UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO / IDPCC

I CURSO PÓS-GRADUAÇÃO DE APERFEIÇOAMENTO EM DIREITO DA INVESTIGAÇÃO CRIMINAL E DA PROVA

A PROBLEMÁTICA DA INVESTIGAÇÃO DO CIBERCRIME

ORIENTADOR: PROFESSOR DOUTOR AUGUSTO SILVA DIAS

VERA ELISA MARQUES DIAS

LISBOA, NOVEMBRO DE 2010

ÍNDICE:

Introdução:

Neste estudo propomo-nos abordar a problemática do cibercrime, a face lunar das vantagens da Internet, pois elas facilitam a vida aos cibercriminosos e exasperam os ciberinvestigadores.

Ora, para compreensão do submundo do cibercrime é essencial o estudo das motivações e vulnerabilidades dos seus actores, das específicas características deste tão específico tipo de crime e as dificuldades que as autoridades sentem no seu combate e que os utilizadores têm em prevenir-se.

Mais nos propomos analisar as respostas legislativas nacionais e internacionais que têm vindo a ser dadas a este tipo de criminalidade, nomeadamente a Convenção sobre o Cibercrime e a nova Lei do Cibercrime. Importa, ainda, discutir a aplicação ou não do Direito Penal do Risco ao contexto da criminalidade informática.

Dada a omnipresença da Internet na vida de todos os cidadãos é urgente o conhecimento deste fenómeno criminológico, de modo a poder identificar as causas e as possíveis medidas de prevenção e reacção.

1 O Cibercrime

1.1 A Internet, a Sociedade da Informação e o Cibercrime

Aquando da criação da **Internet**, em 1969, pelo governo norte-americano, com objectivos militares, ninguém vaticinava a importância astronómica que iria ter na vida de todos nós[1]. Alastrando-se por toda a população mundial, tornou-se num cibermundo sem fronteiras espaciais, territoriais, sociais, económicas, culturais, etárias, linguísticas e raciais, surgindo a chamada "**Sociedade da Informação"**. Para a tão falada globalização contribuíram outros factores como as telecomunicações e as redes de transportes, mas foi com a Internet que nasceu a "sociedade global", caracterizada pela interligação mundial de computadores, redes e sistemas informáticos e telemáticos. Com o aparecimento da cibernética, da digitalização e sobretudo de uma comunidade com uma cibercultura e ciberespaço próprio deu-se a evolução para a "**Sociedade Digital**"[2].

A popularidade da internet provém da sua capacidade de proporcionar uma comunicação e circulação transnacional de informação, da amálgama de serviços e dados fácil e instantaneamente disponíveis, e tudo isto à velocidade de um clique a baixos custos. Nos dias de hoje, com especial incidência nos países mais desenvolvidos, a internet tem um papel fulcral ao nível de todas as infra-estruturas estratégicas e nevrálgicas do país, como governamentais, militares, de segurança[3], económicas, de telecomunicações, de transportes, educacionais, energéticas, de saúde e serviços de socorro e emergência. Mas a sua importância não se fica por aqui pois estende-se a todo o tipo de relações, como as comerciais, negociais, empresariais, financeiras e económicas, e com o nascimento das redes sociais, *blogues* e fóruns, passou a fazer parte da vida social, pessoal e dos tempos livres dos utilizadores.

Como podemos constatar, a internet tentacularmente conseguiu infiltrar-se em todos os ramos da nossa vida, fazendo parte integrante dela. A galáxia internet vai ultrapassar os

[1] HUGO LANÇA SILVA, As leis do comércio electrónico: tentativa de desconstrução de um complexo puzzle, Verbo Jurídico, 2007, em http://www.verbojuridico.pt, avança como paralelo de que: "A globalização que tanto se alarde nos nossos dias, se teve a sua génese nas Descobertas dos bravos marinheiros lusitanos, encontra o seu epicentro na Internet"; PABLO MEXÍA GARCIA "El Derecho de Internet", Principios de Derecho de Internet, Prainter, Tirant lo Blanch, Valencia, 2002, p. 99 e ss.

[2] ROVIRA DEL CANTO, Delincuencia Informática y Fraudes Informáticos, Estúdios de Derecho Penal dirigidos por Carlos María Romeo Casabona, 33, Editorial Comares, Granada, 2002, p. 7-9.

[3] Onde se inclui, entre outros, os sistemas de defesa, a segurança de estações nucleares e sistemas de controlo de tráfego terrestre, marítimo e aéreo.

dois mil milhões de utilizadores até ao fim de 2010[4]. Esta interacção dos utilizadores torna a rede extremamente poderosa, sendo uma fonte colossal de comunicação, o que leva à afirmação de que quem não está na *net* está "*unplugged*"[5].

Todavia, as vantagens da internet que levaram a uma explosão de utilizadores e volume de circulação de informação, também levaram à multiplicação na penumbra de **condutas lesivas e ilícitas**, praticáveis e praticadas, na internet, ou por intermédio dela. Foi descoberto um campo fértil, vulnerável, de lucro fácil, com riscos físicos inexistentes, a baixo custo, e com uma grande probabilidade de impunidade, não só para o cometimento de novos delitos, como também para revisitar os crimes tradicionais, agora com a exponencial ajuda e cumplicidade da internet. A própria natureza da rede, ou seja a interconexão de computadores e sistemas, aliada à dependência informática de todos os sectores, deixa-nos a todos expostos e torna-nos alvos extremamente vulneráveis a ataques perante falhas de segurança e dá vida a "*virtual criminal communities*[6] e ao "mundo *underground*"[7]. A forte relação de dependência da sociedade da informação - e com tendência a aumentar – em relação às redes e sistemas informáticos, leva a que o **cibercrime** se torne cada vez mais *frequente, diverso, móvel, internacional* e *perigoso* [8], o que impõe um elevado grau de segurança, fiabilidade e eficiência, de modo a evitar que este crime se torne no almejado crime perfeito. Para tal é necessário que a sociedade de informação assente numa segurança informática que assegura a confidencialidade, a integridade e a disponibilidade fiável dos sistemas[9].

---

[4] O número de utilizadores duplicou nos últimos cinco anos, conforme anunciou a International Telecommunication Union (ITU), acrescentando que 65 por cento estão em países desenvolvidos e apenas 13,5 por cento em países em desenvolvimento, em http://clix.expresso.pt/telecomunicacoes-mais-de-2-mil-milhoes-de-pessoas-com-acesso-a-internet-ate-ao-fim-de-2010=f610310.

[5] MONTEIRO NETO, "Crimes informáticos uma abordagem dinâmica ao direito penal informático, Computer crimes: a dynamic approach on Computer Science Penal Law", Pensar, Fortaleza, volume 8, nº8, Fevereiro, 2003: [39-54], p. 43, em http://www.unifor.br/notitia/file/1690.pdf.

[6] EUROPOL, High Tech Crimes Within The EU: Old Crimes New Tools, New Crimes New Tools, Threat Assessment 2007, High Tech Crime Centre, 2007, p. 36, 32, em http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf; LINO SANTOS, "Cibersegurança – A resposta à emergência", Planeamento Civil de Emergência, Revista nº 19, Ano 2008, in www.cnpce.gov.pt, p. 36.

[7] JUAN SALOM CLOTET, "Delito Informático y su Investigación", Delitos Contra y A Través de las Nuevas Tecnologías Cómo Reducir su Impunidad?, Cuadernos de Derecho Judicial, III, Consejo General Del Poder Judicial, Centro de Documentación Judicial, 2006, p. 106.

[8] Como refere ULRICH SIEBER, Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME-Study-, 1998, p. 60, em http://www.archividelnovecento.it/archivinovecento/CAPPATO/Cappato/Faldone64-12Dirittiumanipaesiextracom/DonneAfghanistan/Desktop/sieber.pdf. O primeiro cibercrime aconteceu nos EUA, nos anos 60, através de um sistema de blue box, v. SÁNCHES MAGRO, "El Ciberdelito y sus Implicationes Procesales", Principios de Derecho de Internet, Prainter, Tirant lo Blanch, Valencia, 2002, p. 261.

[9] PEDRO VERDELHO, "Cibercrime e segurança informática", Polícia e Justiça, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III série, nº 6, Julho-Dezembro, 2005, Coimbra Editora, p. 162.

1.2 Definição, Tipologia e Classificação de Cibercrime

A prática de crimes na internet assume várias nomenclaturas como cibercrime, crime digital, crime informático, crime informático-digital, *high technology crimes*, *computer-related* crime. Não existe consenso quanto à expressão, quanto à definição, nem mesmo quanto à tipologia e classificação destes crimes[10]. Acompanhando a mais recente legislação internacional e nacional adoptamos a nomenclatura de cibercrime, não nos vedando o uso de outras como sinónimo.

Nos últimos tempos, os crimes do ciberespaço mais falados – porque mais frequentes – são *phishing*[11] e o *carding*, o *hacking*, a pedo-pornografia infantil e a pirataria informática. Contudo, a panóplia de tipo de crimes praticada na internet é muito maior e diversificada correspondendo a cada um diferentes ***modus operandi*** e técnicas, que se adaptam constantemente às novas tecnologias. Entre eles podemos referir o *cracking*, *phreaking*, *cracking of passwords*, *identity theft*, *data diddling*, *trojan horse*, *trap doors*, *between-the-lines entry*, *bitknapping*, *pharming*, *SMiShing*, *vishing*, *web defacing*, *phatbot*, *trojan horses*, *botnets*, *worms*, *hijackers*, *keylogger*, *spyware*, bomba lógica ou programa-*crash* e vírus vários[12].

O cibercrime atinge toda a gente e está a aumentar em Portugal e quase duplicou de 2009 para 2010, passou de 600 para 1000 o número de processos por crime informático, resultando em perdas médias de 241 euros[13]. Avisa JAVIER ILDEFONSO que "*Antes, os hackers queriam dar cabo do seu PC. Agora querem dar cabo da sua vida*"[14]

A COMISSÃO EUROPEIA engloba no cibercrime três categorias de actividade criminosa, a saber, os **crimes tradicionais** cometidos com o auxílio do computador e redes informáticas, os **crimes relacionados com o conteúdo**, nomeadamente a publicação de conteúdos ilícitos por via de meios de comunicação electrónicos, e os **crimes exclusivos das redes electrónicas**[15].

---

[10] São várias as classificações na criminalidade informática, como detalhadamente descreve SILVA RODRIGUES, Direito Penal Especial, Direito Penal Informático-Digital, Coimbra, 2009, p.168-194; SOFIA CASIMIRO, A responsabilidade civil pelo conteúdo da informação transmitida pela Internet, Coimbra, Almedina, 2000, p. 19.

[11] Entre Janeiro e Outubro de 2010 o phishing representou mais de dois milhões e meio de euros, em http://diariodigital.sapo.pt/news.asp?section_id=18&id_news=473383&page=0, 13.10.2010.

[12] Para uma definição e descrição detalhada de cada um deles ver: EUROPOL, op. cit., p. 20-45; LOURENÇO MARTINS, op. cit., p. 13-14; GARCIA MARQUES e LOURENÇO MARTINS, op. cit., p. 497, 502-505; SÁNCHES MAGRO, op. cit., p. 272-274.

[13] ANA RITA GUERRA, "Processos de crime informático quase duplicam em 2010", 14.10.2010, http://www.ionline.pt/conteudo/83163-processos-crime-informatico-quase-duplicam-em-2010. Já entre 2007 e 2008 o número de inquéritos associado a esta criminalidade cresceu 293 por cento no espaço de um ano, quanto a valores atingindo o aumento de 870 por cento, passando de 24 mil para mais de 210 mil euros, conforme, LICÍNIO LIMA, "Lei do Crime Ineficaz", Diário de Notícias, 21.11.2009, em http://www.inverbis.net/actualidade/leicibercrime-ineficaz.html.

[14] ANA RITA GUERRA, op.cit.

[15] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l14560_pt.htm. Com outra sistematização, a doutrina e jurisprudência americana aplicam a seguinte divisão de

Já a principal doutrina portuguesa[16] distingue entre quatro grupos a criminalidade relacionada com a utilização de computadores e em especial na internet:

1 - Os crimes que recorrem a meios informáticos, não alterando o tipo penal comum, correspondem a uma especificação ou qualificação deste, são exemplo a devassa por meio de informática (art. 193º do Código Penal), o crime de burla informática e o crime de burla informática nas telecomunicações (art. 221º);

2 - Os crimes relativos à protecção de dados pessoais ou da privacidade (Lei nº 67/98, de 26 de Outubro, transposição da Directiva nº 95/46/CE e a Lei nº 69/98, de 28 de Outubro);

3 - Os crimes informáticos em sentido estrito, sendo o bem ou meio informático o elemento próprio do tipo de crime. Estes crimes são praticados contra e através do computador, este é o alvo da actividade criminosa, também classificados como *vertical use of hi-tech*[17]. Neste grupo inserem-se os crimes previstos na Lei nº 109/2009 de 15 de Setembro;

4 - No último grupo temos os crimes relacionados com o conteúdo, onde se destacam a violação do direito de autor, a difusão de pornografia infantil [art. 172º, nº 3, alínea d)][18] ou a discriminação racial ou religiosa [art. 240º, nº 1, alínea a)]. Neste grupo a reacção repressiva tem de especializar por força do meio utilizado.

---

categorias: "1 Computer as the target (e.g. computer intrusion, data theft, techno-vandalism, techno-trepass). 2 Computer as the instrumentality of the crime (e.g. credit card fraud, telecommunications fraud, theft, or fraud). 3 Computer as incidental to other crimes (e.g. drug trafficking, money laudering, child pornography). 4 Crimes associated with the prevalence of computers (e.g. copyright violation, software piracy, component theft). EOGHAN CASEY, Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet, Academic Press, 2000, p. 17-18.

[16] OLIVEIRA ASCENSÃO, "Criminalidade Informática", Estudos sobre Direito da Internet e da Sociedade da Informação, Almedina, 2001, p. 286-287; PEDRO VERDELHO, "Cibercrime", Direito da Sociedade da Informação, APDI, volume IV, Coimbra Editora, p. 347. Com uma divisão bipartida, SILVA RODRIGUES, op. cit., distingue entre criminalidade informático-digital própria ou "pura" e criminalidade informático-digital imprópria ou "impura". Nos primeiros engloba os crimes em que "o sistema informático ou o fluxo informacional ou comunicacional que neles se encontra armazenado é o objecto da conduta criminosa" (p. 147 e 279 e ss). Quanto aos segundos são os crimes em que o "sistema informático é um meio para a prática de crimes informáticos" (p. 147 e 351 e ss.); Resumidamente concluem GARCIA MARQUES e LOURENÇO MARTINS, Direito da Informática, Lições de Direito da Comunicação, Almedina, 2000, p. 495, que da criminalidade informática fazem parte os "delitos que usam o computador como instrumento, aqueles que o têm por objecto, e ainda os delitos em que o ordenador, sendo ainda um instrumento, é utilizado para violar direitos de personalidade".

[17] EUROPOL, op. cit., p. 4; PAULO SANTOS, RICARDO BESSA e CARLOS PIMENTEL, "CYBERWAR o fenómeno, as tecnologias e os actores", FCA, Editora de Informática, Lda, 2008, p. 12; PEDRO DIAS VENÂNCIO, Breve introdução da questão da Investigação e Meios de Prova na Criminalidade Informática, p. 7.

[18] Alguns diplomas como a Convenção sobre a Cibercriminalidade e a Decisão nº 2000/375/JAI do Conselho da União Europeia de 29 de Maio de 2000 tomaram parte no combate à pornografia infantil na internet e ao aliciamento e perseguição de crianças para fins sexuais («grooming»).

2 Os Sujeitos do Cibercrime

2.1 O sujeito activo / agente

Hoje em dia os grupos criminosos na internet são vários, com diferentes modos de actuação e diversas motivações[19]. A personagem mais conhecida deste mundo virtual do crime é o ***HACKER***[20], tendo as primeiras gerações deste grupo participado no desenvolvimento dos computadores pessoais[21]. Entre os hackers mais famosos temos Kevin Mitnick[22], Dennis Ritchie[23] e Reonel Ramones[24].

A não percepção directa da operação, visto que esta é executada pelo computador com inexistência de presença física do autor e da vítima, o não uso de violência, e, por vezes, o anonimato das duas partes, torna a acção mais fácil, moralmente mais tolerável e com menos riscos para o autor do crime[25]. Este recorre muitas vezes a desculpas de auto-

[19] GARCIA MARQUES e LOURENÇO MARTINS, op. cit., p. 500, ordena a tipologia dos delinquentes informáticos entre amadores, perturbados, membros do crime organizado, quebra sistemas (hackers) e extremistas idealistas. Já quanto à motivação escalona entre utilitaristas, empreendedores, agressivos e destruidores. Por outro lado, EOGHAN CASEY, op. cit., p. 33-39, agrupa os comportamentos em "power reassurance/compensatory, power assertive/entitlement, anger retaliatory/displaced, sadistic/anger excitation, opportunistic, and profit oriented.

[20] Os hackers acedem, sem autorização dos seus legítimos titulares, a computadores, sistemas e redes informáticas ou telemáticas alheias. Quanto ao seu nível de perícia podemos dividir os hackers em três grupos: 1 - Os script kiddies, também conhecidos por losers, short-pants ou lammers, têm um nível baixo, geralmente são jovens estudantes curiosos que se estão a iniciar na informática e que simplesmente reproduzem as técnicas de hacking que são ensinadas em pormenor em muitos sites; 2 - Os hackers de nível médio, com mais experiência, conhecem em pormenor as técnicas e utilizam os programas de outros, não os sabendo escrever nem desenvolver. Estes hackers estudam as vulnerabilidades da rede informática e identificam os potenciais alvos, conquistando o controlo dum sistema de informação; 3 - Os hackers de nível alto, também conhecidos por "Elite" ou "Gurus", são os especialistas e mentores entre estes grupos. São extremamente eficientes, eficazes e metódicos, dedicando-se à criação de vírus, programas e técnicas de hacking, as quais compartilha com os restantes, aconselhando-os e dando inclusive assistência técnica. ULRICH SIEBER, "Criminalidad Informática: Peligro y Prevención", op.cit., p. 77; PAULO SANTOS, RICARDO BESSA e CARLOS PIMENTEL, op. cit., p. 59 e 60; ULRICH SIEBER, "Documentación para una aproximación al Delito Informático", op.cit., p. 78; ROVIRA DEL CANTO, op.cit, p. 109-114. Segundo MORÓN LERMA, in Internet y Derecho Penal: Hacking y otros conductas ilícitas en la red, Pamplona: Aranzadi, 1999, as condutas dos hackers não deveriam ser reguladas pelo Direito Penal. No meio dos cibercriminosos é sagrada a distinção entre hackers e crackers, pois os últimos têm como objectivo a corrupção e quebra dos programas informáticos, apagar informação ou tornar um sistema informático ou mesmo um sítio inoperativo e inutilizável.

[21] Foi o caso de Stephen Wozniak e Stephen Jobs co-fundadores da Apple.

[22] Considerado o mais famoso hacker do mundo, de nickname "Condor" inspirou o filme "Os três dias do Condor". Por aceder às redes do FBI e a redes militares e causar milhões de dólares de prejuízos, foi preso em 1995 e libertado em 2000. PAULO SANTOS, RICARDO BESSA e CARLOS PIMENTEL, op. cit., p. 64; EOGHAN CASEY, op. cit., p. 11-12.

[23] Criou diversos vírus, o sistema operativo mais popular da informática, o UNIX e a famosa linguagem de programação "C". PAULO SANTOS, RICARDO BESSA e CARLOS PIMENTEL, op. cit., p. 63.

[24] Alegado autor do vírus "Love Letter". IDEM, op. cit., p. 66.

[25] MATA Y MARTÍN "Criminalidad Informática: una introducción al Cibercrime", Temas de Direito da Informática e da Internet, Ordem dos Advogados (Conselho Distrital do Porto), Coimbra Editora, 2004, p. 202; XAVIER BELLEFONDS, A Informática e o Direito, Computer Law, Colecção Jurídica Internacional, St. Au Byn, G&A Editores, 2000, p. 50; LOURENÇO MARTINS Criminalidade Informática", Direito da Sociedade da Informação, APDI, volume IV, Coimbra Editora, págs. 9-41, p. 13.

legitimação e à despersonalização da vítima para ultrapassar as barreiras do sentimento de culpa e do desvalor ético-social[26].

O perfil do cibercriminoso é descrito como um génio na área da informática, peritos em computadores e programação, homem[27], estudante com um Q.I. acima da média, introvertido, associal, e que age pelo desafio de superação da máquina[28]. Com esta visão romântica, potenciada pela comunicação social, o criminoso informático é, por vezes, visto como um *Robin Wood* virtual aceite e não censurado pela sociedade, sendo depois de condenados, contratados por grandes empresas[29]. Este perfil, contudo, evoluiu bastante nos últimos tempos e tem vindo a ser substituído por novas categorias criminológicas de delinquentes, não tão jovens nem tão inteligentes, desprovidas de qualquer *tecno-ética*, cujo objectivo já não é quebrar sistemas mas sim extrair informação e usá-la ou vende-la. O móbil preponderante para as práticas ilícitas no meio digital é o *animus lucrandi*, o lucro monetário fácil – "*hacking for dollars*"-, sendo os outros complementares, pois o "*cibercrime é mais rentável do que muitos outros crimes como o tráfico de droga*"[30].

Um dos grupos que nasceu com a ajuda da internet, através de inúmeros *sites* e redes sociais que ensinam detalhadamente como praticar estes crimes, assim como pela disponibilização de *softwares* e *hardwares*, foi o ***CRIMINOSO DE OPORTUNIDADE***[31].

Talvez o grupo mais comum e dissimuladamente letal seja os ***INSIDERS***, também chamados de "cibercriminosos de colarinho branco". Estes são funcionários altamente

[26] GARCIA MARQUES e LOURENÇO MARTINS, op. cit., p. 502.

[27] As mulheres são uma minoria nas comunidades fechadas de hackers. Grace Hooper, considerada a primeira hacker do mundo, criou na década de 50 e 60 a linguagem Flowmatic e Cobol, o primeiro compilador A-O Math Matic. IDEM, op. cit., p. 61; MAJID YAR, Cibercrime and Society, Sage Publications, 2006, p. 35-36.

[28] Mais detalhadamente, o cibercriminoso é introvertido tímido e de instinto aventureiro, destemido, com desejo de notoriedade, de demonstrar as falhas do sistema e aumentar os seus conhecimentos informáticos, prestando, assim, ainda segundo os próprios, "um favor aos incomodados". A competitividade, o status e reconhecimento entre os seus pares, o aumento da auto-estima ou a pura diversão são outras das motivações deste grupo.

[29] A contratação de criminosos informáticos pode ter como objectivo a sua participação no sistema de segurança informática, de modo a eliminar as falhas deste, mas também pode ter intenções ilícitas como o roubo de informação confidencial aos seus concorrentes ou a sua denegrição. ANDRÉS BLASCO, "Qué Es Internet?", Principios de Derecho de Internet, Prainter, Tirant lo Blanch, Valencia, 2002, p. 52; EUROPOL, op. cit., p. 14; Vide também MONTEIRO NETO, op.cit., p. 41; E SALVATORE RESTA, Salvatore, I Computer Crimes Tra Informatica E Telematica, CEDAM – Casa Editrice Dott. Antonio Milani, 2000, p. 176.

[30] EUROPOL, op. cit., p. 4 e 54; Rovira Del Canto, op.cit, p. 108.

[31] Aqui ganha vida o provérbio "a oportunidade faz o ladrão". Com noções mínimas na área da informática, mas com o auxílio referido, ao deparar-se com a facilidade de contornar falhas de segurança e seguros pelo anonimato desta via praticam os chamados "special oportunity crime", quebrando, assim, a resistência que teriam no mundo real para a prática da conduta criminosa. MONTEIRO NETO, op.cit., p. 41; SALVATORE RESTA, op. cit., p. 176-177.

qualificados e colaboradores de confiança da entidade patronal, que se aproveitam do conhecimento interno da empresa, do seu sistema informático e suas debilidades, para praticar actividades ilícitas, como alterações informáticas, eliminação de dados, sabotagem de sistemas ou serviços e venda de informações confidenciais a concorrentes[32]. Por vezes as entidades empregadoras, após o despedimento, esquecem-se de invalidar as credenciais de acesso, o que facilita a vida aos ex-funcionários rancorosos ou com desejo de vingança.

Tendo na sua génese a ideologia defendida, temos o ***HACTIVISM***[33], que recorre ao uso de técnicas de *hacking*, principalmente contra Estados ou grandes empresas, para chamar à atenção e difundir a sua causa, geralmente mensagens políticas. Um dos casos mais famosos foi o da Estónia em 2003, do qual resultaram inúmeros prejuízos[34]. Recentemente o *hacker* Julian Assange tornou-se notícia ao roubar informações confidenciais aos poderes instituídos e divulgá-las no seu *site Wikileaks*[35].

Os grupos mais temidos são as Organizações Criminosas e os ciberterroristas. A maioria das ***ORGANIZAÇÕES CRIMINOSAS*** usa a internet tanto para coordenar os membros como para branquear – *ciber-laudering* - e dissimular as suas condutas ilícitas, recrutando ou contratando técnicos altamente especializados, usando também os cibercrimes como forma de financiamento[36]. O cenário do ***CIBERTERRORISMO*** é algo que, depois do 11.09.2001 nos E.U.A, do 11.03.2004 em Espanha e do 07.07.2005 no Reino Unido, tem sido levado a sério pelos especialistas. Dois dias após a eleição, o Presidente dos E.U.A., Barack Obama, mostrou-se preocupado com a devastação que um ataque terrorista pode provocar a uma

[32] Muitos são viciados na internet – internet addiction disorder - onde se desenrola quase toda a sua vida à parte do mundo real. Entre as suas motivações estão o descontentamento, revolta ou ressentimento contra a entidade empregadora, a resolução de problemas relacionados com dinheiro, a ganância, a vingança, a ascensão profissional ou simplesmente por falta de ética e de deontologia profissional. PAULO SANTOS, RICARDO BESSA e CARLOS PIMENTEL, op. cit., p. 69-73; MAJID YAR, op. cit., p. 34-35.

[33] Como o próprio nome deixa adivinhar o hactivism é a mistura do hacking com o activism, ou seja, o activista usa técnicas de hacking para promover as suas ideias e convicções, de modo a poderem influenciar a tomada de decisões. Vide PAULO SANTOS, RICARDO BESSA e CARLOS PIMENTEL, op. cit., p. 75-84.

[34] Entre Abril e Maio de 2008, a Estónia foi alvo deste fenómeno, quando em reacção à decisão de recolocar na periferia da cidade de Tallin um memorial soviético da II Guerra Mundial, hacktivistas bombardearam os servidores, fornecedores e portais públicos e privados com ataques do tipo DDos, com origem em botnets. De realçar que para além dos enormes prejuízos financeiros e de imagem das empresas, também teve um impacto efectivo na vida dos cidadãos, visto que provocou falhas nas caixas ATM. Outro exemplo foi protagonizado por hactivistas portugueses através de um ataque web deface aos sites do Governo Indonésio aquando o massacre de Santa Cruz em Timor Leste. V. LINO SANTOS, op. cit., p. 35-36.

[35] Este hacker, considerado pela CIA e pelo Pentágono uma perigosa ameaça nacional, "protagonizou a divulgação da maior fuga militar de sempre: 91731 documentos classificados sobre a guerra no Afeganistão", por outro lado recebeu o Prémio Media, da Amnistia Internacional, em 2009 e o Prémio Index Censura em 2008. V. ISABEL NERY, "O guerrilheiro da verdade", Mundo Perfil, Revista Visão, de 29 de Julho de 2010.

[36] EUROPOL, op. cit., p. 17; LOURENÇO MARTINS, op. cit., p. 11.

rede electrónica de sistemas de dados e na economia americana e global[37]. Tendo em conta o elevado grau de dependência dos serviços e infra-estruturas básicas em relação às redes, se a internet for alvo de um ataque, concertado na forma de *cyberattack* ou *cyberwarfare*, poderá levar à paralisação e ao caos do país ou países em causa. Outro dos grandes medos deste tipo de ataque, que usa a globalidade da internet, está relacionado com a possibilidade do massivo número de vítimas atingido[38].

Utilizada por alguns terroristas, como a *Al-Qaeda*[39], a internet é um veículo rápido, barato, anónimo, remoto e global para divulgar informações e propagandas terroristas, espalhar o medo na opinião pública, assim como para recrutar novos membros e treiná-los sem necessidade de presença física. De sublinhar que a propaganda e recrutamento não se destina somente a países árabes, mas a pessoas de todas as nacionalidades[40].

Contudo, avisam PAULO SANTOS, RICARDO BESSA e CARLOS PIMENTEL que muitas vezes "*verifica-se um fenómeno de exploração política e especulação mediática sobre esta temática, que não raro, ultrapassa os limites da realidade, gerando o temor na opinião pública*", surgindo também grupos de pessoas e empresas sedentas pela exploração profissional desta área, aproveitando-se do sentimento de insegurança da população[41].

Podemos, assim, concluir que o cibercriminoso pode ser qualquer um, "*não sendo a personalidade do mesmo nenhum factor determinante, mas sim o seu móbil*"[42].

---

[37] Em BOB WOODWARD, "A Ciberguerra do Futuro", Focus Magazin (trad. Cláudio Castro), Focus 574/2010, p. 106. No mesmo artigo podemos ler que Mike McConnell alertou para a vulnerabilidade dos EUA a ataques cibernáticos, tendo deduzido que se os 19 terroristas do 11 de Setembro tivessem conhecimentos informáticos, poderiam ter provocado um efeito muito maior na economia americana do que a queda das torres do World Trade Center. No seguimento desta preocupação foi recentemente criado o Cyber Command no exército dos E.U.A, sincronizando as redes de defesa e segurança nacionais, pois como afirma Keith Alexander "O espaço digital é essencial para a nossa forma de viver e o Cyber Command sincroniza os nossos esforços em redes de defesa", 4/11/2010, em http://diariodigital.sapo.pt/news.asp?section_id=44&id_news=477020.

[38] Tanto na crise do Kosovo - chamada "The War of the Web" -, como na guerra do Iraque, a internet foi usada pelas células criminosas para o cruzamento e troca de informações e contra-informações, manobras de diversão e engodo. PAULO SANTOS, RICARDO BESSA e CARLOS PIMENTEL, op. cit., p. 85.

[39] Com dificuldades no apoio à sua logística de treinos, a organização terrorista Al-Qaeda tem vindo a treinar os seus recrutas pela Web e pelos chat rooms. V. LINO SANTOS, op. cit., p. 37; Segundo PAULO SANTOS, RICARDO BESSA e CARLOS PIMENTEL, op. cit., p. 85, 88, 90, 93, existem dados que a Al-Qaeda utiliza a internet para "comunicar e disseminar os seus planos operacionais pelos seus elementos", pois "em túneis do Afeganistão utilizados pelos terroristas, tropas americanas encontraram planos da Al-Qaeda para atacar redes de computador e documentos em que se descrevia que recrutas desta organização criminosa estavam a receber formação especializada em sistemas "High-tech".

[40] EUROPOL, op. cit., p. 38; MAJID YAR, op. cit., p. 50-61.

[41] Op. cit., p. 87-88.

[42] ROVIRA DEL CANTO, op.cit, p. 108.

2.2 O sujeito passivo / vítima

A vítima do cibercrime poderá ser qualquer pessoa, física ou jurídica, individual ou colectiva, públicas ou privadas, em qualquer momento ou circunstância, bastando para tal estar ligado a um sistema ou rede informática ou telemática. O elevado número de vítimas e a indeterminação da sua quantidade e identidade leva a inserir estas vítimas na construção dogmática do «sujeito passivo em massa»[43].

O estudo vitimológico da relação entre a vítima e o cibercriminoso pode revelar-se de extrema importância para a identificação do agente, pois podemos estar perante uma *vítima-alvo* sendo a escolha intencional, por existir um elo ou ligação, como no caso de um ex-relacionamento ou ex-empregador, ou perante uma *vítima colateral* ou uma *vítima simbólica*[44].

Os lesados ou vítimas são muitas vezes empresas, Bancos, Seguradoras e entidades financeiras que preferem não apresentar queixa às autoridades e resolver o problema internamente absorvendo as perdas com receio de que tal ataque a ser conhecido leve ao seu descrédito e perda de reputação e confiança junto do mercado e clientes, causando, prejuízos superiores ao ataque sofrido, o que é agravado nas situações em que pode haver responsabilidade legal, devido ao dever de protecção de dados confidenciais[45]. Outra das razões comuns é o desconhecimento ou ignorância do sujeito passivo de que foi vítima, e a crença da ineficácia da investigação policial e na impunidade destes crimes[46]. As vítimas singulares são, por vezes, utilizadores incautos, que negligenciam a segurança permitindo a introdução de programas maliciosos e, por vezes, até ingénuos, fornecendo *passwords* e dados pessoais *on line* sem verificar a sua fidedignidade, o que leva aos crimes de roubo de identidade, ao *phishing* entre outros[47].

---

[43] ROMEO CASABONA, "De los Delitos Informáticos al Cibercrimen. Una aproximación Conceptual y Político-Criminal", El Cibercrimen: Nuevos Retos Jurídico Penales, Nuevas Respuestas Político-Criminales, Granada, Comares, 2006, p. 27.

[44] EOGHAN CASEY, op. cit., p. 164-166, 174-175.

[45] A não cooperação e colaboração da vítima impede uma melhor avaliação das imperfeições e riscos e o aumento do know how das autoridades, da qualidade das medidas de segurança e dos meios de detecção do cibercrime. Contudo, aquela decisão é aprovada por alguma doutrina, como ULRICH SIEBER, "Documentación (…)", op.cit., p. 95; EOGHAN CASEY, op. cit., p. 228, que propõe a criação de uma entidade fidedigna que assegure a privacidade das empresas e dados fornecidos e informando os investigadores de modo que estes possam melhorar o seu trabalho; V. EUROPOL, op.cit., p.27; MAJID YAR, op. cit., p. 14; SALVATORE RESTA, op. cit., p. 180-82.

[46] EUROPOL, op. cit., p. 8, 29; ROVIRA DEL CANTO, op.cit, p. 88.

[47] ANA ISABEL CABO, "Nova lei facilita investigação", Criminalidade Informática, Boletim da Ordem dos Advogados, nº 65, Abril 2010, p. 31; Todavia, mesmo que o utilizador utilize medidas preventivas ou de protecção estas não são infalíveis, sendo quase impossível navegar sem ser alvo de um vírus informático ou dum site comprometido. LINO SANTOS, op. cit., p. 39.

3 As Características do Cibercrime

A problemática do cibercrime advém das suas características, isoladas ou em conjunto, são elas que dificultam a sua prevenção, investigação, repressão e punição e colocam, nos últimos tempos, este tipo de crime nos mais estudados e temidos.

3.1 Transnacionalidade e A-Temporalidade

Como narra SILVA RODRIGUES a internet "*tornou-se numa terra de ninguém e numa terra de todos, num tempo de todos e num tempo de ninguém*"[48]. É com o carácter transfronteiriço ou extra-territorialidade da internet que nos apercebemos da dimensão planetária da rede e entramos no mundo virtual global. Através das redes informáticas internacionais o utilizador consegue aliar a quantidade à velocidade, pois são permitidas enormes transferências de dados e informação, por todo o globo, à velocidade de segundos[49]. Com a ausência de fronteiras estaduais desaparece também todo o controlo feito "entre portas" e potencia a criação de um mundo sem lei[50]. O utilizador consegue, no conforto do seu lar, atingir qualquer pessoa em qualquer país. Por exemplo, um pedófilo em Portugal pode vender imagens pornográficas de menores, através de um servidor americano, a todos os países com acesso[51]. A distância continental entre pessoas, dados e serviços reduz-se a um simples clique. Esta característica leva, assim, a um exponencial agravamento dos danos das condutas criminosas, pois podem atingir um número massivo de pessoas e em qualquer lugar que estas se encontrem.

Já com o seu carácter **a-temporal**, ou seja entre a prática da inicial acção ilícita pelo autor e a sua materialização final através da produção do resultado pode existir uma separação temporal, é possível, ataques faseados, "retardados" ou "ao relógio", como também a sua interrupção, suspensão ou anulação fáctica[52]. Esta é uma das características mais apreciada e aproveitada pelos criminosos, nomeadamente organizações criminosas,

---

[48] SILVA RODRIGUES, op. cit., p. 161.

[49] ULRICH SIEBER, Legal Aspects (...), op.cit., p. 32-33.

[50] A Internet é na sua génese anárquica, sendo famosa a proclamação de Perry Barlow: "Governos do mundo industrial, em nome do futuro, pedimos que nos deixem sós. Não são vocês personas gratas entre nós. Falta-lhes soberania e legitimidade ética para implantar regras ou métodos. Temos motivos de sobra para temer-lhes. O ciberespaço não se ajusta em suas fronteiras"- Declaração de Independência da Internet em 1996.

[51] Ilustrativo é o exemplo dado por FARIA COSTA, Direito Penal e Globalização, Reflexões não locais e pouco globais, Wolters Kluwer, Coimbra Editora, 2010, p. 17, segundo o qual é real a possibilidade de um hacker em Portugal entrar no sistema informático de um hospital brasileiro e desligar a monitorização das funções vitais de um paciente, matando-o.

[52] ROVIRA DEL CANTO, op.cit, p. 96.

podendo "sob controlo *remoto*" praticar crimes, o que permite um detalhado planeamento[53].

3.1.1 A deslocalização

Como refere DIAS VENÂNCIO[54] deparamo-nos tanto com uma deslocação criminosa para a internet, como uma deslocação criminosa na internet. Assistimos, assim, à deslocalização das práticas criminosas para a internet, que antes eram cometidas pelos métodos tradicionais e agora valem-se das ferramentas proporcionadas pelo ambiente digital, o que aliado ao carácter anónimo e à aparente impunidade alicia e conduz certas pessoas a consumarem crimes que de outra forma não praticariam.

E também a uma deslocalização na internet, que consiste na deslocalização de conteúdos[55] de um servidor para outro, para fugir às malhas da lei. Deste modo, ao ser detectada uma actividade proibida ou conteúdos ilícitos num determinado *site*, *e-mail*, ou rede social, pelas autoridades onde o servidor se aloja e aquelas obriguem este a bloquear ou a encerrar o ponto emissor, os infractores simplesmente transferem a actividade e/ou os conteúdos para um servidor de outro país[56]. Ora, deste modo, a competência territorial muda, tornando técnica e juridicamente difícil que as autoridades do país A. imponham que os servidores do país B. executem as suas decisões. E logicamente o cibercriminoso vai escolher deslocar os seus conteúdos para um servidor que se localize num país em que a sua conduta não seja crime ou cuja legislação seja parca ou o favoreça, ou naqueles em que os instrumentos de investigação criminal são deficientes, privilegiando também aqueles que não tenham celebrado acordos de extradição. Estes servidores são os chamados **servidores *off-shore***, "zonas francas" ou "paraísos cibernéticos" e garantem a impunidade aos cibercriminosos[57]. Acusa SÁNCHEZ MAGRO que é necessário

---

[53] SILVA RODRIGUES, op.cit., p. 242- 244; EUROPOL, op. cit., p. 50-51.

[54] Op. cit., p. 6.

[55] Esta técnica de deslocalização de conteúdos conhecida por "mirrors" ou espelhos, que começou como forma de reagir contra as limitações à liberdade de expressão. Esta prática consiste no apelo entre a "comunidade internetiana" para reproduzirem o conteúdo proibido noutras páginas em servidores localizados em países em que tal conduta não é proibida e punível, podendo, devido ao carácter global da internet, ser acedido nos países onde é proibido. Este efeito dominó, em cadeia leva à difusão incontrolável do conteúdo, perdendo-se o rasto às reproduções e torna-se juridicamente impossível punir os seus actores. Vide SOFIA CASIMIRO, op. cit., p. 73-74; PAULO SANTOS, RICARDO BESSA e CARLOS PIMENTEL, op.cit., p. 6-7; e HUGO LANÇA SILVA, op.cit., p.11.

[56] Na mesma linha DIAS VENÂNCIO op. cit., p. 6.

[57] Estabelecemos o paralelo com a afirmação de MARIA JOSÉ MORGADO, "Criminalidade Global e insegurança Local, Um caso, Algumas questões", Colóquio Internacional: Direito e Justiça no Século XXI, Coimbra, 2003, p. 10, em http://www.ces.uc.pt/direitoXXI/comunic/MariaJoseMorgado.pdf, p. 11, quando refere que o mundo é "tornado pequeno demais pela Internet, e grande demais pelos paraísos fiscais". Um dos paraísos cibernéticos mais conhecidos, nomeadamente no caso do worm "I Love You" (2000) são as Filipinas, visto não terem legislação sobre "computer hacking". Vide MAJID YAR, op. cit., p. 2-3; SILVA RODRIGUES, op. cit., p. 239; LINO SANTOS, op. cit., p. 38; JOEL PEREIRA, Compêndio Jurídico Sociedade da Informação, Quid Juris, Lisboa, 2004, p. 500.

responsabilizar os provedores de serviço da internet quanto à identificação e perseguição dos criminosos[58].

3.1.2 A diversidade de ordens jurídicas e o princípio da territorialidade

A **diversidade de ordens jurídicas** existentes e a qualificação diferente de ilícito é outro dos problemas, pois leva a que à mesma infracção sejam aplicadas sanções diferentes e mesmo que uma conduta seja crime num país e noutro não, o que leva à deslocalização.

Apesar da internet ser internacional, quando um crime é praticado temos de determinar qual a lei aplicável. Ora, no caso do cibercrime coloca-se a dúvida se se aplica a lei do país onde está o servidor utilizado pelo infractor, onde o infractor praticou a infracção, onde reside o infractor, ou onde o(s) resultado(s) da sua conduta é produzido, o que se pode verificar em diversos países. O enquadramento do cibercrime tem vindo a ser feito na problemática dos ***delitos à distância***, ou seja, o lugar onde o autor cometeu o crime é diferente do lugar onde o resultado é produzido. Neste contexto a aplicação do princípio da territorialidade[59] puro levaria a grandes limitações e ineficácia da investigação e julgamento destes crimes[60].

A aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses tornou-se mais clara com o art. 27º da Lei nº 109/2009 de 15 de Setembro. Segundo o citado artigo, salvo tratado internacional, a lei penal portuguesa é aplicável aos factos cometidos por Portugueses, se não lhes for aplicada outra lei penal; aos fisicamente praticados em território português ou que visem sistemas informáticos localizados em território português; e também cometidos em benefícios de pessoas colectivas com sede em território português (nº 1). Em caso de conflitos de jurisdição positivos entre Estados membros a decisão cabe aos órgãos e mecanismos instituídos da União Europeia (nº 2). A decisão de aceitação ou transmissão do procedimento deve ser tomada tendo em conta o local da prática dos factos, a nacionalidade do autor e o local onde este foi encontrado (nº 3).

---

[58] SÁNCHES MAGRO, op. cit., p. 286.

[59] A maioria dos países, no qual se inclui Portugal, rege-se pelo princípio da territorialidade (atenuado por outros princípios), ou seja, aplica-se a lei do território onde foi cometida a infracção. Contudo, a transnacionalidade das condutas criminosas levanta problemas quanto à competência internacional em matéria de litígios relativos à internet.

[60] Para a determinação do lugar onde se deve considerar cometido o crime com vista à determinação de qual território é a lei penal é aplicável são defendidas três tipos de teorias: a teoria da acção, a teoria do resultado e a teoria da ubiquidade. Segundo a teoria da ubiquidade é aplicável um critério misto, ou seja, tanto se considera praticado o crime no lugar em que a acção criminosa teve lugar, ou no caso dos crimes por omissão, o lugar em que o autor deveria ter agido (teoria da acção), como no lugar onde se produziu o resultado (teoria do resultado). Este critério é o seguido em alguns países, de forma, a que os delitos à distância não escapem impunes nas falhas de jurisdição, contudo, também pode provocar alguns riscos como conflitos de jurisdição, ou colocar em causa a tradições politico-criminais e jurídico-constitucionais. Vide MATA Y MARTÍN, op. cit., p. 231-234; SÁNCHES MAGRO, op. cit., p. 282-283.

3.2 Permanência, Automatismo e Repetição

A **permanência** do facto é considerada a característica preponderante na ajuda à comissão do crime e determina o carácter automático e repetitivo da conduta criminosa, levando ao aumento exponencial dos danos. Manipulado o programa informático ou alterada a base de dados, em cada novo acesso o computador repete automaticamente o comando criminoso realizado pelo autor, tornando a comissão permanente[61]. O carácter **automático** e repetitivo inerente aos computadores e sistemas informáticos aliados à sua velocidade e instantaneidade leva à multiplicação ilimitada da acção criminosa, atingindo, deste modo, um número indeterminado de pessoas[62]. A possibilidade de **repetição** favorece a reiteração, quase irresistível, na comissão, pois após detectar uma falha ou uma brecha na segurança, vai continuar a aproveitar-se dela quando bem entender[63].

3.3 Anonimato

O **anonimato** é muito apreciado nas redes, poder navegar, visitar e conversar sem ter de se identificar. Contudo, este anonimato quando sai do âmbito do direito à reserva da vida privada e entra na impossibilidade de punição dos actores dos actos ilícitos é abdicável[64].

Inegavelmente o anonimato, a camuflagem ou o uso de identidade falsa é a característica mais aliciadora, tentadora e propulsora para a iniciação da prática criminosa na internet. É, também, a característica mais assegurada, recorrendo os infractores mais especializados ou as organizações através deles a técnicas que lhes permitam ocultar ou dissimular a sua identidade e as suas condutas, como a técnica de *spoofing*, programas de anonimização e codificação, que diariamente são aperfeiçoados e transformados. Para além de se assegurar o anonimato do autor também se pode ocultar a própria informação através de mecanismos de cifra forte ou de encriptação, como a estenografia, e outros disponíveis gratuitamente na rede[65]. Podem, assim, os cibercriminosos diminuir ou eliminar o risco de ser descoberto ou condenado, apagando todas as provas do ciberrastro[66].

---

[61] ULRICH SIEBER, "Criminalidad Informática (...)", op.cit., p. 29-30; ROVIRA DEL CANTO, op.cit, p. 78-79.
[62] SILVA RODRIGUES, op. cit., p. 231 e ss.
[63] ULRICH SIEBER, "Criminalidad Informática (...)", op.cit., p. 29. A configuração destas condutas é para alguma doutrina enquadrada na figura do crime continuado, recorrendo à Parte Geral do Código Penal, enquanto para outros são modalidades de acções criminosas de comissão instantânea e de efeitos permanentes. ROVIRA DEL CANTO, op.cit, p. 78-79.
[64] SOFIA CASIMIRO, op. cit., p. 77.
[65] LINO SANTOS, op. cit., p. 38.
[66] ROVIRA DEL CANTO, op.cit, p. 82. SILVA RODRIGUES, op. cit., p. 228. LINO SANTOS atribui a existência do anonimato a "deficiências técnicas – também chamadas de vulnerabilidades de desenho – nos protocolos e aplicações que suportam as comunicações pela Internet, quer pela falta de regulamentação no acesso", em op. cit., p. 38.

3.4 Alta Tecnicidade

O elevado grau de tecnicidade do cibercrime favorece o anonimato, muitos dos dados estão protegidos por programas de encriptação e palavras passe de modo a barrarem o acesso a terceiros. Ora, a sua descodificação e manipulação de programas, a identificação do infractor, a busca do rasto das operações informáticas e de toda a trama maliciosa, e a recolha de provas digitais aceitáveis em julgamento impõem uma **alta tecnicidade** ao investigador, dificultando tanto a investigação como a prova[67], o que aumenta a probabilidade de impunidade.

3.5 Disseminação e Potenciação dos Danos

A extensa e alta lesividade provocada pelos crimes informáticos ultrapassa em muito a dos crimes tradicionais. Tal deve-se à sua *rentabilidade*, pois o investimento é mínimo em relação ao lucro ou benefício que daí poderá advir, à economia de esforço permitida pelo automatismo e ao potencial elevado número de vítimas que a transnacionalidade faculta. Ao que se junta a disseminação e multiplicação dos efeitos lesivos, através do "efeito cascata" ou do "efeito dominó", consequência da interligação de todos os sectores da sociedade à rede[68]. Por vezes, os danos individuais são insignificantes, os chamados "delitos de bagatela". Contudo, esta diminuta quantia pode atingir quantias astronómicas se somados os prejuízos de todas as pessoas vítimas, afectando inclusive os sistemas informáticos e a segurança e fiabilidade na informação e nos dados[69], sendo o exemplo mais flagrante é a *salami technique* ou a "técnica do salame"[70].

A mesma lógica seguem os *danos morais*, quando o prejuízo não é exclusivamente económico e se atinjam bens como a honra, intimidade privada ou a imagem. Uma mensagem com conteúdos ilícitos na internet pode ter consequências devastadoras e irreparáveis, como por exemplo uma mensagem de cariz difamatório ou racista.

Defende alguma doutrina como resposta a criação de crimes perigo ou risco quando a segurança e fiabilidade da informação, dos dados informáticos e dos sistemas informáticos esteja em causa, não devendo a quantia do prejuízo económico determinar a existência do

[67] SILVA RODRIGUES, op. cit., p. 237.
[68] ROVIRA DEL CANTO, op.cit, p.80; SILVA RODRIGUES, op.cit., p. 235. Um dos crimes que provoca descomunais perdas monetárias é o phishing, estando este fenómeno cada vez mais ligado à criminalidade organizada. V. EUROPOL, op. cit., p. 28-29.
[69] ROVIRA DEL CANTO, op.cit, p. 81.
[70] Usando esta técnica são desviadas quantias diminutas, mesmo cêntimos, de diversas contas bancárias para a do infractor. No entanto, parecendo tratar-se apenas de cêntimos, não havendo grande prejuízo, se essa operação for feita a milhares de pessoas o prejuízo já é muito avultado. O criminoso informático consegue assim uma fonte gigantesca e ilimitada de dinheiro, e as suas pequenas transferências passam despercebidas aos legítimos titulares das contas e às entidades bancárias.

crime em si, a sua consumação ou a execução, nem mesmo como atenuante, só devendo ser atendido para efeitos de qualificação ou agravação do tipo[71].

A denominada ***cifra negra*** ou obscura consiste na quantidade de crimes que não são levados ao conhecimento das autoridades, sendo este número extremamente elevado. Deste modo, não podemos ter conhecimento da realidade do cenário criminoso, o que impossibilita o conhecimento do efectivo número de crimes, o seu estudo, estatística, e reclamação de meios de prevenção e combate[72]. A elevada cifra negra neste tipo de criminalidade tem como causas a falta de denúncia, a grande tecnicidade, a deficiente segurança, a falta de meios de detecção e controlo adequados, a falta de prevenção e a diminuta percentagem de detecção e condenação. Tal leva ao nascimento de um sentimento de impunidade em relação a estes crimes, a que se junta a absorção da criminalidade informática pelos crimes tradicionais levando a que os primeiros não apareçam nas estatísticas[73].

4 As Dificuldades de Investigação do Cibercrime

4.1 Os Problemas

A dificuldade de *prevenção*, *investigação*, *perseguição*, *comprovação* e *punição* sendo uma característica do cibercrime é também a consequência de todas as outras características, sendo estas que a geram. As referidas características facilitam a comissão do crime e ao mesmo tempo dificultam a sua investigação e perseguição judicial[74].

São apontados como principais problemas na investigação a falta de legislação adequada, a falta de metodologia no tratamento da especificidade deste crime, a interoperatividade dos sistemas, e a lentidão da cooperação e falta de partilha de informações tanto entre entidades nacionais diferentes como ao nível internacional[75]. A elevada tecnicidade e especialidade destes crimes, o que aliado ao crescente elevado número de processos e de dados a rastrear, leva a uma elevada morosidade e a encargos

[71] ROVIRA DEL CANTO, op.cit, p. 82; SILVA RODRIGUES, op.cit., p. 236.
[72] SALVATORE RESTA, op. cit., p. 180-182.
[73] SÁNCHES MAGRO, op. cit., p. 267; ROVIRA DEL CANTO, op.cit, p. 88-93.
[74] ROMEO CASABONA, op. cit., p. 3.
[75] EUROPOL, op. cit., p. 24.

económicos e de gestão insustentáveis[76]. Investigações em crimes, como o tráfico de pornografia infantil na internet[77], esbarram com a falta de recursos técnicos e humanos necessários à vasta análise, despistagem, descodificação dos dados, nomeadamente de fotografias e vídeos que estão encriptados ou dissimulados e à identificação e localização tanto dos criminosos como das vítimas[78].

A estas dificuldades junta-se a transnacionalidade que leva a que a cena do crime se estenda por todo o globo, sendo extremamente complexo deslindar o *cibertrail* ou rasto cibernético que se pode alastrar pelos cinco continentes[79]. O *inter criminis* de um cibercrime é muito enleado e elaborado, pois em regra os actos digitais são praticados em diversos pontos, o que envolve vários países e consequentemente diferentes jurisdições.

A ciberinvestigação centra-se, em primeiro lugar, na análise dos dados de tráfego, de modo a localizar a origem da comunicação, ou seja qual o IP (*Internet Protocol)* de origem[80] e a que usuário está esse IP vinculado[81]. Para tal é necessário o acesso ao registo dos ficheiros históricos – *logs* - com ele relacionado e arquivados pelos ISPs[82], cuja

---

[76] ULRICH SIEBER, "Criminalidad Informática (...)", op.cit., p. 32-33; SÁNCHES MAGRO, op. cit., p. 266.

[77] Este crime cada vez mais rentável desemboca em tráfico de seres humanos, imigração ilegal, turismo sexual, lavagens de dinheiro, extorsão, prostituição e abuso sexual de crianças («grooming»). Técnica muito usada pelos pedófilos consiste na auto-instalação de um programa tipo troyano, de modo a criar a dúvida se foi ele a cometer o crime ou outro usuário remoto. SALOM CLOTET, op. cit., 128.

[78] A que agrava o facto dos cibercriminosos estarem a ficar cada vez mais sofisticados, experientes e poderosos devido à troca e venda planetária de informações e conhecimentos entre eles. Um dos recentes métodos usados para evitar a detecção é a "splitting technique", que consiste na divisão de tarefas entre cibercriminosos de várias partes do globo, que são especialistas em determinada área. EUROPOL, op. cit., p. 24, 28; PINÓS FERNÁNDES, op. cit., p. 236. Aqui o que ajuda bastante o investigador é a vaidade do cibercriminoso que deixa a sua marca, o que proporciona linhas de investigação que permitem a sua identificação, como afirma SALOM CLOTET, op. cit., p. 113. As Organizações criminosas são muito bem organizadas e flexíveis, mudando imediatamente de tácticas e técnicas de exploração ilícita da tecnologia quando detectadas pelas autoridades. Muito utilizados por estas Organizações são o phishing, o carding, o tráfico destes dados e o roubo de identidade, que são efectuados sempre de países distantes e não cooperantes, o que torna crítico traçar o rasto do dinheiro e respectiva imputação. V. EUROPOL, op. cit., p. 25, 27.

[79] Como afirma SILVA RODRIGUES (op.cit p. 245): "o rasto cibernético criminoso galga, sem pedir autorizações, as fronteiras de diversos Estados soberanos". O parlamento sul-coreano indicou que os recentes ciberataques feitos esta semana contra o país foram provenientes de 89 endereços IP de 16 países, incluindo os EUA, o Japão e a China, em http://tsf.sapo.pt/PaginaInicial/Internacional/Interior.aspx?content_id=1304530, 10.07.2009.

[80] A forma utilizada para chegar até ao agente é fazer o percurso ao contrário, ou seja, desde o computador da vítima (ponto receptor) até ao computador do agente (ponto emissor) – método reversivo.

[81] É de sublinhar que o usuário poderá não ser o titular do IP. SALOM CLOTET, op. cit., p. 111 e ss, sistematiza a investigação em três fases: a fase prévia, na qual se determina o facto e delito; a fase da investigação, com vista a determinar quem cometeu o crime e como o cometeu; e a fase incriminatória em que se obtém e assegura as provas do crime.

[82] Como refere STEPHEN W. COGAR, Obtaining admissible evidence from computers and internet service providers, The FBI Law Enforcement Bulletin, 2003, em http://www2.fbi.gov/publications/leb/2003/july03leb.-pdf: "The best source for learning the identity of anonymous persons who Access the Internet is through their ISP"; MELGAREJO LÓPEZ, "Investigación Criminal y Proceso Penal: Las Directrices de la Propuesta del Consejo de Europa sobre Cyber-Crime y de la Directiva del Comercio Electrónico", Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet, Aranzadi, 2002, p. 250-252 e 258-264.

colaboração, intervenção e responsabilização é decisiva. Há que desenlear esta cadeia lógica. Identificado o ponto emissor, identifica-se o IP, que poderá estar alojado num domicílio ou local de trabalho[83], mas também num local público. Em seguida a investigação dirige-se na análise do localizado sistema informático, buscando provas da prática da infracção. Mas tal tarefa é extremamente difícil porque para além dos procedimentos técnicos, os investigadores ainda têm de se deparar com programas de anonimização, codificação e anti-rastro, e com a falta de controlo e identificação dos usuários nas empresas e principalmente em locais públicos como cibercafés, universidades ou bibliotecas. De referir que mesmo chegando aos dados de tráfego, estes são insuficientes, mas contêm sempre em si elevados vestígios, a informação só estaria completa com os dados de base e dados de conteúdo mas o acesso a estes, porque compreendem dados pessoais, é restrito e especificamente determinado na lei.

É vital assegurar a viabilidade e aceitação da ***prova digital***[84] em julgamento, assegurando a comprovação dos elementos constitutivos do tipo legal respectivo, pois se a prova não for válida a melhor das investigações será inútil. Para tal é necessário que o acesso, recolha, conservação e análise da prova forense seja sempre efectuado com procedimentos específicos, de modo seguro e expedito mantendo a sua autenticidade, integridade e conformidade à lei[85], competindo essa tarefa a especialistas com conhecimentos técnico-científicos, para evitar contaminações que levarão à sua

[83] Como esclarece PINÓS FERNÁNDES, "Cuestiones Procesales Relativas a la Investigación y Persecución de Conductas Delictivas en Internet", Contenidos ilícitos y responsabilidad de los prestadores de servicios de Internet, Aranzadi, 2002, p. 240.

[84] A prova digital é constituída por dados de tráfego, dados de base e dados de conteúdo e tem como características ser temporária, frágil, alterável, volátil, imaterial, complexa ou codificada/encriptada, dispersa, dinâmica e mutável. Vide SILVA RODRIGUES, op.cit., p. 724-729.

[85] EOGHAN CASEY, op. cit., p. 226-227. O mesmo autor propõe um "digital evidence map" que indique onde a prova de encontra na rede, por quanto tempo irá lá permanecer e quais os procedimentos para a recolher de modo seguro e expedito mantendo a sua autenticidade, integridade e conformidade à lei e afirma que "investigators require detailed information about digital evidence to help them recognize, collect, document, preserve, classify, compare and individualize it" (p. 227). Já DELLA VECCHIA PEREIRA, "Investigação Digital: conceitos, ferramentas e estudo de caso", em http://www.infobrasil.inf.br/userfiles/26-05-S5-2-68766-Investigacao%20Digital.pdf, expõe-nos duas metodologias que conforme o tipo de crime digital em causa devem ser escolhidas pelos peritos, a metodologia Live Forensic, que consiste na investigação do equipamento ainda em funcionamento, permitindo a aquisição de informações voláteis e a metodologia Post Mortem Forensic em que a análise é realizada após o equipamento ser desligado. Nos EUA a Scientific Working Group on Digital Evidence elaborou um documento informativo dos procedimentos a tomar quanto à prova digital – Best Practices for Computer Forensics (em http://www.oas.org/juridico/spanish/cyb_best_pract.pdf, version 2.1, July 2006. Na lógica de que o computador não é apenas o meio de cometer um crime, mas fornece também elementos de prova essenciais de um crime, a União Europeia criou o projecto CTOSE (Cyber Tools On-Line Search for Evidence: Outils de recherche de preuves électroniques) e o C*CAT (Cyber-Crime Adviser Tool), v. SILVA RODRIGUES, op.cit., p. 729-731.

inutilidade[86]. A prova digital não é igual à tradicional, sendo vital a sua rápida e precisa recolha, se não em tempo real, pelo menos em tempo útil, devido ao seu carácter temporário e volátil, de modo a evitar a sua destruição[87]. Esta é uma guerra perdida sem a colaboração expedita e cooperação estreita dos ISPs, que só são obrigados a preservar determinadas categorias de dados e por um tempo limitado[88].

4.2 Algumas Soluções

Para fazer frente aos *cyber*-attacks de grande escala contra as *Critical Information Infrastructures* (CIIs), a Comissão Europeia propõe um plano de acção, contra os *cyber*-attacks de grande escala, baseado em cinco pilares: Preparação e prevenção, recorrendo às equipas de Resposta de Emergência (CERTs - *Computer Emergency Response Teams*[89]) com o apoio da ENISA[90]; Detecção e resposta, desenvolvendo a *European Information and Alert System* (EISAS); Mitigação e recuperação, através de simulações e de uma forte cooperação entre CERTs; Cooperação internacional; e, por fim, estabelecer critérios para *European Critical Infrastructures* no sector das TIC (Tecnologias da Informação e Comunicação)[91].

---

[86] A sua validade depende do cumprimento das regras ao nível "do seu acesso, recolha, armazenamento, transferência, preservação ou apresentação/repetição", em SILVA RODRIGUES, op.cit., p. 727-729. O referido autor defende um modelo de investigação forense digital gizado – Modelo Dinâmico-Reversivo (op.cit, p. 194 e 524 e ss.); Ver também PINÓS FERNÁNDES, op. cit., p. 246.

[87] Como nos alerta PINÓS FERNÁNDES, op. cit., p. 246, nota 38, "No hay que olvidar que cualquier manipulación, por pequeña que sea, altera el contenido de un ordenador, ya sea en los ficheros de registro del sistema operativo o de outro tipo, sin olvidar la posibilidad de que el usuario haya colocado las trampas que haja creído oportunas para destruir determinada información en caso de acceso no autorizado". Porque como refere ULRICH SIEBER, in Legal Aspects (…), op.cit., p. 100: "Due to these new technical developments and to the growing use of computers in all areas of economic and social life, courts and prosecution authorities depend to an increasing extent on evidence stored or processed by modern information technology".

[88] Quanto a esta matéria v. a Lei 41/2004, a Directiva nº 2002/58/CE, de 12 de Junho, a Directiva 2006/24/CE de 15 de Março, a Lei nº 31/2008 de 17 de Julho, a Lei 32/2008, de 17 de Julho, a Portaria nº 469/09, de 6 de Maio. Quanto à responsabilização dos prestadores de serviço v. Directiva 2000/31, de 8 de Junho, o Decreto-Lei nº 7/2004, de 7 de Janeiro.

[89] A nível nacional a FCCN (Fundação para a Computação Científica Nacional), através do seu serviço CERT.PT tem vindo a promover e formar novas CSIRT, tendo uma grande experiência no tratamento, coordenação e resposta a incidentes de segurança informática, como nos é dito no seu site http://www.cert.pt/index.php/pt/institucional/enquadramento-e-motivacao.

[90] Agência Europeia para a Segurança das Redes e da Informação visa o reforço das capacidades da EU, dos Estados-membros e do sector das empresas no que diz respeito à prevenção, resposta, assistência, aconselhamento e gestão de problemas ligados à segurança das redes e da informação. Vide Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004, que cria a Agência Europeia para a Segurança das Redes e da Informação, em http://europa.eu/legislation_summaries/information_society/l24153_pt.htm.

[91] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 30 March 2009 on Critical Information Infrastructure Protection - "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" [COM(2009) 149 final- Not published in the Official Journal], in http://europa.eu/legislation_summaries/information_society/si0010_en.htm. Nesta Comunicação somos

a) Prevenção **-** a melhor arma para detectar, evitar, combater e mitigar os efeitos do cibercrime é a informação, a consciencialização, a prevenção e a preparação, aumentando a *literacia informática*. A prevenção deve ser feita através de sensibilização, seminários, campanhas públicas ou privadas, direccionadas à totalidade da população ou a um determinado grupo de risco, alertando os utilizadores dos riscos e perigos da internet e de como se podem proteger, criando formas de ajuda e acompanhamento, mas também passa pela informação, bom senso e uso responsável de cada utilizador[92]. A prevenção do crime informático deve, assim, ser feita tanto pelas empresas através da tomada de consciência do problema e da imprescindibilidade das medidas de segurança, como pela informação às potenciais vítimas das técnicas de manipulação e seu encobrimento[93].

A outro nível, a aposta deve ser feita no apoio tecnológico e financeiro à investigação e desenvolvimento na área da segurança e em medidas de protecção, como o uso de *passwords* e em técnicas de protecção, como tecnologias que autentiquem o utilizador, o uso de assinaturas digitais, *back-ups* systems, a obrigação de identificação real por detrás dos *nicks* e pseudónimos, filtros entre outras soluções técnicas que assegurem a segurança e fiabilidade nas comunicações[94].

Nesta tarefa, o sistema educativo, o governo, empresas de informática comunicação e segurança independentes e os ISPs têm um papel fulcral no desenvolvimento de soluções técnicas e na criação de infra-estruturas seguras, assim como na informação e educação dos

---

alertados que o World Economic Forum previu, em 2008, uma probabilidade de 10 a 20% de um ciber-ataque de grande escala nos próximos dez anos, que ascenderá a prejuízos de USD 250 biliões.

[92] EUROPOL, op. cit., p. 30-31; SILVA RODRIGUES, op.cit., p. 238. Não são só os chamados utilizadores privados que não estão suficientemente informados acerca dos perigos da sociedade da informação, que não se previnem contra os cibercrimes ou que desconhecem quais as medidas de protecção que devem usar, também, as empresas e indústrias, os governos e os políticos e quase todos os ramos da nossa sociedade pecam neste conhecimento. Vide ULRICH SIEBER, Legal Aspects (…), op.cit., p. 207. Como refere CARLOS GAMEIRO, "O Risco da Informação em Ambiente Electrónico", Estudos de Direito e Segurança, Faculdade de Direito da Universidade Nova de Lisboa, Almedina, 2007, p. 135: "O atingir dos objectivos de protecção, passa por uma política concertada entre o Estado, as organizações e o cidadão/utilizador.

[93] Para alguns a descrição detalhada das técnicas de sabotagem é prejudicial porque deste modo se estaria a ensinar futuros cibercriminosos. Contudo, tal é essencial para alertar as vítimas que não estando familiarizadas com estas técnicas ficam expostas e desprotegidas perante os ataques maliciosos. E também é manifesto que estas técnicas já são conhecidas e dominadas entre a comunidade de piratas informáticos e aqueles que se querem iniciar neste caminho têm muitos sites, livros e revistas especializados que ensinam a técnica em pormenor, inclusive com o auxílio de hackers experientes, é o caso do "Jargon File" e do "The Hacker´s Dictionary". Vide EUROPOL, op. cit., p. 13; ULRICH SIEBER em "Criminalidad Informática (…)", op.cit., p. 34 e em "Documentación (…)", op.cit., p. 77.

[94] ULRICH SIEBER, Legal Aspects (…), op.cit., p. 201-202. Para atingir esse objective é necessário ter em conta o custo financeiro das medidas de segurança, pois nem todos os utilizadores têm essa capacidade de investimento.

utilizadores[95]. Essencial é, também, a investigação e o estudo detalhado dos factores criminógenos, de modo a poder antever e assim prevenir o desenvolvimento de novas formas de cibercrime, tomando medidas eficazes no seu combate. Uma efectiva protecção impõe o conhecimento das causas e origens do cibercrime, "*a identificação das ameaças, a redução das vulnerabilidades, minimizando os danos e o tempo de reacção*"[96].

b) Multidisciplinaridade **-** as técnicas de investigação e perseguição criminal de crimes cibernéticos têm de se apoiar noutras ciências, como a engenharia e tecnologia informática, a psicologia criminal, a sociologia, a ciência forense criminal, entre outras, pois só desta forma se poderá cimentar a *Ciência Forense Digital*[97]. É essencial que o investigador digital se faça acompanhar de especialistas na área, que dominem as redes e as técnicas, pois só assim poderá interceptar, interpretar e conservar apropriadamente os dados.

c) Formação e recursos adequados aos profissionais **-** o sucesso da investigação depende da formação e treino especializado das autoridades policiais, judiciárias, advogados e restantes operadores jurídicos e funcionários[98]. Afigura-se urgente a criação de polícias especializadas - os previstos *cibercops*, "*electronic police patrols*"[99] ou *Task Forces especializadas*[100] - com elevados conhecimentos científicos, técnicos e forenses na área. Vaticina LOPES ROCHA que "*a polícia do futuro muito próximo vai ser metade humana, metade robô*" e que quanto "*aos tribunais, há escolhas a fazer: especialização e carreiras novas*" [101].

Capital é também a existência de apoio financeiro e de recursos técnicos, humanos e monetários, sendo este o "calcanhar de Aquiles" em relação às poderosas Organizações Criminosas, com acesso à tecnologia de ponta. Só através do conhecimento do funcionamento da rede e do domínio do ciberespaço se poderá fazer uma perseguição em

---

[95] IDEM, p. 203-204. PEDRO VERDELHO defende que a via mais eficaz consiste na "definição de boas práticas, não obrigatórias, que confiram fiabilidade e segurança aos ISP, levando os utilizadores a optar por aqueles que lhes ofereçam mais garantias" (em "Cibercrime e segurança informática", op. cit., p. 169).

[96] CARLOS GAMEIRO, op. cit., p. 132.

[97] SILVA RODRIGUES, op.cit., p. 229.

[98] ULRICH SIEBER, "Criminalidad Informática (...)", op.cit., p. 33; EOGHAN CASEY, op. cit., p.223. Em Portugal, é da competência reservada da Polícia Judiciária, em todo o território, a investigação da criminalidade informática.

[99] ULRICH SIEBER, Legal Aspects (...), op.cit., p. 103 e ss.

[100] COM/97/0157: "Um problema cada vez mais preocupante é o aparecimento dos cibercrimes, como lavagem electrónica de dinheiro, jogos a dinheiro ilegais, intrusão maliciosa e violação dos direitos de autor. Na Europa (Europol), bem como no contexto internacional mais vasto (P8) foram criadas Task Forces especializadas e foi reforçada a cooperação operacional transfronteiras em áreas fundamentais como a "caça" em tempo real e da "busca e apreensão" de elementos de prova digitais."

[101] Op. cit., p. 33.

tempo real, diminuir o tempo de busca, e realizar uma correcta recolha de prova digital que permita a condenação dos infractores.

d) Regulação internacional – a uniformidade legal internacional tanto a nível substantivo como processual permite uma maior compreensão e operacionalidade entre as autoridades dos diferentes Estados. É exigido ao legislador uma grande capacidade de previsão, adaptação e acompanhamento dos desenvolvimentos técnicos[102] e da multiplicação de condutas criminosas, que se desenrolam a uma velocidade não compatível com a técnica legislativa. Só com quadros normativos similares[103], a cooperação internacional será verdadeiramente eficaz, extinguindo-se os "paraísos cibernéticos". Sendo de referir a inabdicável conformidade com a protecção dos direitos humanos assegurada nas diversas Convenções e legislações[104]. Neste âmbito seria de extrema importância a ratificação da Convenção sobre o Cibercrime pelo maior número de países.

Todavia, a legislação não deverá ser somente criminal, devendo inclusive apoiar-se na lei civil e administrativa, que por vezes se torna bem mais eficaz[105]. Apoiada é também a criação de códigos de conduta ou regras informais, a chamada *soft law*.

e) Comunicação, cooperação e coordenação internacionais - A decifração desta problemática assenta na seguinte imposição: "*para combater uma rede é preciso responder com uma rede*"[106], ou seja, é necessária uma rede com vários pontos de contacto que dê o alerta de emergência e uma resposta rápida e eficaz, diminuindo os tempos de resposta e o agravamento dos danos. Os autores são unânimes na solução apresentada para combater estes crimes e tal passa incontornavelmente pela cooperação internacional, a exemplo do Acordo *Shengen*, da Rede Judiciária Europeia, da Eurojust ou da Europol[107], que deve ser feita tanto a nível estatal e das autoridades policiais e judiciais, como pelas empresas e entidades privadas, nomeadamente a industria de comunicação, ou organizações[108]. O ideal será a comunicação, a interligação próxima, a entreajuda operacional através da partilha de

---

[102] LINO SANTOS, op.cit., p. 38.

[103] PEDRO VERDELHO, "A nova Lei do Cibercrime", Lei nº 109/2009, Boletim da Ordem dos Advogados, nº 65, Abril 2010, p. 34. A inexistência de harmonização dos tipos legais dificulta em muito a cooperação, exemplo disso é a punição do facto somente quando houver prejuízo patrimonial nos E.U.A.

[104] Como a Declaração Universal dos Direitos do Homem, a Convenção Europeia dos Direitos do Homem ou a Convenção para a Protecção dos Direitos do Homem e das Liberdades Fundamentais.

[105] ULRICH SIEBER, Legal Aspects (…), op.cit., p. 198.

[106] HILLAR AARELEID, responsável pelo CSIRT da Estónia, apud LINO SANTOS, op.cit., p.41.

[107] ROMEO CASABONA, op. cit., p. 61-64; SOFIA CASIMIRO, op. cit., p. 76; LINO SANTOS, op.cit., p. 39.

[108] Exemplo desta visão no sector empresarial internacional é a criação por líderes empresarias mundiais do GBDe – Global Business Dialogue on Electronic Commerce, que consiste numa rede de políticas de desenvolvimento da economia online. PEDRO VERDELHO, "Cibercrime e segurança informática", op. cit., p. 166.

informações, *know how*, e a articulação em tempo real entre todas estas entidades, ao nível internacional[109].

A resposta a ataques coordenados e de grande envergadura, cometidos contra infra-estruturas nacionais de informação, só é possível com uma colaboração global, tal foi evidente no caso da Estónia que só com a conjugação de esforços de equipas de segurança (CSIRT) e de ISPs internacionais foi possível superar a situação. Um Estado isolado não teria meios técnicos nem humanos para controlar e por termo a um ciber-ataque de grande dimensão[110]. A este nível, é essencial a criação de pontos de contacto, quer ao nível estatal ou privado, de equipas internacionais de resposta a emergências e de medidas tecnológicas de protecção e de segurança[111], que assegurem a mútua colaboração, assistência e repressão internacional no combate eficaz ao cibercrime. A cooperação e a colaboração são vitais não só para o combate a ataques globais, mas também à complexa prevenção, detecção, perseguição, comprovação e repressão deste tipo de crimes, porque o "*crime moveu-se da esfera local para a transnacional ou global e é necessário acompanhá-lo nessa viagem*"[112]. Deve, pois, ser combatida com as mesmas armas, ou seja, aproveitando as ferramentas oferecidas pela Sociedade da Informação na prevenção, investigação, prova e repressão da conduta ilícita[113].

f) Outras: outras propostas vão no sentido da atribuição de funções de ordenação e sancionamento aos ISPs, exigindo-se para o acesso a aceitação de códigos de conduta predefinidos, da arbitragem por magistrados virtuais dirimindo conflitos entre os utilizadores, da criação de Tribunais *ad hoc* ou de Tribunais Internacionais com uma única legislação aplicável e com uma só jurisdição, ou por alternativas extrajudiciais, como os mecanismos de solução extrajudicial de conflitos[114].

---

[109] Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões - Rumo a uma política geral de luta contra o cibercrime [COM(2007) 267 final – não Publicada no Jornal Oficial], in http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l14560_pt.htm; EUROPOL, op. cit., p. 25-26.

[110] LINO SANTOS, op.cit., p. 36, 38.

[111] ULRICH SIEBER refere que "the most effective means against illegal actions in the field of computer crime are technical and organizational safety measures", em Legal Aspects (…), op.cit., p. 208; ROMEO CASABONA, op. cit., p. 68.

[112] SILVA FERNANDES, op. cit., p. 109.

[113] ULRICH SIEBER refere que "the most effective means against illegal actions in the field of computer crime are technical and organizational safety measures", em Legal Aspects (…), op.cit., p. 208; ROMEO CASABONA, op. cit., p. 68.

[114] CLAUS ROXIN, Pasado, presente y futuro del Derecho Procesal Penal, Colección Autores de Derecho Penal, Rubinzal – Culzoni Editores, 2007, p. 62-70; SÁNCHES MAGRO, op. cit., p. 284-286. Contudo, a criação de órgãos ou legislações internacionais esbarram com a soberania estatal e a diversidade de legislações de cada país, podendo passar a solução pelo alargamento de competência das jurisdições dos estados. Exemplo de alternativa extrajudicial é a criação de um centro de arbitragem internacional pela OMPI (Organização Mundial de Propriedade Intelectual), para a litígios em matéria de propriedade intelectual.

5 Possíveis Soluções Político-Criminais, em especial, o Direito Penal do Risco

5.1 O Direito Penal do Risco

A discussão em torno da "**Sociedade do Risco"** apareceu nos anos 80 relativamente aos perigos tecnológicos, como os industriais, os nucleares, os ambientais e a manipulação genética. Foi ULRICH BECK que se debruçou sobre o estudo da Sociedade do Risco, sendo um dos primeiros a reconhecer o estranho paradoxo de que o risco pode ser aumentado com o desenvolvimento e progresso da tecnologia, ciência e industrialismo, ao contrário do que seria esperado[115]. Os chamados novos riscos estão directamente relacionados com o fenómeno da globalização e com a insegurança derivada dos desenvolvimentos técnico-científicos. São infligidos ou potenciados por decisões humanas não intencionais, são transfronteiriços, ubiquitários, transgeracionais, imprevisíveis, indetectáveis, invisíveis, inseguráveis, incalculáveis, dinâmicos, complexos, têm uma dimensão social, desenvolvendo-se e transformando-se técnico-socialmente muito rápido, e escapam ao controlo[116]. Para enfrentar estes novos riscos a sociedade, com medo e insegura, refugia-se e recorre ao Direito Penal, que na forma de "**Direito Penal do Risco**" responde numa

[115] Afirma o famoso sociólogo alemão que nos encontramos perante uma modernidade reflexiva ou segunda modernidade reflexiva, que consiste num processo de autoconfrontação com os efeitos da sociedade do risco com os próprios fundamentos do desenvolvimento desmesurado e as antinomias em relação à primeira modernidade. V. ULRICH BECK, World Risk Society, Polity Press, Cambridge, 2000, p. 133 e ss.; ULRICH BECK, "A Reinvenção da Política, Rumo a uma teoria da modernidade reflexiva", Modernização Reflexiva: Política, Tradição e Estética no Mundo Moderno, Celta Editora, Oeiras, 2000, p. 2, 5 e 6; SILVA DIAS, Ramos Emergentes do Direito Penal Relacionados com a Protecção do Futuro (Ambiente, Consumo e Genética Humana), Coimbra Editora, 2008, p. 22 e em «Delicta In Se» e «Delicta Mere Prohibita»: Uma Análise das Descontinuidades do Ilícito Penal Moderno à Luz da Reconstrução de uma Distinção Clássica, Coimbra Editora, 2008, p. 223 e ss.; SILVA FERNANDES, Globalização, "Sociedade de Risco" e o Futuro do Direito Penal, Panorâmica de alguns problemas comuns, Almedina, 2001, p. 55 e ss.; ULRICH BECK, A Sociedade Global do Risco, Uma discussão entre Ulrich Beck e Danilo Zolo, trad: Selvino J. Assmann, 2000, in http://www.cfh.ufsc.br/~wfil/ulrich.htm); DARRYL S. L. JARVIS, Theorizing Risk: Ulrich Beck, Globalization and the Rise of the Risk Society, Lee Kuan Yew School of Public Policy, NUS – National University of Singapore, http://www.risk-and-regulation.com/wp-content/uploads/2010/05/RR3-Beck.pdf, p. 4, 9-12).

[116] Como explana ANTHONY GIDDENS, "Viver numa sociedade pós-tradicional", Modernização Reflexiva: Política, Tradição e Estética no Mundo Moderno, Celta Editora, Oeiras, 2000, p. 92, a "globalização é uma questão ´aqui dentro' que afecta, ou melhor, que está dialecticamente relacionada com os pormenores mais íntimos das nossas vidas". Ao que ULRICH BECK, World Risk Society, op. cit., p. 142, acrescenta "The global threats have led to a world in which the foundations of the established risk logic are undermined and invalidated, in which there are only difficult-to-control dangers instead of calculable risk. The new dangers destroy the pillars of the conventional calculus of security (…)", vide também p. 143; Sobre a temática, ULRICH BECK, "A Reinvenção da Política, Rumo a uma teoria da modernidade reflexiva", Modernização Reflexiva (…), op.cit., p.4; SILVA DIAS, Ramos Emergentes (…), op. cit., p. 22-24 e em «Delicta (…)», op. cit., p.229-232; SILVA FERNANDES, Globalização, op. cit., p. 48-49. ULRICH SIEBER, Legal Aspects (…), op.cit., p. 196; NIEVES SANS MULAS, "La Validez del Sistema Penal Actual Frente a los Retos de la Nueva Sociedad", El Sistema Penal Frente a Los Retos de La Nueva Sociedad", Editorial Colex, 2003, p. 11-13; FIGUEIREDO DIAS, O Papel do Direito Penal na Protecção das Gerações Futuras, em http://www.defenseociale.org/revista2002/8.1.htm.

lógica preventiva e antecipa a tutela[117] dos bens jurídicos supra-individuais considerados essenciais, tipificando condutas de *perigo abstracto*[118], reformulando e flexibilizando categorias clássicas, através da punição de condutas negligentes ou tentadas, abdicando de relações de causalidade, de critérios típicos de imputação, do dolo e do princípio da taxatividade.

Devido à transformação e evolução tecnológica, à sua complexidade e dinamismos, que levam ao surgimento de novas modalidades e formas de comissão, na formulação tipológica requer-se a criação de tipos delituais amplos, utilizando cláusulas gerais e conceitos indefinidos ou *leis penais em branco*, para flexibilizar os tipos penais e que devem ser elaborados com critérios uniformes a nível internacional[119], equiparando-se, em prol de uma maior funcionalização, a responsabilidade das pessoas colectivas à das pessoas físicas[120]. O grande desafio é o equilíbrio entre a segurança e a mínima restrição às garantias e liberdades fundamentais dos cidadãos[121]. MARIA JOSÉ MORGADO julga essencial a incriminação cada vez mais ampla e menos vinculada nestas formas especiais do crime e coloca a questão "*da necessidade dum direito penal preventivo, capaz duma intervenção mais eficaz, sem nunca beliscar as garantias essenciais do processo criminal democrático*"[122].

Contra o Direito Penal do Risco acusa-se a excessiva antecipação da tutela, a sobre-criminalização na protecção de interesses colectivos, o excesso de proibições *per se*, e o prejuízo de figuras de responsabilidade estrita[123]. Critica-se a criação de um direito penal do risco com cariz de prevenção geral de intimidação, que não atenta à prevenção geral de

---

[117] Como refere SILVA DIAS, Ramos Emergentes (...), op. cit., p. 26, promove-se um Direito Penal preventivo centrado na "gestão dos riscos". A antecipação da tutela recua a um ponto anterior à lesão, bastando-se com a probabilidade da mesma, com a perigosidade da mera acção, adequada a abstractamente a provocar uma possível lesão do bem, mediante um juízo ex ante de perigosidade, como explica SILVA FERNANDES, op. cit., p. 94.

[118] Sobre a validade dos crimes de perigo abstracto v. FARIA COSTA, O Perigo em Direito Penal (...), op.cit., p. 620-652.

[119] ROVIRA DEL CANTO, op.cit, p. 44 e 188; SILVA RODRIGUES, op.cit, p. 238, 227.

[120] SILVA FERNANDES, op. cit., p. 86; ULRICH SIEBER, Legal Aspects (...), op.cit., p. 197.

[121] ROMEO CASABONA, op. cit., p. 68; JOSÉ EDUARDO DE FIGUEIREDO DIAS, "Direito à Informação, Protecção da Intimidade e Autoridades Administrativas Independentes", Estudos em homenagem ao Prof. Doutor Rogério Soares, Stvdia Ivridica 61, Ad Honorem-1, Boletim da Faculdade de Direito, Universidade de Coimbra, Coimbra Editora, 2001, 615 e ss., 632-634, 652, analisa os problemas de articulação do direito à informação com a protecção da intimidade da vida privada e a sua potenciação na sociedade do risco e da informação, nomeadamente no ciberespaço.

[122] Op. cit., p. 10; enuncia também "alguns dos grandes desafios do direito e processo penal do século XXI: - o reforço dum direito e processo penal de intervenção com salvaguarda do princípio da culpa jurídico penal; - o reforço dum direito penal do risco, capaz de maior eficácia na protecção dos interesses individuais e colectivos com salvaguarda das garantias do processo penal democrático; - Um direito Penal capaz de fazer face aos riscos da vida moderna e das novas formas de criminalidade organizada global sem perder a sua face humana e justa. - Um direito penal dum mundo tornado pequeno demais pela Internet, e grande demais pelos paraísos fiscais" (p. 11).

[123] ROVIRA DEL CANTO, op.cit, p. 49-50; SILVA FERNANDES, op. cit., p. 71-75.

integração nem se preocupa com a real defesa da ordem jurídica, de duvidosa constitucionalidade, vulnerando os princípios do direito penal liberal, sendo politizado, instrumentalizado e com tendências totalitaristas[124]. Despoletado pelo 11 de Setembro o *Direito Penal do Inimigo* assenta na luta contra o terrorismo, o qual se associa o ciberterrorismo, transformando o Estado num "*voyeur*", que através de medidas extremas, discricionárias, populistas e irracionais controla a vida dos cidadãos que vivem como que num aquário debaixo do olho do "*Big Brother*"[125].

5.2 O Direito Penal do Risco Informático e da Informação

Quanto à ***criminalidade informática*** coloca-se a questão da sua inserção ou não na sociedade do risco, sendo objecto da protecção do Direito Penal do Risco, resposta que divide a doutrina.

a) Do lado do sim, ROVIRA DEL CANTO defende acerrimamente o "***Direito Penal Global do Risco Informático e da Informação***"[126] e enquadra a nova criminalidade praticada através das tecnologias informáticas e da informação na sociedade do risco[127]. Segundo ROVIRA DEL CANTO as respostas doutrinais à problemática da criminalidade informática incidiram em três teorias, a saber: a *teoria da Lei Penal da Informação*[128]; a *teoria da harmonização legal internacional*[129]; e a *teoria da sociedade do risco*. Propondo,

[124] DYELLBER ARAÚJO, "Institutos Penais de Emergência – "Novas" Fórmulas para Velhos Dilemas – Uma Análise dos Novos Estudos de Política Criminal Voltada aos Indesejados pela Sociedade", Direito Penal Hoje Novos desafios e novas respostas, Coimbra Editora, 2009, p. 146; SILVA FERNANDES, op. cit., p. 91-92 e 114.

[125] No pólo oposto encontramos o Direito Penal do Cidadão que pugna pelas esferas de liberdade. V. DYELLBER ARAÚJO, op. cit., p. 165 e ss; SILVA DIAS, «Delicta (…)», op. cit., p. 264-265.

[126] Op.cit, p. 53-56. O autor fundamenta a sua necessidade, descrevendo e aplicando-o a todas as características e factores do cibercrime, op. cit., p. 116-118.

[127] Já SILVA RODRIGUES, (op.cit, p. 22, 200 e ss.), prefere a nomenclatura de "Direito Penal Informático-Digital" (p. 194). Para alguns autores o "Direito Penal Informático" tem autonomia normativa e científica, enquanto, que para outros é somente uma específica área de incriminação penal referente à informática, como podemos constatar em SILVA RODRIGUES, op.cit, p. 194 e ss. / FARIA COSTA, "Algumas Reflexões sobre o Estatuto Dogmático do Chamado "Direito Penal Informático", Direito Penal da Comunicação (Alguns escritos), Coimbra Editora, 1998, p. 112-119 e em "Les Crimes Informatiques et d´Autres Crimes dans le domaine de la Technologie Informatique au Portugal", idem, p. 17-18; JOÃO BARBOSA DE MACEDO, "Algumas Considerações Acerca dos Crimes Informáticos em Portugal", Direito Penal Hoje Novos desafios e novas respostas, Coimbra Editora, 2009, p. 228; MAJID YAR, op. cit., p. 11-12.

[128] Segundo a teoria da Lei Penal da Informação, a informação constitui um novo bem económico, cultural e político mas também um potencial perigo, o que conduz à necessidade de efectuar-se de uma regulação penal dos bens imateriais, que logicamente deve ser feita em moldes diferentes da dos bens materiais atenta a sua especialidade (op.cit, p. 188).

[129] Já a teoria da harmonização legal internacional nasce como uma resposta da sociedade global a esta nova criminalidade. É notório que reacções nacionais isoladas são ineficazes e estão destinadas ao fracasso. A mobilidade transnacional, à velocidade de meio segundo, de dados e informação exige também uma resposta internacional assente numa estratégia adequada e comum. Só com uma intensa e contínua cooperação entre os Estados e as organizações supranacionais se pode almejar uma eficaz prevenção e perseguição destes crimes (op .cit, p. 51-52).

o mesmo autor, a conjugação das referidas teorias complementando-se entre si, como modo adequado de reacção. Defende uma evolução e modificação estrutural e tipológica do actual Direito Penal, constituindo um Direito Penal Global do Risco Informático e da Informação, que seria composto por um "*conjunto de normas penais reguladoras dos ilícitos vinculados aos riscos derivados do uso de meios informáticos e telemáticos, os dados e a informação em si mesma*[130].

O objecto desta protecção reforçada é a informação e os dados em si mesmos, como bens de valor económico-social e a segurança e fiabilidade colectiva da sociedade nos sistemas e redes informáticas e de telecomunicações[131]. A diferença existente entre os crimes informáticos e os crimes tradicionais impõe a adequação e transformação das medidas a tomar para combater os primeiros, o que leva a uma mudança de paradigma. Sustenta ULRICH SIEBER que, na moderna sociedade do risco, os esforços para reduzir os riscos devem incidir em medidas técnicas, estruturais e educacionais, tendo sempre em conta a especificidade do bem informação e sendo esta uma sociedade global todas as medidas devem ser concertadas internacionalmente[132].

Esta posição defende que se estivermos perante um uso indevido de elementos ou sistemas informáticos e de telecomunicações que suponham um ataque grave à informação e aos dados em si mesmos, aos programas, sistemas ou redes informáticas e de telecomunicações, e quando seja susceptível de afectar a mesma em relação à segurança, fiabilidade e utilização pacífica, devemos enquadrar estas condutas no crime de risco informático e da informação, cujas modalidades devem ser previstas expressamente e analisadas no âmbito do Direito Penal do Risco Informático e da Informação. Caso contrário, ou seja, se não houver possibilidade de afectação, directa ou indirecta, não estamos perante um crime de risco informático e da informação[133].

b) Do lado do não, SILVA DIAS coloca a criminalidade informática fora dos novos riscos da sociedade do risco e da protecção do futuro, pois defende que se trata de novas

[130] Op.cit, p. 53-56. Sendo o bem jurídico a proteger – a informação e os dados em si mesmos e a segurança e fiabilidade dos sistemas e redes informáticas e de telecomunicações – de natureza pluriofensiva e colectiva e existindo um grave e sério risco que ameace afectar este bem é justificada a técnica da tipificação dos crimes de perigo. Op.cit, p. 44-45, 187; e LOURENÇO MARTINS, op. cit., p. 17.

[131] ROVIRA DEL CANTO, op.cit, p. 187. O lado negro do rápido progresso e evolução das novas tecnologias informáticas e o aperfeiçoamento dos hardwares e dos softwares desemboca no medo e a insegurança dos cidadãos e a incapacidade de resposta dos Estados face a esta nova criminalidade.

[132] A informação é o actual principal bem económico, cultual e politico, mas simultaneamente, e por causa disso, um grande perigo potencial. Para fazer face a estes perigos, o legislador tem de atentar à mudança social de paradigma de bens materiais para bens imateriais e a estes não é adequada a analogia das regras dos primeiros, v. ULRICH SIEBER, Legal Aspects (...), op.cit., p. 194-195, 201.

[133] Conclui ROVIRA DEL CANTO, op.cit, p. 188.

formas de agressão a interesses eminentemente individuais, não autónomas relativamente aos bens jurídicos clássicos, cujos efeitos "*se esgotam num tempo presente consubstanciado na vida do acto ou da vítima*", e "*não são geradoras de grandes riscos que afectem ou comprometam as bases naturais da existência humana presente e futura*"[134]. Na mesma lógica, FARIA COSTA acusa a existência de uma tentativa de diabolização da informática o que leva a dar corpo a todas as formas para a sua possível contenção e defende que a **específica área da incriminação referente à informática** pode continuar a estudar-se com os instrumentos tradicionais do direito penal, podendo ser perfeitamente inseridos nos títulos de crimes já existentes, como contra as pessoas e contra o património[135].

6 A Resposta Legislativa

6.1 Internacional

Alguns Organismos Internacionais têm-se debruçado sobre o assunto, como a **OCDE**[136], a **O.N.U**[137], a Interpol, o *P8 Countries*[138], entre outros. A **União Europeia** tem dedicado especial atenção ao cibercrime tendo legislado através de diversos instrumentos jurídicos neste âmbito, como foi o caso da Decisão-Quadro 2005/222/JAI, relativa a ataques contra os sistemas de informação, da Decisão-Quadro 2004/413/JAI, relativa à exploração sexual de crianças, da Decisão 2001/413/JAI, relativa ao combate à fraude e contrafacção de meios de pagamento que não em numerário, da Directiva 2002/58/CE, relativa à privacidade das comunicações electrónicas e a Comunicação da Comissão Europeia, de 22 de Maio de 2007, "Rumo a uma política geral de luta contra o cibercrime"[139]. Importantes

[134] SILVA DIAS, op. cit., p. 50-53.
[135] "Algumas Reflexões (...), op.cit, p. 115-117. V. SILVA DIAS, Ramos Emergentes(...), op. cit., p. 51, e em «Delicta (...)», op. cit., p. 225 e ss.
[136] A Organização para a Cooperação e Desenvolvimento Económico adoptou o "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" (1980), o "Manual on the Prevention and Control of Computer-related Crime" (1994) e a Recommendation Concerning Guidelines for the Security of Information Systems (1992).
[137] A Assembleia Geral das Nações Unidas adoptou, a 15/11/2000, a Convenção das Nações Unidas contra o Crime Organizado Transnacional que no seu art. 27º nº 3 prevê a repressão da criminalidade cometida por meio das modernas tecnologias, e sobre a sua égide foram elaborados os manuais "United Nations Manual on the Prevention and Control of Computer-Related Crime" (1994), "Guidelines on the Use of Computerised Personal Data Flow"(Resolução 44/132, UN Doc. E/CN.4/Sub.2/1988/22).
[138] Constituído pelo P8 Expert Group on "Misuse of International Data Networks" e pelo P8 Subgroup on High Tech Crime.
[139] Ver nota 91.

foram também a Recomendação R(81) 12, a Recomendação R(85) S, a Recomendação R(89) 9 e a Recomendação R(95) 13 do **Conselho da Europa**[140].

O instrumento internacional de maior relevo na área do cibercrime é a **CONVENÇÃO SOBRE O CIBERCRIME** do Conselho da Europa de 23 de Novembro de 2001[141] destinada a «*proteger a sociedade do cibercrime, inter alia, através da adopção de legislação adequada e da melhoria da cooperação internacional*», de modo a «*tornar mais eficazes as investigações e os processos penais respeitantes às infracções penais relacionados com sistemas e dados informáticos, bem como permitir a recolha de prova, em formato electrónico*»[142].

Com este fim, a Convenção impõe aos Estados signatários que adequem o seu Direito Penal substantivo e adjectivo interno às especificidades destes crimes, tendo como objectivo a harmonização de legislações, incluindo instrumentos processuais e de produção de prova adequados e simplificar a cooperação internacional de modo a facilitar e agilizar a detecção, a investigação, a recolha de prova e a perseguição. Busca a harmonização do *direito penal material*[143] e de modo a potenciar a perseguição e investigação pelas autoridades policiais e judiciais a Convenção sugere a implementação de medidas específicas processuais adequadas a este tipo de criminalidade e promove a cooperação internacional[144]. Todavia, para esta Convenção funcionar em pleno e regular todo o ciberespaço tinha de ser ratificada por todos os países o que não acontece, nomeadamente

[140] Outras contribuições importantes foram dadas pelo P8 Subgroup on High-Tech Crime, pela Interpol, pela Association International de Droit Pénal, pela WIPO e WTO, vide ULRICH SIEBER, Legal Aspects (…), op.cit., p. 146-192.

[141] Legatária directa da Recomendação nº R (89) 9, a Convenção sobre a Cibercriminalidade foi adoptada pelo Comité dos Ministros do Conselho da Europa em 8 de Novembro de 2001, tendo sido aberta à assinatura, em Budapeste, em 23 de Novembro de 2001, foi assinada, até à data, por 42 Estados, entre os quais se encontravam 4 Estados não membros do Conselho da Europa (África do Sul, Canada, E.U.A. e Japão) e ratificada por 10. A Convenção foi complementada pelo Protocolo adicional relativo à incriminação de actos de natureza racista e xenófoba cometidos através de sistemas informáticos, em 28 de Janeiro de 2003. Esta matéria não foi incluída inicialmente por oposição de alguns países como os E.U.A. que receavam a incompatibilidade com a sua Primeira Emenda, que garante a liberdade de expressão.

[142] Preâmbulo da Convenção.

[143] A Convenção divide os crimes em infracções contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos, onde inclui o acesso ilegítimo (art. 2º), a intercepção ilegítima (art. 3º), a interferência em dados (art. 4º), a interferência em sistemas (art. 5º) e o uso abusivo de dispositivos (art. 6º); infracções relacionadas com computadores, que abarca nomeadamente a falsidade informática (art. 7º) e a burla informática (art. 8º); e infracções relacionadas com o conteúdo e relacionadas com a violação do direito de autor e direitos conexos' art. 9º (infracções relacionadas com pornografia infantil) e art. 10º respectivamente.

[144] Entre elas temos a conservação expedita dos dados informáticos armazenados e a divulgação parcial de dados de tráfego (arts. 16º e 17º), a injunção para divulgação de dados que estejam na posse de alguém (art. 18º), a busca e apreensão de dados informáticos armazenados (art. 19º), a recolha de dados em tempo real de dados informáticos (art. 20º) e a intercepção de dados relativos ao conteúdo (art. 21º). Debruça-se, ainda na formulação de princípios gerias relativos à, tão desejada rápida e eficaz, cooperação internacional (arts. 23º e ss.), na qual se insere a Rede 24/7 (art. 35º) e sobre a assistência mútua (29º-30º).

com a China que também não ratificou qualquer tratado internacional neste âmbito, restando quando esta está envolvida apenas em vias diplomáticas sempre frágeis[145].

6.2 Nacional

Em Portugal, a matéria da criminalidade informática está **regulada** dispersamente por vários diplomas, nomeadamente no Código Penal, na Lei nº 109/2009 de 15 de Setembro, na Lei da Protecção de Dados Pessoais (Lei nº 67/98, de 26 de Outubro[146]), na Lei da Protecção Jurídica de Programas de Computador (Decreto-Lei nº 252/94, de 20 de Outubro[147]), no Código de Direitos de Autor e dos Direitos Conexos (Decreto-Lei nº 63/85, de 14 de Março[148]) e no Regime Geral das Infracções Tributárias (Lei nº 15/2001, de 05 de Junho[149]).

Na adaptação da Convenção[150], a Lei nº 109/2009 de 15 de Setembro ou **LEI DO CIBERCRIME**, já no seguimento da Lei nº 109/91 de 17 de Agosto[151], no âmbito do direito penal **material** tipificou cinco crimes informáticos em sentido estrito: a *falsidade informática* (art. 3º), o *dano relativo a programas ou outros dados informáticos* (art. 4º), a *sabotagem informática* (art. 5º), o *acesso ilegítimo* (art. 6º), a *intercepção ilegítima* (art. 7º) e a *reprodução ilegítima de programa protegido* (art. 8º)[152].

A grande evolução da nova Lei é ao nível **processual** e da cooperação internacional. No âmbito processual é vital a adopção de eficazes disposições processuais específicas porque

[145] O relatório da GhostNet em Portugal da Trusted Tecnologies constata a infiltração de uma rede de espionagem electrónica em diversos organismos públicos do Estado português, cfr. JOÃO GONÇALVES DE ASSUNÇÃO, "(In)segurança e a nova ´lei do cibercrime', em http://www.abreuadvogados.com-/xms/files/05_Comunicacao/Artigos_na_Imprensa/Artigo_JGA_SOL_16.01.10.pdf.

[146] Alterada pela Declaração de Rectificação nº 2-A/95, de 31 de Janeiro e pelo Decreto-Lei nº 334/97, de 27 de Novembro. Tipifica o crime derivado do não cumprimento de obrigações relativas à protecção de dados (art. 43º), o crime de acesso indevido (art. 44º), o crime de viciação ou destruição de dados pessoais (art. 45º), o crime de desobediência qualificada (art. 46º) e o crime de violação do dever de sigilo (art. 47º).

[147] Alterado pela Rectificação nº 2-A/95, de 31 de Janeiro e pelo Decreto-Lei nº 334/97, de 27 de Novembro. Tipifica o crime de reprodução de computador não autorizada (art. 14º).

[148] Com a última alteração pela Lei nº 16/2008, de 01 de Abril. Consagra o crime de usurpação (art. 195), o crime de contrafacção (art. 196º),o crime de violação do direito moral (198º) e o crime de aproveitamento de obra contrafeita ou usurpada (199º do CDADC).

[149] Já com diversas alterações, consagra o crime de falsidade informática (art. 128º).

[150] Na adaptação da Convenção sobre o Cibercrime do Conselho da Europa e da transposição da Decisão Quadro nº 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação.

[151] Também chamada de Lei da Criminalidade Informática foi totalmente inspirada na Recomendação nº R (89) 9 do Comité de Ministros aos Estados-membros. Alterada pelo Decreto-Lei nº 323/2001, de 17 de Dezembro.

[152] Foram mantidas as tipificações previstas na Lei nº 109/91 de 17 de Agosto ou Lei da Criminalidade Informática e introduzidas novas variantes criminais, de forma a adaptar a legislação à constante evolução de condutas criminosas nesta área. Vide PEDRO VERDELHO, "A nova Lei do Cibercrime", op.cit., p. 34.

estamos perante crimes específicos que destinam ao fracasso a aplicação de procedimentos tradicionais. Estas disposições processuais, essenciais para agilizar a investigação e a punição do cibercrime, são também aplicadas a qualquer infracção penal cometidas por meio de um sistema informático e à recolha de prova em suporte electrónico de qualquer infracção penal.[153]

Tendo em vista a obtenção de prova, foi previsto a *preservação expedita de dados* até ao limite máximo de um ano (art. 12º) e a *revelação expedita de dados de tráfego* (art. 13º), que são medidas cautelares e provisórias, destinadas sobretudo aos ISPs, com vista a salvaguardar a produção futura de prova agilizando a investigação. Já a *injunção para apresentação ou concessão de acesso a dados* (art. 14º), que corresponde à *production order* inglesa, e a *pesquisa de dados informáticos* (art. 15º) são medidas coercivas impostas a quem tenha a disponibilidade dos dados. Estipula-se também a *apreensão de dados informáticos* (art. 16º), e a *apreensão de correio electrónico* quando forem encontrados dados ou documento de informáticos necessários à produção de prova (art. 17º). A apreensão dos dados informáticos pode ser feita pela apreensão do suporte, pela realização de uma cópia dos dados, pela apresentação por meios tecnológicos e pela eliminação não reversível ou bloqueio do acesso aos dados. De notar, que em alguns casos, é permitido aos órgãos de polícia criminal actuar sem autorização prévia da autoridade judiciária. A *intercepção de comunicações* pode destinar-se ao registo de dados relativos ao conteúdo das comunicações ou somente à recolha e registo de dados de tráfego (art. 18º) e as *acções encobertas* foram consideradas admissíveis no âmbito do cibercrime, se verificados os requisitos do art. 19º.

Quanto à necessária eficácia e agilização da cooperação internacional é relevante estabelecimento de um *ponto de contacto permanente*, assegurado pela Polícia Judiciária, no seguimento da *Rede 24/7* da Convenção, certificando assim a assistência, aconselhamento técnico, a preservação e a recolha de prova, a localização de suspeitos e informações jurídicas a outros pontos de contactos de outros países (art. 20º e ss).

[153] Artigo 11º, reprodução das alíneas b) e c) do nº 2 do art. 14º da Convenção.

Conclusão:

A Internet veio alterar drástica e definitivamente a vida de todos, As infra-estruturas básicas de uma sociedade e das suas empresas públicas e privadas ficaram dependentes dela e os utilizadores particulares integram-se numa cibercomunidade. A Internet potenciou e efectivou a globalização, dando origem a uma "aldeia global" que vive na Sociedade da Informação.

Contudo, atrás das fantásticas e inegáveis vantagens da Internet vieram também as práticas criminosas, que se multiplicam, diversificam e tornam-se cada vez mais perigosas, adaptando-se rapidamente às inovações tecnológicas e fugindo ao controlo legal.

Os cibercriminosos tanto usam o computador como alvo ou objecto da conduta criminosa, como um instrumento ou meio para praticar o crime. O cibercriminoso pode ser qualquer um e atingir qualquer um, sendo o seu principal móbil, o lucro monetário.

As dificuldades de prevenção, investigação, perseguição, comprovação e punição do cibercrime jazem nas suas características. O seu carácter transnacional, que permite o refúgio nas leis territoriais mais favoráveis e um ciberrasto mundial, aliado à permanência do facto que é automático, com a protecção do anonimato das redes, leva a uma extensa e alta lesividade dos danos, sendo a cifra negra elevada, o que aproxima o cibercrime do almejado crime perfeito.

As soluções apontadas para combater este tipo específico de criminalidade são a prevenção, através da sensibilização das vítimas e aumento da literacia informática de toda a sociedade; a formação especializada dos profissionais que se dedicam a esta área, acompanhada de recursos adequados; e a conjugação de uma uniformidade legal internacional, com a cooperação e coordenação internacionais de autoridades e entidades públicas e privadas, pois só com uma resposta global se pode ganhar a luta com um crime transnacional.

Discutível é o enquadramento do cibercrime na sociedade do risco. Para alguma doutrina impõe-se a sua regulação por um Direito Penal Global do Risco Informático, que responde numa lógica preventiva e antecipa a tutela, já para outra parte da doutrina este crime pode ser perfeitamente combatido com os instrumentos penais tradicionais.

A resposta internacional de maior relevo foi a Convenção sobre a Cibercrime, que impôs a modificação do direito interno dos Estados signatários, dando origem em Portugal à Lei do Cibercrime em Setembro de 2009.

Bibliografia:

ANDRÉS, Javier de Blasco – "Qué Es Internet?", Principios de Derecho de Internet, Prainter, Tirant lo Blanch, Valencia, 2002.

ARAÚJO, Dyellber Fernando de Oliveira – "Institutos Penais de Emergência - "Novas" Fórmulas para Velhos Dilemas - Uma Análise dos Novos Estudos de Política Criminal Voltada aos Indesejados pela Sociedade", Direito Penal Hoje Novos desafios e novas respostas, Orgz: Manuel da Costa Andrade e Rita Castanheira Neves, Coimbra Editora, 2009.

ASCENSÃO, José de Oliveira – "Criminalidade Informática", Estudos sobre Direito da Internet da Sociedade da Informação, Almedina, 2001.

ASSUNÇÃO, João Gonçalves de– "(In)segurança e a nova ´lei do cibercrime', *in* http://sol.sapo.pt/Common/print.aspx.

BECK, Ulrich – *World Risk Society*, Polity Press, Cambridge, 2000.
– A Sociedade Global do Risco, Uma discussão entre Ulrich Beck e Danilo Zolo, trad: Selvino J. Assmann, 2000, *in* http://www.cfh.ufsc.br/~wfil/ulrich.htm ou http://lgserver.uniba.it.

BECK, Ulrich / **GIDDENS**, Anthony / **LASH**, Scott – *Modernização Reflexiva: Política, Tradição e Estética no Mundo Moderno*, trad. Maria Amélia Augusto, Celta Editora, Oeiras, 2000.

BELLEFONDS, Xavier Linant de – *A Informática e o Direito, Computer Law*, Colecção Jurídica Internacional, tradução de Isabel Maria Brito St. Au Byn, G&A Editores, 2000.

CABO, Ana Isabel – "Nova lei facilita investigação", Criminalidade Informática, Boletim da Ordem dos Advogados, nº 65, Abril, 2010.

CASEY, Eoghan – *Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet*, Academic Press, 2000.

CASIMIRO, Sofia de Vasconcelos – *A responsabilidade civil pelo conteúdo da informação transmitida pela Internet*, Coimbra, Almedina, 2000.

COGAR, Stephen W. – "Obtaining admissible evidence from computers and internet service providers", The FBI Law Enforcement Bulletin, Jul 1, 2003, p. 11-15, em http://www2.fbi.gov/publications/leb/2003/july03leb.pdf.

COSTA, José Francisco de Faria – *Direito Penal e Globalização, Reflexões não locais e pouco globais*, Wolters Kluwer Portugal, Coimbra Editora, 2010.
– *O Perigo em Direito Penal (contributo para a sua fundamentação e compreensão dogmáticas)*, Coimbra Editora, 2000.
– "Algumas Reflexões sobre o Estatuto Dogmático do Chamado "Direito Penal Informático", *Direito Penal da Comunicação (Alguns escritos)*, Coimbra Editora, 1998.
– "Les Crimes Informatiques et d´Autres Crimes dans le domaine de la Technologie Informatique au Portugal", *Direito Penal da Comunicação (Alguns escritos)*, Coimbra Editora, 1998.

DIAS, Augusto Silva – *Ramos Emergentes do Direito Penal Relacionados com a Protecção do Futuro (Ambiente, Consumo e Genética Humana)*, Coimbra Editora, 2008.
– *«Delicta In Se» e «Delicta Mere Prohibita»: Uma Análise das Descontinuidades do Ilícito Penal Moderno à Luz da Reconstrução de uma Distinção Clássica*, Coimbra Editora, 2008.

DIAS, Jorge de Figueiredo – *O Papel do Direito Penal na Protecção das Gerações Futuras, in* http://www.defenseociale.org/revista2002/8.1.htm.
– "O Direito Penal entre a "Sociedade Industrial" e a "Sociedade do Risco", Estudos em homenagem ao Prof. Doutor Rogério Soares, Stvdia Ivridica 61, Ad Honorem-1, Boletim da Faculdade de Direito, Universidade de Coimbra, Coimbra Editora, 2001, p.583-613.

DIAS, José Eduardo de Figueiredo – "Direito à Informação, Protecção da Intimidade e Autoridades Administrativas Independentes", Estudos em homenagem ao Prof. Doutor Rogério Soares, Stvdia Ivridica 61, Ad Honorem-1, Boletim da Faculdade de Direito, Universidade de Coimbra, Coimbra Editora, 2001, p. 615-653.

DIAS, Pedro Simões – "O «Hacking» enquanto crime de acesso ilegítimo. Das suas especialidades à utilização das mesmas para a fundamentação de um novo direito", *in* http://www.uria.com/esp/actualidad_juridica/n14/art04.pdf

EUROPOL – *High Tech Crimes Within The EU: Old Crimes New Tools, New Crimes New Tools*, Threat Assessment 2007, High Tech Crime Centre, 2007, *http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssessment2007.pdf*

FERNÁNDES, José Ernesto Pinós – "Cuestiones Procesales Relativas a la Investigación y Persecución de Conductas Delictivas en Internet",

FERNANDES, Paulo Silva – *Globalização, "Sociedade de Risco" e o Futuro do Direito Penal, Panorâmica de alguns problemas comuns*, Almedina, 2001.

GAMEIRO, Carlos – "O Risco da Informação em Ambiente Electrónico", Estudos de Direito e Segurança, Faculdade de Direito da Universidade Nova de Lisboa, Almedina, 2007.

GUERRA, Ana Rita – "Processos de crime informático quase duplicam em 2010", 14.10.2010, http://www.ionline.pt/conteudo/83163-processos-crime-informatico-quase-duplicam-em-2010.

GONZÁLEZ, Juan José López – La respuesta procesal a la delincuencia informática: especial atención al convenio sobre el cibercrimen, *Direito Informático Ético*", Septiembre 2003, em http://www.juridicas.com/areas_virtual/Articulos/20-Derecho%20Inform%E1tico/200309-5755119810322511.html

JARVIS, Darryl S. L. – *Theorizing Risk: Ulrich Beck, Globalization and the Rise of the Risk Society*, Lee Kuan Yew School of Public Policy, NUS – National University of Singapore, 2010, em http://www.risk-and-regulation.com/wp-content/uploads/2010/05/RR3-Beck.pdf.

LIMA, Licínio – "Lei do Crime Ineficaz", Diário de Notícias, 21.11.2009, em http://www.inverbis.net/actualidade/leicibercrime-ineficaz.html

LÓPEZ, Antonio Melgarejo – "Investigación Criminal y Proceso Penal: Las Directrices de la Propuesta del Consejo de Europa sobre *Cyber-Crime* y de la Directiva del Comercio Electrónico",

MACEDO, João Carlos Cruz Barbosa de – "Algumas Considerações Acerca dos Crimes Informáticos em Portugal", Direito Penal Hoje Novos desafios e novas respostas, Orgz: Manuel da Costa Andrade e Rita Castanheira Neves, Coimbra Editora, 2009.

MARCHENA, Manuel Gómez – "Algunos Aspectos Procesales de Internet", Problemática Jurídica en Torno al Fenómeno de Internet, Consejo General del Poder Judicial, Madrid, 2000, p. 45-86.

MARQUES, Garcia / **MARTINS**, Lourenço – *Direito da Informática*, Lições de Direito da Comunicação, Almedina, 2000.

MARTINS, A. G. Lourenço – "Criminalidade Informática", Direito da Sociedade da Informação, APDI, volume IV, Coimbra Editora, págs. 9-41.

MATA, Ricardo M. y Martín – "Criminalidad Informática: una introducción al Cibercrime", Temas de Direito da Informática e da Internet, Ordem dos Advogados (Conselho Distrital do Porto), Coimbra Editora, 2004.

MENDES, Paulo de Sousa – "A Responsabilidade de Pessoas Colectivas no âmbito da Criminalidade Informática", Direito da Sociedade da Informação, APDI, volume IV, Coimbra Editora, págs. 385-404.

MEXÍA, Pablo Gracia – "El Derecho de Internet", Principios de Derecho de Internet, Prainter, Tirant lo Blanch, Valencia, 2002.

MORGADO, Maria José – "Criminalidade Global e insegurança Local, Um caso, Algumas questões", Colóquio Internacional: Direito e Justiça no Século XXI, Coimbra, 2003, na URL: http://www.ces.uc.pt/direitoXXI/comunic/MariaJoseMorgado.pdf.

MORÓN, Esther Lerma – *Internet y Derecho Penal: Hacking y otros conductas ilícitas en la red*, Pamplona: Aranzadi, 1999.

NERY, Isabel – "O guerrilheiro da verdade", Mundo Perfil, Revista Visão, de 29 de Julho de 2010.

NETO, João Araújo Monteiro – "Crimes informáticos uma abordagem dinâmica ao direito penal informático, *Computer crimes: a dynamic approach on Computer Science Penal Law*", Pensar, Fortaleza, volume 8, nº8, Fevereiro, 2003: [39-54], em http://www.unifor.br/notitia/file/1690.pdf

PEREIRA, Evandro Della Vecchia – "Investigação Digital: conceitos, ferramentas e estudo de caso", *in* http://www.infobrasil.inf.br/userfiles/26-05-S5-2-68766-Investigacao%20Digital.pdf

PEREIRA, Joel Timóteo Ramos – *Compêndio Jurídico Sociedade da Informação*, Quid Juris, Lisboa, 2004.

PHILLIPS, Beth – *News Release*, Office of The United States Attorney Western District of Missouri, July, 2010, *in* www.usdoj.gov/usao/mow/index.htlm

PINHEIRO, Luís Lima – "Competência Internacional em matéria de Litígios Relativos à *Internet*", Direito da Sociedade da Informação, APDI, volume IV, Coimbra Editora, págs. 171-189.

PIZARRO, Sebastião Nóbrega – *Comércio Electrónico, Contratos Electrónicos e Informáticos*, Almedina, 2005.

RESTA, Salvatore – *I Computer Crimes Tra Informatica E Telematica*, CEDAM – Casa Editrice Dott. Antonio Milani, 2000.

ROCHA, Manuel Lopes – "A propósito de cibercrime e direito de autor", Globalização, Boletim da Ordem dos Advogados, nº 65, Abril 2010.

RODRIGUES, Benjamim Silva – *Direito Penal Especial, Direito Penal Informático-Digital*, Coimbra, 2009.

ROMEO, Carlos María Casabona – "De los Delitos Informáticos al Cibercrimen. Una aproximación Conceptual y Político-Criminal", *El Cibercrimen: Nuevos Retos Jurídico Penales, Nuevas Respuestas Político-Criminales*, Granada, Comares, 2006.

ROVIRA, Enrique Del Canto – *Delincuencia Informática y Fraudes Informáticos*, Estúdios de Derecho Penal – 33 Editorial Comares, Granada, 2002.

ROXIN, Claus – *Pasado, presente y futuro del Derecho Procesal Penal*, Colección Autores de Derecho Penal, Rubinzal, Culzoni Editores, 2007.

SALOM, Juan Clotet – "Delito Informático y su Investigación", Delitos Contra y A Través de las Nuevas Tecnologías Cómo Reducir su Impunidad?, Cuadernos de Derecho Judicial, III, Consejo General Del Poder Judicial, Centro de Documentación Judicial, 2006.

SÁNCHES, Andrés Magro – "El Ciberdelito y sus Implicationes Procesales", Principios de Derecho de Internet, Prainter, Tirant lo Blanch, Valencia, 2002.

SANS, Nieves Mulas – "La Validez del Sistema Penal Actual Frente a los Retos de la Nueva Sociedad", El Sistema Penal Frente a Los Retos de La Nueva Sociedad", Editorial Colex, 2003.

SANTOS, Lino – "Cibersegurança - A resposta à emergência", Planeamento Civil de Emergência, Revista nº 19, Ano 2008, *in* www.cnpce.gov.pt

SANTOS, Paulo / **BESSA**, Ricardo / **PIMENTEL**, Carlos – "*CYBERWAR* o fenómeno, as tecnologias e os actores", FCA, Editora de Informática, Lda, 2008

SIEBER, Ulrich – *Legal Aspects of Computer-Related Crime in the Information Society – COMCRIME,Study*,1998,.http://www.archividelnovecento.it/archivinovecento/CAPPATO/Cappato/Faldone6412Dirittiumanipaesiextracom/DonneAfghanistan/Desktop/sieber.pdf

– "Criminalidad Informática: Peligro y Prevención", Delincuencia Informática, IURA-7, PPU, Barcenona, 1998 (trad. Elena Farré Trepat);

– "Documentación para una aproximación al Delito Informático", Delincuencia Informática, IURA-7, PPU, Barcenona, 1992 (trad. Ujala Joshi Jupert).

SILVA, Pablo Rodrigo Alflen da – *Características de um Direito Penal do Risco*, 2008, em http://jus2.uol.com.br/doutrina/texto.asp?id=11390

VENÂNCIO, Pedro Dias – *Breve introdução da questão da Investigação e Meios de Prova na Criminalidade Informática*, Verbojuridico, Dezembro, 2006, in http://www.verbojuridico.com.

VERDELHO, Pedro – "A nova Lei do Cibercrime", Lei nº 109/2009, Boletim da Ordem dos Advogados, nº 65, Abril 2010.
– "A Convenção sobre Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa", Direito da Sociedade da Informação, APDI, volume VI, Coimbra Editora, 2006, págs. 257-276.
– "Cibercrime e segurança informática", Polícia e Justiça, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III série, nº 6, Julho-Dezembro, Coimbra Editora, 2005.
– "Cibercrime", Direito da Sociedade da Informação, APDI, volume IV, Coimbra Editora, 2003, págs. 347-383.

VERDELHO, Pedro / **BRAVO**, Rogério / **ROCHA**, Manuel Lopes (coord. e notas)
– *Leis do Cibercrime*, volume 1, CentroAtlantico.pt, Portugal, 2003.

WOODWAR, Bob – "A Ciberguerra do Futuro", Focus Magazin (trad. Cláudio Castro), Focus 574/2010, p. 106.

YAR, Majid – *Cibercrime and Society*, Sage Publications, 2006.