo dos governos, das autoridades competentes, dos serviços de justiça criminal, de autoridades locais, e das associações especializadas que eles tiverem criado na Europa, de sectores privados e voluntários, bem como de investigadores e do público, com o apoio dos meios de comunicação". Definição do conceito de Prevenção Criminal - conforme preceituada no art.º 1 n.º 3 da Decisão do Conselho de 28 de Maio de 2001, que veio criar uma Rede Europeia de prevenção da criminalidade. Disponível na WWW: <URL:http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:153:0001:0003:PT:PD>

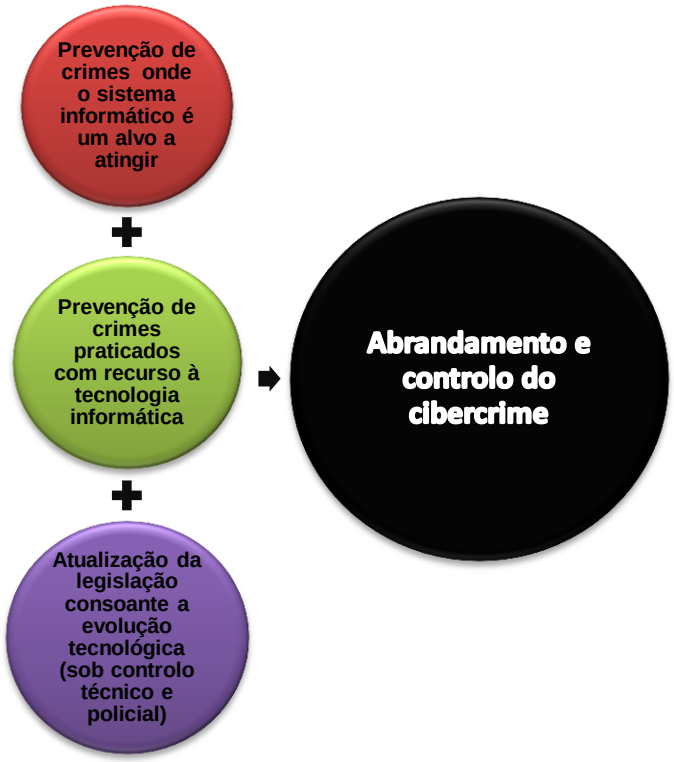
Uma medida já entreposta nesse sentido, relativo ao combate ao cibercrime deu-se com a criação de um grupo de estudo para a implementação, do já mencionado Gabinete de Cibersegurança em Portugal. Acredita-se, que este projeto é um dos mais importantes passos na segurança cibernética em Portugal. A necessidade de assegurar a segurança de um determinado número de estruturas estratégicas e essenciais ao funcionamento nacional, imperou na decisão das instâncias governamentais. É por isso que se acredita que o fator preventivo é essencial, devendo ser privilegiado e conjugado com outros fatores, o que irá proporcionar uma maior eficácia no combate ao cibercrime.

Outro dos pontos a ter em conta pelas entidades responsáveis, é fazer com que a LC acompanhe a evolução tecnológica, evitando dessa forma que se verifique o que aconteceu à LCI, que não acompanhou o desenvolvimento evolutivo das novas tecnologias, nomeadamente quanto aos progressos verificados neste ramo. Esta desatualização conduziu ao longo dos anos à sua parcial ineficácia, dificultando a investigação de uma criminalidade cada vez mais especializada e sofisticada.

Ao longo deste estudo, referimos a existência de crimes praticados contra os sistemas informáticos e, ainda a existência de criminalidade, onde a informática é o meio técnico utilizado para os praticar. No seguimento desta diferenciação, julga-se essencial, distinguir a forma como pode ser feita a prevenção do cibercrime. Como tal, defendemos a criação de três formas preventivas distintas. A primeira, direcionada exclusivamente para a prevenção dos crimes onde os sistemas informáticos são o alvo dos cibercriminosos, e a segunda, vocacionada para a prevenção dos crimes onde a informática é apenas um objeto da sua prática. A estas duas formas preventivas juntar-se-á uma terceira, relacionada com a atualização da legislação. Quando sejam verificadas evoluções tecnológicas de tal ordem que permitam aos cibercriminosos contornar a legislação em vigor, deverão então ser realizadas as alterações necessárias à lei. Nesse sentido deverá existir uma colaboração estreita entre investigadores criminais e especialistas informáticos na

identificação de novas formas de cibercrime não previstas na legislação. Estas três formas preventivas só serão eficazes quando conjugadas entre elas. Apresentamos, a seguir, o esquema, daquilo que avançamos:

Figura n.º 3 – Esquema Preventivo



Se por um lado, a particularidade do meio digital, nomeadamente, do ciberespaço, requer procedimentos preventivos específicos, por outro, não pode ser esquecido, o que está previsto na Constituição da República Portuguesa, mais concretamente no n.º 3 do artigo 272.º, o qual preceitua que a "prevenção dos crimes (…) só pode fazer-se com observância das regras gerais sobre polícia e com respeito pelos direitos, liberdades e garantias dos cidadãos". Nesse sentido, e ainda recorrendo às entrevistas realizadas no presente estudo, reforçamos o que atrás referimos com a opinião do terceiro entrevistado (especialista em direito do cibercrime) quando realça o facto de não querer "uma lei favorável aos criminosos, nem favorável aos policiais". A

LC é uma lei que está "na linha do princípio da proporcionalidade" [E3, Q5]. E, segundo nossa opinião, assim deverá manter-se.

Grabosky e Smith, realçam a importância da participação de todos, na prevenção criminal, afirmando que *"It has long been recognized that the criminal justice system is a very imperfect means of social control, and that effective crime prevention requires the contributions of families, schools and many other instructions of civil society. This is no less the case with digital crime that it is with traditional forms of crime"* (2001, p. 39 *in* Crime and the Internet). Nesta linha de pensamento concordamos, completamente, com a ideia destes dois autores, uma vez que não podem existir dúvidas de que toda a sociedade deve participar na prevenção criminal, seja ela levada a cabo no meio tradicional ou no meio digital. Em primeiro lugar, estamos convictos que a prevenção do cibercrime deve ter o seu início no meio escolar, onde a educação para o uso das tecnologias da informação deve tornar-se uma prioridade, atendendo ao papel que estas ocupam no atual formato de sociedade de informação. Com o inquérito aplicado neste estudo, verificou-se que um grande número de inquiridos (21,5 por cento) indicou já ter praticado atos que se enquadram em práticas cibercriminosas. Sabemos, que os resultados obtidos não são representativos da população portuguesa, contudo acreditamos que o futuro passa por uma correta educação da utilização das potencialidades que a informática e a Internet conferem. Este ponto foi abordado na segunda entrevista, realizada neste estudo, tendo sido referido que o fator preventivo passa por "uma questão de educação e desde tenra idade" referindo ainda que "cada pessoa, que passe por uma educação que o obrigue a olhar para todos estes problemas, de uma forma consciente acaba por, mais tarde, ter uma visão completamente diferente e não o de uma perspetiva transgressora ou ainda de obter enriquecimento para o próprio através desses meios" [E2,Q3]. Assim sendo, é importante que os jovens sejam preparados para o uso correto da Internet e dos sistemas informáticos, sensibilizando-os para os perigos existentes no ciberespaço.

A prevenção a desenvolver junto da sociedade deve ser alvo de uma maior divulgação, pois apesar de já existirem algumas campanhas de sensibilização junto da população, as que existem são pouco ou nada divulgadas. A PSP tem vindo a alertar, na sua página *on-line*, para alguns esquemas criminais que se enquadram na prática do cibercrime. A instituição associou-se, recentemente, ao programa Internet Segura[55], cujo portal foi criado, com o objetivo de "sensibilizar, formar, informar e denunciar". Contudo, alerta-se para a necessidade desse mesmo portal ser atualizado, pois na secção da legislação ainda não se encontra disponível a nova LC sendo apenas possível consultar a já revogada LCI. Relembra-se que no inquérito aplicado, 47,7 por cento dos inquiridos disse não saber da existência da LC.

A prevenção do cibercrime, não passa, apenas pela sensibilização e formação da população, passa também por um processo defensivo, onde as empresas e as instituições bancárias devem estar envolvidas. Só assim é que acreditamos ser possível alcançar melhorias na defesa dos sistemas informáticos. Esse envolvimento deve existir também nos diversos pontos estratégicos nacionais, como na área da saúde (indica-se como exemplo a salvaguarda da informação clínica de cada utente), da defesa, da justiça, da segurança interna, das energias. Todos estes ramos devem estar seguros de potenciais ataques. Mas para isso, é necessário conferir aos técnicos especializados nesta área, a possibilidade de poderem criar as ferramentas necessárias que permitam melhorar a segurança dos sistemas operativos, e de outros setores necessários à segurança informática e das redes informáticas.

Se, por um lado, a legislação penal foi criada como instrumento para reprimir todas as práticas tipificadas na lei como crime, por outro, a mesma não deixa de assegurar, também, a sua vocação preventiva. Não restam dúvidas de que o fator legal ocupa um lugar importante na luta contra o cibercrime. Deste, dependem a celeridade na atuação e a eficácia necessária à investigação de

([55]) Disponível na WWW:
<URL: http://www.internetsegura.pt/pt-PT/Default.aspx. >

qualquer tipo de crime e, especialmente, daqueles que são praticados no ciberespaço. Por consequente, não deverão constar, na lei, normas que fomentem ambiguidades, conforme as que têm sido apontadas entre a LC e a Lei 32/2008 de 17 de Julho, reiterando-se a ideia de que uma lei criada para enfrentar a cibercriminalidade, não poderá ser eficaz se não for regularmente atualizada e adaptada às necessidades exigidas pela realidade criminal. O fator legal deverá, também, zelar pelos direitos, liberdades e garantias de todos os cidadãos, nomeadamente no que diz respeito à utilização da informática e da Internet. Contudo, o combate à cibercriminalidade requer, para além da cooperação internacional, que falemos num novo conceito, e que neste caso denominamos de cooperação global interna. Seria necessário que os pressupostos deste conceito fossem adotados em Portugal. Trata-se de uma cooperação, onde é requerida a colaboração de todos os cidadãos, tendo como objetivo principal a colaboração e empenho de todos na prevenção do cibercrime em Portugal. Desde a família à escola, às autoridades, aos especialistas em informática, aos ISP, todos devem empenhar-se, no sentido de contribuir para um ciberespaço mais seguro, onde as práticas criminais devem ser denunciadas às autoridades. Por isso, acreditamos que as perspetivas de futuro para o cibercrime em Portugal passem, por uma política criminal vocacionada para a prevenção direcionada às populações, às empresas, às instituições públicas e privadas, e ainda pela defesa dos sistemas informáticos através do reforço de segurança dos programas instalados nos computadores, mas também por uma prevenção onde todos devem ter uma participação ativa.

Como referimos anteriormente, o combate ao cibercrime passa por uma conjugação de fatores que poderão revelar-se eficazes nesse propósito. Esses fatores são a prevenção criminal, a prevenção legal e a cooperação global interna. Vejamos, na página a seguir, um esquema que retrata o funcionamento do programa preventivo que defendemos:

Figura n.º 4 – Funcionamento do programa preventivo

A pequena engrenagem acima representada, pretende demonstrar que o programa preventivo que defendemos só funciona se cada um dos elementos estiverem devidamente sincronizados com os restantes. O fator preventivo é indicado como um fator fundamental na prevenção do cibercrime, pois é com ele que se desenvolvem todas as iniciativas necessárias para o seu combate; o fator legal, essencial para determinar o que é crime e o que não é, e a cooperação global interna, que é da responsabilidade de todos. Se um destes elementos não funcionar, conforme acontece num mecanismo, toda a máquina preventiva parará. Como disseram Grabosky e Smith sobre a importância do factor preventivo na luta contra o cibercrime "*it is a great deal more difficult to pursue an online offender to the ends of the earth than to prevent the offence in the first place*" (2001, p.39 *in* Crime and the Internet).

Conclusões

Antes de nos debruçarmos nas conclusões propriamente ditas, revela-se importante assinalarmos algumas das limitações com as quais nos deparamos na realização deste estudo. Por um lado, não se verificou que exista, em Portugal, estudos que abordem o cibercrime como problemática criminal. Por outro lado, trata-se de um tema que, nos últimos tempos, tem despertado a atenção de toda a comunidade científica e política, sendo frequente vermos surgir novas resoluções relacionadas com o combate ao cibercrime. Assim sendo, é importante ter em atenção, quando se tecem considerações acerca das perspetivas apontadas para o futuro do cibercrime em Portugal, que quer os dados e opiniões recolhidas ao longo deste estudo quer as propostas de futuro, apresentadas, foram as que se acreditou serem as mais adequadas no período temporal em que o trabalho foi elaborado.

A informática e a Internet integram o dia-a-dia da população. O cibercrime é fruto do aproveitamento destas novas tecnologias para práticas ilícitas. Para além de não conhecer fronteiras na sua atuação, o cibercrime permite atualmente aos seus autores alcançar ganhos monetários consideráveis. Para isso, é feito um aproveitamento das falhas de segurança dos sistemas informáticos, possibilitadas, sobretudo, pela falta de aposta no campo preventivo e, particularmente, na pesquisa informática defensiva bem como na falta de formação e educação dos atuais e futuros utilizadores. Tudo aquilo, que neste momento concluímos, foi obtido através das leituras realizadas, das entrevistas concedidas e dos inquéritos aplicados.

A Cciber de Budapeste foi das maiores resoluções tomadas, a nível internacional, no combate ao cibercrime. Após Portugal ser signatário da referida convenção, criaram-se as condições necessárias para que a LCI fosse adaptada consoante as resoluções tomadas. A entrada em vigor da LC em substituição da LCI, garantiu que o ordenamento jurídico português fosse apetrechado com mecanismos adaptados à evolução tecnológica, que se

registou nos últimos 18 anos. A medida processual que mais se destaca na LC está relacionada com a cooperação internacional. Dois dos entrevistados acreditam que a cooperação internacional é uma das mais-valias desta lei. A internacionalização deste fenómeno assim o requer. Podemos então dizer, confirmando uma das hipóteses deste estudo, que o combate ao cibercrime deve, em primeiro lugar, ser feito a nível internacional.

Com os dados obtidos, através dos inquéritos por questionário, e relembrando que a amostra utilizada não é representativa da totalidade da população portuguesa, verificou-se que há ainda quem não proteja o seu computador das ameaças que pairam no ciberespaço. Verifica-se ainda a banalização das descargas de conteúdos protegidos com direitos de autor, provavelmente motivadas pela falta de controlo existente na Internet. Esses conteúdos são, muita das vezes, condutores de *malware* (vírus informáticos, *worms*, cavalos de troia, spyware, *keylloger*). Foi ainda possível verificar que dos 65 inquiridos, metade não sabiam da existência da LC, 14 já praticaram factos que se enquadram em cibercrime e 5 disseram já ter sido vítimas do mesmo. Atendendo ao interesse que esta matéria nos suscita, seria interessante, na elaboração de um futuro estudo, aplicar este género de inquérito, a uma amostra representativa da totalidade da população nacional, que assim nos pudesse fornecer dados concretos sobre este tema.

Por fim, no que concerne as perspetivas que traçamos para o cibercrime em Portugal, acreditamos ser possível aplicar, o que anteriormente se expôs. A particularidade do cibercrime faz com que o seu combate passe por uma série de práticas preventivas, que deverão funcionar em harmonia umas com as outras, com vista a reduzir os prejuízos e aumentar os benefícios da utilização da informática e da Internet.

Bibliografia

ACKROYD, S.; HUGHES, J. – **Data Collection in Context**. London, New York: Longman, 1992. ISBN: 0582053110.

ALBARELLO, Luc; DIGNEFFE, Françoise; HIERNAUX, Jean-Pierre; MAROY, Christian; RUQUOY, Danielle; DE SAINT-GEORGES, Pierre – **Práticas e Métodos de Investigação em Ciências Sociais**. 2.ª ed. Lisboa: Gradiva, 2005. ISBN 972-662-554-8.

ANDRADE, Manuel da Costa; DIAS, Jorge de Figueiredo – **Criminologia, O Homem Delinquente e a Sociedade Criminógena**. Coimbra: Coimbra Editora, Reimpressão, 1997. ISBN 972-32-0069-4.

ASSOCIAÇÃO PORTUGUESA DO DIREITO INTELECTUAL – **Direito da Sociedade da Informação Volume IV**. (Com a colaboração de Pedro Verdelho [et al]) Coimbra: Coimbra Editora, 2003. ISBN 972-32-0915-2.

AZZOUZI, Ali; – **La Cybercriminalité au Maroc**. 2010. ISBN 978-9954-9072-0-7.

BACHELARD, Gaston – **A Epistemologia**. Lisboa: Edições 70, 2006. ISBN 972-44-1268-7.

BARDIN, Laurence – **Análise de Conteúdo**. Lisboa: Edições 70, 2009. ISBN 972-44-1506-2.

BELL, Judith – **Como Realizar Um Projecto de Investigação**. 5.ª ed. Lisboa: Gradiva, 2010. ISBN 972-662-524-7.

BRAVO, Rogério, COSTA, Francisco – **Spam e Mail Bomb, Subsídios para uma perspectiva criminal**. Lisboa : Quid Juris, 2005. ISBN 972-724-239-1.

BRAZ, José – **Investigação Criminal - A organização, o método, a prova - Os desafios da nova criminalidade**. 2ª ed. Lisboa: Almedina Editora, 2010. ISBN 978-972-40-4350-0.

CASEY, Eoghan – **Digital Evidence and Computer Crime – Forensic Science, Computers and Internet** (with contributions from Susan W. Brenner ... [et al.]). 3.ª ed. San Diego, California: Elsevier Edition, 2011. ISBN 978-0-12-374268-1.

CASTELLS, Manuel – **A Galáxia Internet – Reflexões sobre Internet, Negócios e Sociedade**. 2.ª ed. Lisboa: Fundação Calouste Gulbenkian, 2007. ISBN 978-972-31-1065-4.

CUSSON, Maurice – **Criminologia.** 2.ª ed. Alfragide: Casa das Letras, 2002. ISBN 972-46-1620-9.

ECO, Umberto – **Como se faz uma Tese em Ciências Humanas**. 16.ª ed. Lisboa: Editorial Presença, 2010. ISBN 972-23-1351-3.

ESPÍRITO SANTO, Paula – **Introdução à Metodologia das Ciências Sociais. Génese, Fundamentos e Problemas.** 1.ª ed. Lisboa: Edições Silabo, 2010. ISBN 972-618-603-8.

FONTANEL, Jacques – **A Globalização em "Análise" Geoeconomia e estratégia dos actores**. Lisboa: Instituto Piaget, 2007. ISBN 972-771-915-0.

GUERRA, Isabel Carvalho – **Pesquisa Qualitativa e Análise de Conteúdo – Sentidos e formas de uso**. 1.ª ed. Cascais: Princípia, 2010. ISBN 978-972-8818-66-1.

GUISNEL, Jean – **Espionagem na Internet**. Lisboa: Difusão cultural, 1997. ISBN 972-709-280-2.

LE DORAN, Serge ; ROSÉ Philipe – **Cyber Mafias**. Paris : Editions Denoël, 1998. ISBN 2.207.246.11.6.

LEVY, Pierre – **Ciberdemocracia**. Lisboa : Stória Editores, 2002. ISBN 972-771-672-5.

MACHADO, Helena – **Manual de Sociologia do Crime**. Lisboa: Edições Afrontamento, 2008. ISBN 978-972-36-0979-0.

MAROCO, João – **Análise Estatística – Com utilização do SPSS** – 3.ª ed. Lisboa: Edições Sílabo, 2007. ISBN 978-972-618-452-2.

MARTIN, Daniel – **La criminalité informatique. Cyber-crime, sabotage, piratage, etc. Evolution et répression.** 1.ª ed. Paris: Editions Presses Universitaires de France, 1998. ISBN 2 13 048488 3.

MARTINS, António [et al] – **Ciberlaw em Portugal, O direito das tecnologias da informação e comunicação**. 1.ª ed. Lisboa: CentroAtlantico.pt, 2004. ISBN 972-8426-95-X.

NORONHA, Mário; NORONHA, Zélia – O Homem em Sociedade, Aspectos sicossociológicos. 1.ª ed. Lisboa: Plátano Edições Técnicas, 2003. ISBN 972-707-372-7

ORDEM DOS ADVOGADOS (Conselho Distrital do Porto) – **Temas de Direito de Informática e da Internet** (com a colaboração de Carlos Ruiz Miguel [et al]). 1.ª ed. Porto: Coimbra Editora 2004. ISBN 972-32-1219-6.

PANSIER, Frederic- Jerôme – **La criminalité sur Internet**. 2.ª ed. Paris : Presse Universitaires de France, 2000. ISBN 2 13 050510 4.

PEREIRA, Alexandre e POUPA, Carlos – **Como escrever uma tese, monografia ou livro científico usando o word**. 4.ª ed. Lisboa: Edições Sílabo, 2008. ISBN 972-618-511-6.

QUIVY, Raymond e CAMPENHOUDT, Luc Van – **Manual de Investigação em Ciências Sociais**. 5.ª ed. Lisboa: Gradiva, 2008. ISBN 972-662-275-8.

RAUFER, Xavier – **Les nouveaux dangers planétaires – Chaos mondial, décèlement précoce**. Paris : CNRS Editions, 2009. ISBN 978-2-271-06864-4.

RIBEIRO, José Luís Pais – **Metodologia de investigação em psicologia e saúde**. 2.ª ed. Porto: Livpsic, 2008. ISBN 989-8148-16-0.

ROBERT, Philippe – **Sociologia do Crime**. Petrópolis: Editora Vozes, 2007. ISBN 978-85-326-3560-0.

ROCHA, Manuel ; MACEDO Mário – **Direito no Ciberespaço**. 1.ª ed. Lisboa: Edições Cosmos, 1996. ISBN 972-762-003-5.

SAAVEDRA, Rui – **A protecção Jurídica do Software e a Internet**. 1.ª ed. Lisboa: Edição Publicações Dom Quixote lda., 1998. ISBN 972-20-1416-1.

SANTOS, Paulo; BESSA, Ricardo; PIMENTEL, Carlos – **Cyberwar – O Fenómeno, as Tecnologias e os Actores**. Lisboa: FCA – Editora Informática, 2008. ISBN 978-972-722-597-2.

SILVESTRE, Hugo Consciência; ARAÚJO, Joaquim Filipe (2012) – **Metodologia para a Investigação Social**. Lisboa: Escolar Editora, 2012. ISBN 978-972-592-329-0.

SOUSA, Ivo Dias de – **O Lado Negro da Internet**. Lisboa: FCA – Editora Informática, 1999. ISBN 972-722-166-1.

SUB JUDICE, Justiça e Sociedade – **Internet, Direito e Tribunais**. (Com a colaboração de Maria Eduarda Gonçalves [et al]) Coimbra: Almedina Editora, Revista trimestral Setembro de 2006. ISBN 978-972-40-2999-3.

VALENTE, Manuel Monteiro Guedes – **Teoria Geral do Direito Policial**. 2.ª ed. Coimbra: Almedina, 2009. ISBN 978-972-40-4034-9.

–, **Regime Jurídico da Investigação Criminal** – 2.ª ed. Coimbra: Almedina 2004. ISBN 972-40-2139-4.

VENÂNCIO, Pedro – **Lei do Cibercrime**. Lisboa: Coimbra Editora, 2011. ISBN 972-32-1906-7.

VERDELHO, Pedro; BRAVO, Rogério; ROCHA, Manuel Lopes – **Leis do Cibercrime Volume 1**. Lisboa: CentroAtlantico.pt, 2003. ISBN 972-8426-69-0.

WALL, David – **Crime and the Internet** (with contributions from Peter Grabosky [et al]). London : Routledge, 2001. ISBN 0-415-24429-3.

YAR, Majid (2006) – **Cybercrime and Society**. 2.ª ed. London: Sage, 2010. ISBN 978-1-4129-0754-5.

Artigos Científicos

CHAWKI, Mohamed - **Essais sur La notion de Cybercriminalité**. Membre du Conseil d'Etat Doctorant en Droit Pénal de l'Informatique à Lyon III, 2006. [Consult. 15 Jan. 2012], Disponível na WWW: <URL: http://www.ie-ie.ue/bibliotheque/cybercrime.pdf>.

COUNCIL OF EUROPE - Global Project on Cybercrime, Cybercrime Strategies. Strasbourg, 2011. [Consult. 21 Mar. 2012]. Disponível na WWW<URL: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_cy_strats_rep_V20_14oct11.pdf>.

DIAS, Vera Elisa Marques – **A problemática da investigação do cibercrime**. Curso de pós-graduação de aperfeiçoamento em direito da investigação criminal e da prova. 2010. [Consult. 20 Jan. 2012], Disponível na WWW: <URL: http://www.verbojuridico.com/doutrina/2011/veradias_investigacaocibercrime.pdf>.

EUROPOL Public Information - THREAT ASSESSMENT (ABRIDGED) INTERNET FACILITATED ORGANISED CRIME. iOCTA The Hague,

2011. [Consult. 15 Mar. 2012]. Disponível na WWW<URL: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf>.

FINNIE, Toby; PETEE, Tom; JARVIS, John - Future Challenges of Cybercrime Volume 5: Proceedings of the Futures. Quantico, Virginia 2010. [Consult. 19 Mar. 2012]. Disponível na WWW<URL: http://futuresworkinggroup.cos.ucf.edu/publications/FWGV5Cybercrime.pdf>.

LALANDA, Piedade - **Sobre a metodologia qualitativa na pesquisa sociológica**, Análise Social, vol. xxxiii (148), 1998 (4.°), 871-883. [Consult. 20 Abr. 2012]. Disponível na WWW: <URL: www.apis.ics.ul.pt/SendDoc.aspx?d=1072&q=9365

McCONNELL – **Cyber Crime . . . and Punishment ? - Archaic Laws Threaten Global Information**, December 2000. [Consult. 21 Abr. 2012]. Disponível na WWW: <URL: http://www.witsa.org/papers/McConnell-cybercrime.pdf >.

NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves – **Elementos para uma reflexão sobre a ética informacional**. R.CEJ, Brasília, n. º 20, p. 67-73, jan/mar, 2003. [Consult. 02 Fev. 2012]. Disponível na WWW<URL: http://www2.cjf.jus.br/ojs2/index.php/cej/article/viewFile/523/704>.

PLANEAMENTO CIVIL DE EMERGÊNCIA – **Cibersegurança, a resposta à emergência.** Revista n.º 19, 2007. [Consult. 15 Mar. 2012]. Disponível na WWW<URL: http://www.cnpce.gov.pt/archive/doc/revista19.pdf>.

Diplomas legais e jurisprudência consultada

Decisão-Quadro 2005/222/JAI relativa a ataques contra os sistemas de informação.

Directiva 2002/58/CE do Parlamento Europeu e do Conselho de 12 de Julho de 2002 *relativa ao tratamento de dados pessoais e á protecção da privacidade no sector das comunicações electrónicas.*

Directiva 2006/24/CE do parlamento europeu e do conselho de 15 de Março de 2006 *relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações e que altera a Directiva 2002/58/CE.*

Directiva 2011/92/EU do Parlamento Europeu e do Conselho de 13 de Dezembro de 2011 *relativa à luta contra o abuso sexual de crianças e a pornografia infantil.*

DL 252/94, de 20/10 – *Protecção Jurídica do Software.*

Lei 109/91, de 17/08 – *Criminalidade Informática.*

Lei 67/98, de 26/10 – *Protecção de dados pessoais face à informática.*

Lei 122/00, de 04/07 – *Protecção Jurídica de base de dados.*

Lei 5/2004, de 10/02 – *Lei das comunicações electrónicas.*

Lei 41/04, de 18/08 – *Regula o tratamento de dados pessoais e a protecção da privacidade nas telecomunicações electrónicas.*

Lei 31/2008 de 17/07 – *Relativa à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações electrónicas publicamente disponíveis ou de redes públicas de comunicações.*

Relatório Anual de Segurança Interna –2009, 2010, 2011.

Netgrafia

http://www.tsf.pt/PaginaInicial/Portugal/Interior.aspx?content_id=1425403
[Consult. 15 Jan. 2012].
http://www.jn.pt/PaginaInicial/Nacional/Interior.aspx?content_id=1475146
[Consult. 15 Jan. 2012].
http://www1.ionline.pt/conteudo/42900-cibercrime-portugal-tem-uma-lei-de-vanguarda-diz-especialista-
[Consult. 15 Jan. 2012].
http://www.ie-ei.eu/bibliotheque/cybercriminalite.htm
[Consult. 30 Jan.. 2012].
http://www.dn.pt/inicio/portugal/interior.aspx?content_id=1426627
[Consult. 30 Jan.. 2012].
http://www.rbhcs.com/index_arquivos/Artigo.Pesquisa%20documental.pdf >.
[Consult. 30 Jan.. 2012].
http://www.netconsumo.com/2012/03/cibercrime-e-um-risco-elevado-para.html
[Consult. 18 Mar. 2012].
http://sol.sapo.pt/inicio/Tecnologia/Interior.aspx?content_id=43001
[Consult. 2 Abr. 2012].
http://www.cmjornal.xl.pt/detalhe/noticias/opiniao/josebraz/cibercrime010705780
[Consult. 2 Abr. 2012].
http://www.jornaldenegocios.pt/home.php?template=SHOWNEWS_V2&id=533835
[Consult. 2 Abr. 2012].

http://www.oa.pt/upl/%7B3d49f105-1ff4-426f-8c50-ddaee1b8acbb%7D.pdf
[Consult.10 Abr. 2012].
http://www.tvi.iol.pt/noticia/sociedade/comerciantes-justica-furtos-paula-teixeira-da-cruz-confederacao-do-comercio-tvi24/noticia/aa---videos---politica/justica-paula-teixeira-da-cruz-tvi24/1329847-5796.html
[Consult.10 Abr. 2012].
http://under-linux.org/cibercrime-crackers-estao-levando-vantagem-4499/
[Consult.10 Abr. 2012].
http://www.cmjornal.xl.pt/detalhe/noticias/ultima-hora/cibercrime-pedro-verdelho-coordenador-do-gabinete-do-mp
[Consult.10 Abr. 2012].
http://tek.sapo.pt/opiniao/entrevista_lei_do_cibercrime_novas_possibilid_1005696.html
[Consult.10 Abr. 2012].
http://cibercrime.pgr.pt/Actividade/Actividade.html
[Consult. 23 Abr. 2012].
http://exameinformatica.sapo.pt/noticias/internet/2008/01/04/cibercrime-pode-ser-um-novo-11-de-setembro
[Consult. 23 Abr. 2012].
http://economia.publico.pt/noticia/grandes-empresas-de-cartoes-de-credito-admitem-exposicao-de-dados-dos-clientes-1540207
[Consult. 23 Abr. 2012].
http://www.publico.pt/Mundo/governo-britanico-quer-apertar-vigilancia-na-internet-1540328
[Consult. 23 Abr. 2012].
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/default_FR.asp
[Consult. 23 Abr. 2012].
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Interface2010_fr.asp
[Consult. 23 Abr. 2012].
http://arxiv.org/ftp/arxiv/papers/0908/0908.0099.pdf
[Consult. 23 Abr. 2012].
http://www.ionline.pt/mundo/director-da-europol-alerta-ameaca-cibercrime
[Consult. 30 Abr. 2012].
http://expresso.sapo.pt/laboratorio-portugues-testa-pirataria-para-combater-cibercrime=f707397
[Consult. 30 Abr. 2012].
http://expresso.sapo.pt/portugueses-mal-informados-sobre-protecao-contra-cibercrimes=f703175
[Consult. 30 Abr. 2012].
www.apis.ics.ul.pt/SendDoc.aspx?d=1072&q=9365>.
[Consult. 30 Abr. 2012].
http://www.ionline.pt/portugal/cibercrime-pj-reuniu-se-unidade-da-microsoft
[Consult. 30 Abr. 2012].
http://www.lefigaro.fr/actualite-france/2010/03/30/01016-20100330ARTFIG00475-l-europe-declare-la-guerre-a-la-cybercriminalite-.php
[Consult. 30 Abr. 2012].

http://www.pcseguro.pt/blog/?tag=ciber-crime
[Consult. 30 Abr. 2012].
http://www.presseurop.eu/fr/content/news-brief/329031-le-portugal-terrain-de-jeu-des-cybermafias
[Consult. 5 Mai. 2012].
http://www.tecnologia.com.pt/2011/09/cibercrime-ganha-284-mil-milhoes-de-euros-todos-os-anos/
[Consult. 5 Mai. 2012].
http://www.dn.pt/inicio/portugal/interior.aspx?content_id=2169698
[Consult. 5 Mai. 2012].
http://www.fibra.pt/internet/2914-cibercrime-cresce-mais-de-300-em-portugal-e-espanha.html
[Consult. 5 Mai. 2012].
http://www.rtp.pt/noticias/index.php?article=508451&tm=7&layout=122&visual=61
[Consult. 10 Mai. 2012].
http://www.lefigaro.fr/conjoncture/2011/06/30/04016-20110630ARTFIG00750-le-cout-exorbitant-et-opaque-des-cyberattaques.php
[Consult. 10 Mai. 2012].
http://www.rtp.pt/noticias/?article=510282&layout=121&visual=49&tm=4&
[Consult. 10 Mai. 2012].
http://www.tvi24.iol.pt/sociedade/psp-e-mail-burla-fraude-queixas-tvi24/1342489-4071.html
[Consult. 10 Mai. 2012].
http://opiniao.mai-gov.info/2009/10/02/a-nova-lei-do-cibercrime/
[Consult. 12 Mai. 2012].
http://www.cmjornal.xl.pt/detalhe/noticias/nacional/economia/phishing-e-o-crime-informatico-mais-comum-em-portugal
[Consult. 12 Mai. 2012].
http://pplware.sapo.pt/informacao/crime-informatico-atinge-cada-vez-mais-portugueses/
[Consult. 12 Mai. 2012].
http://www.jn.pt/PaginaInicial/Seguranca/Interior.aspx?content_id=2622847&page=-1
[Consult. 22 Jun. 2012].
http://www.kaspersky.com/pt/botnet_economy
[Consult. 22 Jun. 2012].

Lista de Abreviaturas

ANSOL	- Associação Nacional para o Software livre
Cciber	- Convenção do cibercrime
CE	- Comissão Europeia
CP	- Código Penal
CPP	- Código de Processo Penal
DIAP	- Departamento de Investigação e Acção Penal
DQ	- Decisão - Quadro
ISP	- Internet Service Provider
LC	- Lei do Cibercrime
LCI	- Lei da Criminalidade Informática
PSP	- Polícia de Segurança Pública
RASI	- Relatório Anual de Segurança Interna
TIC	- Tecnologias de Informação e da Comunicação
WWW	- World Wide Web

Anexos

Entrevista 1 [E01]

Q1: Que função exerce, atualmente, no seio da Polícia Judiciaria?
Q2: Concorda com a atual redação da lei do Cibercrime?
Q3: Na sua opinião a lei do cibercrime proporcionou a diminuição da criminalidade informática?
Q4: Quais são as potencialidades e os pontos fracos desta lei do cibercrime?
Q5: Quanto às expectativas em relação à cooperação internacional, foram superadas? Haverá mais alguma coisa a fazer nesse sentido?
Q6: Foi possível durante estes dois anos e meio, desde a entrada em vigor da Lei do Cibercrime, ultrapassar o problema levantado sobre o prazo concedido para a validação das apreensões, ou urge alterar algum ponto na Lei do Cibercrime a esse respeito?
Q7: Dê-nos uma opinião sobre o que acrescentaria ou retiraria da Lei do Cibercrime, de forma a permitir uma mais célere investigação.
Q8: Qual a perspetiva de futuro para a Lei do Cibercrime?

Entrevista2 [E02]

Q1: Que função exerce atualmente na sua vida profissional?
Q2: Concorda com a atual redação da lei do Cibercrime, nomeadamente no que diz respeito à sua área profissional?
Q3: Referiu que trabalha na parte da educação. Na sua opinião o que poderia ser feito a título preventivo para evitar cometer os crimes mencionados na lei do cibercrime?
Q4: Acha que esta lei do cibercrime, da forma como está redigida, tem impacto no combate à criminalidade informática?
Q5: Outra questão debruça-se sobre o facto, das operadoras guardarem os dados de tráfego dos utilizadores. De alguma forma, não estamos perante uma

violação da privacidade dos utilizadores, ou pelo contrário é uma mais-valia para a investigação?
Q6: Quais as potencialidades e os pontos fracos desta lei do cibercrime? Inicialmente falou no software, na investigação. Acha que é uma das fraquezas desta lei?
Q7: Qual a perspetiva de futuro para a Lei do Cibercrime?

Entrevista 3 [E03]

Q1: Concorda com a atual redação da lei do Cibercrime?
Q2: Pegando nas suas palavras, do que é uma lei boa….
Q3: Quais as potencialidades e as fraquezas desta lei do cibercrime?
Q4: Pegando aqui nuns comentários que foram feitos na altura…
Q5: Relativamente ao que estava a dizer, houve umas opiniões iniciais antes da aprovação, da entrada em vigor da lei do cibercrime por parte de juízes, chefias da Policia Judiciaria, que referiam que esta lei é uma lei favorável aos criminosos. Na sua opinião, onde é que portanto, poderíamos…
Q6: Relativamente a um ponto que gerou um pouco de discórdia na altura da pré-aprovação da lei do cibercrime tinha a ver com as 72 horas concedidas para a validação das apreensões efetuadas…
Q7: E não acha que a lei em si é limitativa, ou mesmo impeditiva na pesquisa por especialistas informáticos que desenvolvem investigação?
Q8: Qual a sua perspetiva de futuro para a lei do cibercrime?

IMAGEM SOCIAL DO CIBERCRIME EM PORTUGAL

Agradeço desde já a sua colaboração no preenchimento do presente inquérito. As questões enquadram-se na elaboração da dissertação de Mestrado em Ciências Policias no Instituto Superior de Ciências Policiais e Segurança Interna, na especialização de criminologia e investigação criminal. Todas as questões versam sobre a utilização da informática e do fenómeno do cibercrime em Portugal. O inquérito é totalmente anónimo.

Este inquérito tem como objetivo inicial de apurar a forma como o fenómeno do cibercrime é percecionado em Portugal.

Sexo?

- Masculino
- Feminino

Idade?

____

1) – Tem computador? (Se não, passe diretamente à questão n.º 6)

- Sim.
- Não.

2) - O que é para si o cibercrime?

- Descarga de música/filmes/programas com direitos de autor da Internet?
- Subtração de códigos de acesso (passwords) e intrusão em sistemas informáticos alheios.
- Aceder através do computador e da Internet a canais de televisão *pay-per-view* (que carecem do pagamento de uma assinatura).
- Todos os acima referidos.
- Nenhum.
- Não sabe.

3) - Já se deparou com problemas que tenham sido causados pela presença de vírus informáticos no seu computador?

- Sim. Quais? _____
- Não.
- Não sabe.

4) – Protege o seu computador e os dados nele armazenados, de potenciais intrusões ou contaminação por vírus informáticos?

- Sim.
- Não.

Se sim como o faz?

- Descarga gratuita de antivírus através da Internet?
- Adquire antivírus numa loja ou na Internet?
- Não utiliza antivírus.
- Outros? Quais? _____

5) – Qual o grau de perigosidade que para si representa para si, um cibercriminoso?

- Fraco
- Médio
- Grande
- Nenhum

6) – Conhece alguém que já tenha praticado, de qualquer forma, algum cibercrime?

- Sim.
- Não.

7) – Já praticou algum acto na Internet que possa se enquadrar nas práticas cibercriminosas?

- Sim. Quais? _____
- Não.

8) – Crê estar devidamente informado/a acerca do cibercrime?

- Sim.
- Não.

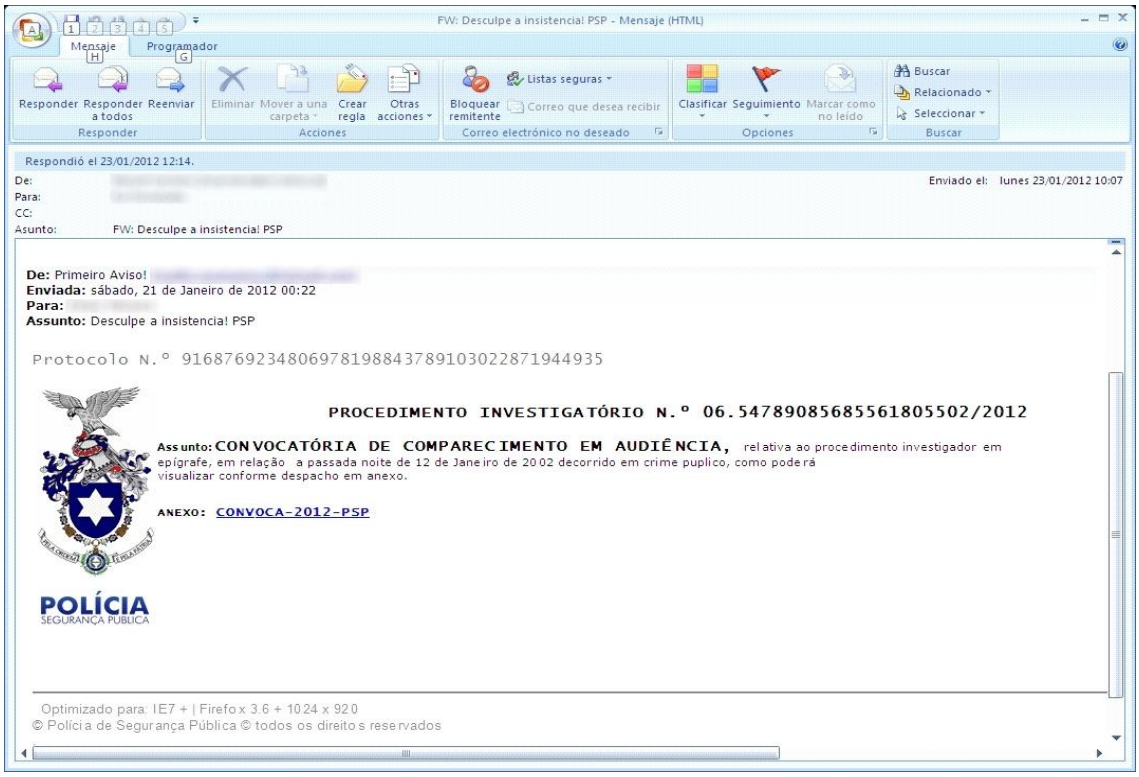
9) – Sabia que em Portugal o cibercrime está previsto na Lei (Lei do Cibercrime)?

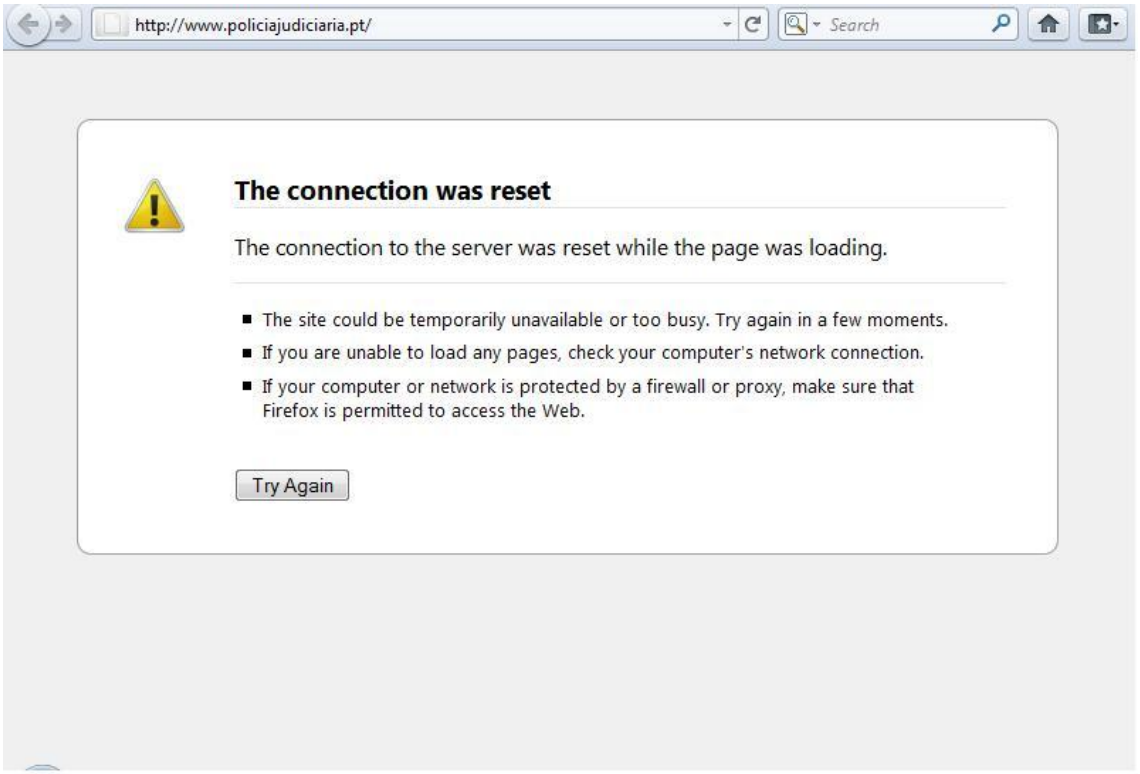
- Sim.
- Não.

10) – Já foi vítima do cibercrime?

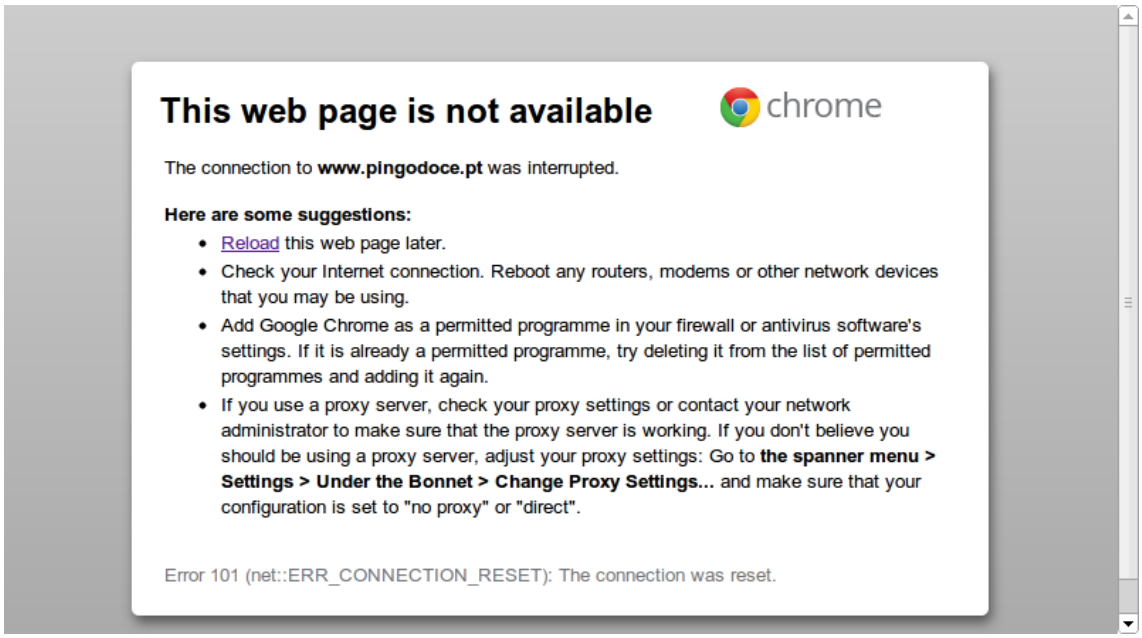
- Sim. Apresentou queixa nas autoridades? - sim - não
- Não.
- Não sabe.


POLÍCIA
SEGURANÇA PÚBLICA
Atenção!!!
Foi detectado um caso de atividade ilegal. O sistema operacional foi bloqueado por violação das leis da República Portuguêsl Foi detectada a violação seguinte:
Do seu endereco IP com o numero de "194.65.237.63" foi feita para acessar sites que contenham pornografia, pornografia infantil, bestialidade, tambem como a violencia sobre as criancas. No computador tambem foram encontrados arquivos de video contendo pornografia, violencia e os elementos de pornografia infantil. Uma vez que tambem spamming e-mail foi feito com subtexto de terrorismo.
O bloqueio do computador é feito para eliminar a possibilidade de ações ilegais por parte deles.
Seus detalhes:
IP:194.65.237.63
Localização: Portugal
ISP:
Para remover o bloco em seu computador, você deve pagar uma multa de 100 €.
Você tem duas formas de pagamento:
1) Efetuar o pagamento pelo Ukash:
Para isso, digite o código que você recebeu na linha de pagamento e clique em OK (se você tiver vários códigos, inseri-los um após o outro, em seguida, pressione OK).
Se o sistema falhar, você deve enviar e-mail de código (deposito@cyber-psp.pt).
2) Efetuar o pagamento via Paysafecard:
Para isso, digite o código que você recebeu (se necessário juntamente com a senha) na linha de pagamento, e clique em OK (se você tiver vários códigos, inseri-los um após o outro, e então clique em OK).
Se o sistema falhar, você deve enviar e-mail o código (deposito@cyber-psp.pt)
Ukash Onde posso comprar Ukash?
Pode adquirir Ukash a partir de centenas de milhar de localizações globais, online, através de carteiras, de quiosques e do Multibanco.
payshop
Payshop - Pode adquirir vouchers Ukash em qualquer um dos mais de 3.600 agentes payshop em Portugal, como papelarias, tabacarias, quiosques e supermercados. Basta indicar ao Agente payshop o montante que pretende. Após o pagamento, o Agente payshop entregar-lhe-á um talão com o código.
OK
paysafecard Onde posso comprar Paysafecard?
Podes obter paysafecards nas cerca de 4.000 lojas da rede PayShop, nas 1.000 estações-dos-correios dos CTT e em toda a rede de caixas automáticas Multibanco.
payshop
MB
ctt
OK


FW: Desculpe a insistencia! PSP - Mensaje (HTML)
Mensaje
Programador
Responder
Responder a todos
Reenviar
Eliminar
Mover a una carpeta
Crear regla
Otras acciones
Bloquear remitente
Listas seguras
Correo que desea recibir
Clasificar
Seguimiento
Marcar como no leído
Buscar
Relacionado
Seleccionar
Respondió el 23/01/2012 12:14.
De:
Para:
CC:
Asunto: FW: Desculpe a insistencia! PSP
Enviado el: lunes 23/01/2012 10:07
De: Primeiro Aviso!
Enviada: sábado, 21 de Janeiro de 2012 00:22
Para:
Assunto: Desculpe a insistencia! PSP
Protocolo N.º 916876923480697819884378910302287194493 5
PROCEDIMENTO INVESTIGATÓRIO N.º 06.5478908568556180 5502/2012
Assunto: CONVOCATÓRIA DE COMPARECIMENTO EM AUDIÊNCIA, relativa ao procedimento investigador em epígrafe, em relação a passada noite de 12 de Janeiro de 2002 decorrido em crime puplico, como poderá visualizar conforme despacho em anexo.
ANEXO: CONVOCA-2012-PSP
POLÍCIA
SEGURANÇA PÚBLICA
Optimizado para: IE7 + | Firefox 3.6 + 1024 x 920
© Polícia de Segurança Pública © todos os direitos reservados


http://www.policiajudiciaria.pt/
Search
The connection was reset
The connection to the server was reset while the page was loading.
The site could be temporarily unavailable or too busy. Try again in a few moments.
If you are unable to load any pages, check your computer's network connection.
If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.
Try Again


From Banco de Portugal <noreply@bportugal.pt>
Subject re: Principios Fundamentais para os Contribuintes
Reply to email@bportugal.pt
To
Banco de Portugal
EUROSISTEMA
Comunicado do Banco de Portugal sobre a Conclusão entre contribuintes e grupos bancários
O trabalhos em causa envolveram oito grupos bancários - Banco Comercial Português (BCP), Banco BPI (BPI), Caixa Geral de Depósitos (CGD), Espírito Santo Financial Group (ESFG), Caixa Económica Montepio Geral (CEMG), Santander Totta (BST), Rentipar Financeira (BANIF) e Sistema Integrado do Crédito Agrícola Mútuo (SICAM), cujos activos representam cerca de 80% do total de activos do sistema bancário nacional.
Documentos Associados
Principios Fundamentais para os Contribuintes (pdf)-345876542
Link malicioso
Lisboa, 20 de Março de 2012
Banco de Portugal © 2009 Todos os direitos reservados.


This web page is not available
chrome
The connection to www.pingodoce.pt was interrupted.
Here are some suggestions:
Reload this web page later.
Check your Internet connection. Reboot any routers, modems or other network devices that you may be using.
Add Google Chrome as a permitted programme in your firewall or antivirus software's settings. If it is already a permitted programme, try deleting it from the list of permitted programmes and adding it again.
If you use a proxy server, check your proxy settings or contact your network administrator to make sure that the proxy server is working. If you don't believe you should be using a proxy server, adjust your proxy settings: Go to the spanner menu > Settings > Under the Bonnet > Change Proxy Settings... and make sure that your configuration is set to "no proxy" or "direct".
Error 101 (net::ERR_CONNECTION_RESET): The connection was reset.


HighTech Brazil HackTeam
Partido Comunista Português hackeado por HighTech Brazil HackTeam
[htbht@hotmail.com.br]
somos
CrazyDuck - No\One - Otrasher
gr33tz
[LLL - Anunnaki - BL4DE - L34NDR0 - Antes Anon - Koubaek_TR_ - Atena - Serpia (viado sumido) - WinRar - SELVAGE - Magoo - MRC]
[Em apoio ao ativismo português]