



DEPARTAMENTO DE DIREITO

MESTRADO EM DIREITO

O CIBERCRIME: DESAFIOS E RESPOSTAS DO DIREITO

Dissertação de Mestrado para a obtenção do grau de Mestre em Direito,
especialidade em Ciências Jurídicas

Autor: Ana Felícia Canilho Santos

Orientadora: Professora Doutora Constança Urbano de Sousa

Setembro de 2015

Lisboa

Referência ao texto:

No presente trabalho adotou-se a grafia em concordância com o novo acordo ortográfico.

“Estou a exigir muito de si? Quem lhe há-de exigir muito senão os seus amigos? Eles receberam o encargo de o não deixar amolecer e, pela minha parte, tenha você a certeza de que hei-de cumprir. Você há-de dar tudo o que puder, e mesmo, e sobretudo, o que não puder; porque só há homem quando se faz o impossível; o possível todos os bichos fazem. Quando você saltar e saltar bem, eu direi sempre: agora mais alto! Que me importa que você caia. Os fracos vieram só para cair, mas os fortes vieram para esse tremendo exercício: cair e levantar-se, sorrindo.”

Agostinho da Silva, Sete Cartas a um Jovem Filósofo (1945)

- A todos os que me incentivaram a chegar até aqui.

Agradecimentos

Um agradecimento especial à Professora Doutora Constança Urbano de Sousa, por ter aceitado ser minha orientadora e por toda a disponibilidade que demonstrou, instigando e estimulando sempre a investigação, exigindo sempre o meu melhor. O qual espero ter cumprido.

À Universidade Autónoma de Lisboa, instituição que frequentei durante estes cinco anos de Licenciatura e Mestrado, que tão calorosamente me recebeu e me moldou.

A todos os funcionários da UAL e em especial ao Sr. José Pereira (Secretaria da UAL), meu colega de turma e amigo que sempre acreditou em mim. Agradeço toda a simpatia com que sempre me recebeu.

Ao Dr. Reginaldo Rodrigues de Almeida, o meu agradecimento por toda a disponibilidade e simpatia com que me recebeu e respondeu às minhas perguntas.

Ao Dr. Rui Batista, Procurador-Adjunto, Colaborador do Gabinete do Cibercrime o meu sincero agradecimento por toda a disponibilidade e simpatia demonstrada e, pelas conversas produtivas sobre Cibercrime.

Ao Dr. Rogério Bravo, Inspetor-Chefe da Polícia Judiciária de Lisboa o meu agradecimento pela disponibilidade em responder sempre às minhas perguntas.

Ao Dr. Pedro Verdelho, Gabinete de Cibercrime e Eng. Lino Santos, FCCN/ CERT.PT, por me terem cedido as imagens em anexo.

Por último, mas não menos importante, à minha família, pela compreensão e apoio que sempre me deram para prosseguir a vida académica. Em especial à minha Mãe por ler todo o meu texto, ajudando-me sempre com correções e sugestões.

A todos vós, os meus sinceros agradecimentos.

Resumo

O Cibercrime não pode ser considerado um “novo” tipo de crime que é capaz de transpor várias jurisdições e leis, já que existem outros exemplos como o tráfico de pessoas, drogas ou armas, que frequentemente transpõem várias fronteiras e vários Estados. No entanto, o perigo dos ataques de *Cibercrime* é que podem abranger várias jurisdições, em segundos.

Face aos desafios que nos são apresentados diariamente, o Direito vê-se obrigado a legislar matérias tão distintas como “espionagem informática”, “acesso ilícito” ou “criação de *software* malicioso”. Do mesmo modo, assistimos à transição dos crimes do mundo real para o mundo virtual e o Direito é também forçado a legislar essa matéria.

A este propósito é necessário que o Direito forneça uma adequada resposta para os novos desenvolvimentos tecnológicos e para os problemas que destes advêm.

Palavras-chave: Cibercrime; Convenção Cibercrime; criminalidade informática; cooperação internacional; *Hackers*.

Abstract

The Cybercrime cannot be considered a "new" type of crime that is able to cross multiple jurisdictions and laws, since there are other examples such as human, drugs or weapons' trafficking, which often span many borders and states. However, the danger of cyber attacks is that they can span multiple jurisdictions in seconds.

Given the challenges that are presented to us daily, the law is obliged to legislate matters as diverse as "computer espionage", "unauthorized access" or "creation of malicious software". Similarly, the real world crimes are migrated to the virtual world, and the Law is forced to legislate this matter as well.

In this connection it is necessary that the law provides an adequate response to new technological developments and the problems that arise from these.

Keywords: Cybercrime; Cybercrime Convention ; Computer crime ; international cooperation; *Hackers*.

Lista de Abreviaturas e Acrónimos

Ac.	Acórdão
AED	Agência Europeia de Defesa
ANACOM	Autoridade Nacional de Comunicações
App.	Application
apud.	Expressão que significa “com”, “junto a”, “em”
ARPANET	Advanced Research Projects Agency Network
Art.	Artigo
ASEAN	Associação de Nações do Sudeste Asiático
B2B	Business-to-Business
B2C	Business-to-Consumer
BIT	(contração de BInary digiT)
BRICS	Brasil, Rússia, Índia, China e África do Sul
CAM	Computer Aided Manufacturing
CDADC	Código de Direitos de Autor e Direitos Conexos
CD-R	Compact Disk Recordable
CEDH	Convenção Europeia dos Direitos do Homem
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team European Union
Cfr.	Confrontar
CJ	Colectânea de Jurisprudência
CNCSeg	Centro Nacional de Cibersegurança
CNI	Centro Nacional de Inteligência

CNPD	Comissão Nacional de Proteção de Dados Pessoais
COM	Component Object Model
CP	Código Penal Português
CPP	Código de Processo Penal
CRP	Constituição da República Portuguesa
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service
DGAJ	Direção Geral da Administração da Justiça
DHCP	Dynamic Host Control Processing
DL	Decreto-Lei
DMZ	Demilitarized zone (computing) ou perimeter network
DNS	Domain Naims (Nome de domínio)
DoS	Denial-of-Service
DQ	Decisão-Quadro
DR	Diário da República
DUDH	Declaração Universal dos Direitos do Homem
EBF	The European Banking Federation
EC3	European Cybercrime Center
ed.	edição
EFMS	Fórum Europeu dos Estados Membros
EM	Estados Membros
ENISA	Agência Europeia para a Segurança das Redes e da Informação
ENSI	Estratégia Nacional de Segurança da Informação

EUA	Estados Unidos da América
ex.	exemplo
FCCN	Fundação para a Computação Científica Nacional
FEM	Fórum Económico Mundial
FTP	File Transfer Protocol
G8	Grupo dos 8 (Chefes de Estado dos Estados Unidos da América, Reino Unido, França, Alemanha, Japão, Canadá, Rússia e da União Europeia)
GBDe	Global Business Dialogue on Electronic Commerce
GNS	Gabinete Nacional de Segurança
GPS	Global Positioning System
GPTIC	Grupo de Projeto para as Tecnologias de Informação e Comunicação da Administração Pública
HTML	Hypertext Markup Language
IAB	Internet Architecture Board
ibidem	“no mesmo trabalho que o anterior, mesma página”
IBM	Industrial Business Machines
IBSG	Internet Business Solutions Group
ICI	Infraestruturas Críticas da Informação
ICT	Information and communications technology
idem	“mesmo autor”
IDPCC	Instituto de Direito Penal e Ciências Criminais
IDS	Intrusion Detection System
IGF	Internet Governance Forum
I.J.C.	Instituto Jurídico da Comunicação

IOSCO	Organização Internacional dos Reguladores dos Mercados de Capitais
IP	Internet Protocol
IRIS	Internet Routing in Space
ISOC	Internet Society
ISP	Internet Service Provider
IT	Information Technology
ITIJ	Instituto das Tecnologias de Informação na Justiça
ITU	International Telecommunication Union
J-CAT	Joint Cybercrime Action Taskforce
JIC	Juiz de Instrução Criminal
JOCE	Jornal Oficial das Comunidades Europeias
JOUE	Jornal Oficial da União Europeia
LC	Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro)
LCE	Lei do Comércio Electrónico (Decreto-Lei n.º 7/2004, de 7 de Janeiro)
LCI	Lei da Criminalidade Informática (Lei n.º 109/1991, de 17 de Agosto – revogada)
LPDP	Lei de Protecção de Dados Pessoais (Lei n.º 67/98, de 26 de Outubro)
LPDPI	Lei de Protecção de Dados Pessoais face à Informática
LPDPT	Lei de Protecção de Dados Pessoais nas Telecomunicações (Lei n.º 41/2004, de 18 de Agosto)
MIT	Massachusetts Institute of Technology
MMS	Multimedia Messaging Service
MoU	Memorandum of Understanding
MP	Ministério Público

MPAA	Motion Picture Association of America
MSN	The Microsoft Network
n.º	número
NAT	Network Address Translation
NATO	North Atlantic Treaty Organization (Organização do Tratado do Atlântico Norte)
NCA	National Crime Agency
NCSD	National Cyber Security Division
Net	Internet
NSI	Network Solutions International
NU	Nações Unidas
OCDE	Organização para a Cooperação e Desenvolvimento Económico
OCX	Organização de Cooperação de Xangai
OEA	Organização dos Estados Americanos
op. cit.	<i>Opere citato</i> (mesma obra, página diferente)
OPC	Órgão de Polícia Criminal
ONU	Organização das Nações Unidas
OSCE	Organization for Security and Co-operation in Europe
OVL	Open Verification Library
p.	página
PCSD	Política Comum de Segurança e Defesa
PGDL	Procuradoria-Geral Distrital de Lisboa
PIB	Produto Interno Bruto

PJ	Polícia Judiciária
pp.	páginas
QFP	Quad Flat Package
RATs	Remote Access Trojans
RCM	Resolução do Conselho de Ministros
ref.	referência
RIAA	Recording Industry Association of America
R.L.J	Revista de Legislação e de Jurisprudência
R.O.A.	Revista da Ordem dos Advogados
SCADA	Supervisory Control and Data Acquisition Systems
SCEE	Sistema de Certificação Eletrónica do Estado
SCO	Shanghai Cooperation Organization
SEA	Syrian Electronic Army
SI	Sistemas de Informação
SIGINT	Sistema de Espionagem Electrónica
SMS	Short Message Service (mensagens escritas)
SPCI	International Conference on Security, Privacy and Confidentiality Issues in Cyberlaw
SRI	Segurança das Redes e da Informação
ss.	seguintes
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFUE	Tratado sobre o Funcionamento da União Europeia
TIC	Tecnologias da Informação e das Comunicações

TJCE	Tribunal de Justiça das Comunidades Europeias
TL	Tratado de Lisboa
TUE	Tratado sobre a União Europeia
UA	União Africana
UCLA	Universidade da Califórnia
UDP	User Datagram Protocol
UE	União Europeia
UKUSA	“United Kingdom – United States of America”
UMIC	Agência para a Sociedade do Conhecimento
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
URL	Uniform Resource Locator
USB	Universal Serial Bus
US-CERT	United States - Computer Emergency Readiness Team
USD	United States Dollar
vol.	volume
WAAR	Web Application Attack Report
WWW	World Wide Web

Índice	Páginas
Referência ao texto.....	3
Dedicatória.....	4
Agradecimentos.....	5
Resumo.....	6
Abstract.....	7
Lista de Abreviaturas e Acrónimos.....	8
Índice.....	15
Introdução.....	18
Capítulo I - A Cibercriminalidade na nova Era Global.....	22
1. Enquadramento.....	22
2. A Sociedade da Informação.....	27
3. O Ciberespaço.....	34
3.1.Evolução.....	34
3.2. A Internet na Era Global.....	43
3.3. A Cibersegurança.....	49
3.4. Os desafios e ameaças do Ciberespaço.....	64
Capítulo II – Cibercrime.....	75
1. Noção.....	75
2. Aspetos fundamentais.....	78
3. A Problemática do Cibercrime e os novos fenómenos criminais.....	80
3.1.Hactivismo.....	86
3.2. Ciberespionagem.....	91
3.3. Ciberguerra/Ciberterrorismo.....	93
4. Tipologia.....	101
4.1. Criminalidade contra a privacidade.....	102
4.2. Crimes informáticos.....	114
4.2.1. Burla Informática.....	117

4.2.2. Falsidade Informática.....	120
4.2.3. Blackboxing e Blueboxing.....	122
4.2.4. Carding.....	123
4.2.5. Transmissão de Vírus.....	124
4.2.6. Acesso ilegítimo	127
4.2.7. Espionagem Informática e o sistema ECHELON.....	128
4.2.8. Interceção ilegítima	131
4.2.9. Reprodução ilegítima de programa protegido.....	134
4.3. Criminalidade organizada.....	136
4.4. Ataques contra sistemas informáticos.....	140
4.5. Pedofilia e Pornografia Infantil.....	143
5. A Cibercriminalidade no plano internacional.....	154
5.1. Tendências	154
5.2. Dificuldades da experiência prática e tentativas de resolução.....	157
Capítulo III - A resposta do Direito à Cibercriminalidade.....	160
1. O Direito Internacional Público.....	160
1.1. Principais instrumentos de Direito Internacional.....	164
1.2. Convenção do Conselho da Europa sobre o Cibercrime.....	169
1.2.1. Disposições de Direito Penal Material.....	171
1.2.2. Disposições de Direito Processual Penal.....	176
1.2.3. Cooperação Internacional.....	179
2. O Direito da União Europeia.....	183
2.1 A estratégia da UE de combate à Cibercriminalidade.....	183
2.2 A Diretiva 2013/40/UE sobre o Cibercrime.....	190
2.2.1. Antecedentes.....	190
2.2.2. Análise das disposições da Diretiva sobre Cibercrime.....	192
2.2.3. Avaliação crítica.....	197
2.3 Resposta Institucional.....	199
2.3.1. Europol	201
2.3.2. Centro Europeu de Cibercriminalidade (EC3).....	204
3. A Luta contra a Cibercriminalidade na Ordem Jurídica Portuguesa.....	208
3.1. Enquadramento.....	208

3.2. Dificuldades e limitações práticas do quadro jurídico interno no combate à Cibercriminalidade.....	212
3.3. Soluções/Mecanismos de Defesa.....	216
Conclusão	218
Bibliografia.....	224
Anexos.....	248
Anexo 1- Glossário.....	248
Anexo 2 - Figuras.....	260
Figura 1 – Esquema exemplificativo “World Wide Web”.....	260
Figura 2 – Esquema exemplificativo de comunicação entre “cliente-servidor”	261
Figura 3 – Exemplo de um ataque de “Phishing” através do correio eletrónico.....	262
Figura 4 – Exemplo de um falso <i>email</i> com o intuito de confirmar os dados bancários do utilizador (<i>Phishing</i>).....	263
Figura 5 – Exemplo de “Pharming” enquanto <i>modus operandi</i>	264
Figura 6 – Exemplo de Transmissão de Vírus através do correio eletrónico.....	265
Figura 7 – Exemplo de uma notificação eletrónica falsa do “Superior Tribunal de Justiça”	266
Figura 8 – Exemplo de uma notificação eletrónica falsa do Ministério Público	267
Figura 9 – Exemplo de transmissão de mensagem “spam” através do correio eletrónico.....	268

Introdução

A evolução tecnológica aliada, ao aparecimento da *Internet*, foi sendo evidente um pouco por todo o mundo, abrangendo os vários sectores de cada sociedade e trazendo desafios para o Direito que são cada vez mais patentes.

As novas tecnologias permitem expandir, de modo extraordinário, as nossas capacidades de processamento, armazenamento, organização, representação e comunicação da informação. No entanto, estamos longe de prever a dimensão que este fenómeno tecnológico pode alcançar.

Um pouco por todo o Mundo, começa já a ser debatido o tema que aqui nos propomos tratar, o *Cibercrime*. Um tema de extrema importância, quer pela frequência com que ocorre quer pela gravidade e os danos que provoca.

Todos os dias, mais de um milhão de pessoas são vítimas de *Cibercrime*. Dada a frequência com que este tipo de crime ocorre e os danos que causa, é já considerado um dos mais graves e lucrativos fenómenos de criminalidade até agora existente. Estima-se que os custos associados ao *Cibercrime* podem atingir um valor global de 388 mil milhões de dólares.

Como iremos ver, à medida que o acesso à *Internet* se expandiu pelo mundo, surgiram inúmeros crimes de natureza virtual, cometidos, quer através do computador quer contra o computador. Desta nova forma de criminalidade nasceu o conceito de *Cibercriminalidade*.

Atualmente existem ameaças de diversa ordem que colocam o Mundo em risco, pondo em causa toda a segurança internacional. Vivemos num clima de crescente preocupação com o aumento de grupos de criminalidade organizada, ataques em larga escala que ultrapassam as fronteiras nacionais e agentes que atuam anonimamente.

Este é um tipo de crime em que os autores, as vítimas e os instrumentos ou produtos do mesmo se localizam e atravessam diversas jurisdições, fazendo com que a abordagem tradicional das entidades responsáveis pela aplicação da lei a nível nacional não seja suficiente.

“Quando os criminosos viajam facilmente por todo o mundo, as intervenções das autoridades não podem ser meramente provinciais. Quando os tipos de crimes

transnacionais e o número de associações criminosas parecem estar a aumentar, nenhum país fica imune, pelo que os Estados tendem a auxiliar-se mutuamente na luta contra esses delitos sofisticados e perigosos. Quando rápidos progressos tecnológicos e uma impressionante mobilidade de pessoas, bens e capitais são aproveitados por criminosos hábeis, que agem sozinhos ou, mais perigoso ainda, em grupos, a aplicação da lei não pode ficar para trás. Quando os criminosos obtêm lucros fabulosos com os seus negócios ilícitos e os conseguem transferir e esconder das autoridades, a comunidade internacional torna-se vítima de diversas formas.”¹

A este propósito é necessário que o Direito forneça uma adequada resposta para os novos desenvolvimentos tecnológicos e para os problemas que destes advêm.

Desde o aparecimento das novas tecnologias em todos os setores e no nosso dia-a-dia, que o Direito se viu obrigado a evoluir e a abranger matérias tão diferentes como a “criação de *software* malicioso” ou a “espionagem informática”. A verdade é que os problemas que nos são apresentados atualmente, são dos mais variados, desde os perigos do conteúdo de alguns sítios eletrónicos, até à própria linguagem tecnológica que é utilizada na *Internet*, que pode induzir em erro muitos dos internautas. De igual modo surgem novos agentes, os chamados “cibercriminosos” e o Direito é também chamado a legislar e a sancionar o comportamento destes.

Todas estas dificuldades ganham uma nova dimensão quando vemos a facilidade com que estes ataques podem ser perpetrados em larga escala, atingindo vários utilizadores, entidades, Estados. E é neste ponto que a atuação europeia e internacional é tão importante.

Ao longo dos últimos anos, a União Europeia em conjunto com outras entidades e organizações internacionais têm adotado importantes estratégias para prevenir estes ataques e atenuar os impactos que estes têm na sociedade, as quais nem sempre foram bem-sucedidas como iremos analisar.

¹ Guia Legislativo para a Aplicação da Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional, um projeto conjunto do Centro Internacional para a reforma do Direito Penal e Política em matéria de justiça criminal e do Centro para a Prevenção Internacional do Crime (UNODC), Vancouver, Março de 2003, p.8.

Com este estudo pretendemos abordar quatro tópicos fundamentais, a saber: o *Cibercrime* e a sua problemática; as respostas do Direito ao *Cibercrime* e a resposta ao nível das organizações internacionais e da assistência técnica.

A questão fundamental que aqui se coloca é como pode o Direito proteger os cidadãos neste novo ambiente digital e global e tentar perceber se existe dissonância entre os Estados ou em que termos pode e deve ser promovida a cooperação entre eles de forma a permitir um combate mais eficaz a este tipo de criminalidade. Este é o grande debate que muitos autores têm tentado resolver e ao qual esperamos dar o nosso contributo com este trabalho.

A fim de dar resposta a todas estas pertinentes e interessantes questões, considerou-se pertinente estruturar a presente dissertação em três grandes capítulos.

No Capítulo I - Será feita uma breve apresentação histórica sobre o tema em apreço, abordando vários pontos importantes que servem de base para os capítulos seguintes. Nomeadamente, iremos abordar a temática da “Sociedade da Informação”: conceito, características, evolução; aspetos positivos e negativos. Em seguida, iremos analisar a temática do “Ciberespaço”: evolução, “a Internet na Era Global”, “a Cibersegurança” e, por fim, “os desafios e ameaças do Ciberespaço”, apontando neste último ponto alguns desafios futuros.

O Capítulo II - Será um capítulo importante, já que é inteiramente dedicado à temática do *Cibercrime*. Nos vários pontos deste capítulo serão abordados os aspetos fundamentais, a noção e toda a problemática que lhe está subjacente, bem como uma análise dos novos fenómenos criminais: *Hactivismo*, *Ciberespionagem* e *Ciberguerra/Ciberterrorismo*. De igual modo, daremos especial relevância à tipologia do *Cibercrime*, abordando cinco tópicos que nos parecem ser mais importantes: a “Criminalidade contra a privacidade”, os “crimes informáticos”, a “criminalidade organizada”, “ataques contra sistemas informáticos” e “pedofilia e pornografia infantil”.

Como forma de conclusão deste capítulo, tentaremos salientar algumas das possíveis tendências quanto ao *Cibercrime* e elencar algumas tentativas de resolução.

O Capítulo III - Será um capítulo chave, onde iremos descortinar “a resposta do Direito à Cibercriminalidade”. Este é um ponto importante do nosso trabalho já que iremos abordar:

- O Direito Internacional Público, nomeadamente, os principais instrumentos de Direito Internacional e uma análise às medidas contidas na Convenção do Conselho da Europa sobre o *Cibercrime*.
- O Direito da União Europeia, desde as estratégias adotadas, passando por uma breve resenha histórica da Diretiva 2013/40/UE sobre *Cibercrime*, até à análise das disposições e uma avaliação crítica das mesmas. Ainda neste ponto, iremos examinar a “Resposta institucional”, mais concretamente, no âmbito do *Cibercrime*: a “Europol” e o “Centro Europeu de Cibercriminalidade/EC3”.
- O Direito Nacional. Neste último ponto iremos investigar a luta contra a *Cibercriminalidade* na ordem jurídica portuguesa. A este propósito será feito um breve enquadramento, seguido do estudo das dificuldades e limitações práticas, sentidas no combate à *Cibercriminalidade*. Por fim, apontamos algumas soluções e mecanismos de defesa que poderão atenuar os efeitos deste fenómeno.

Como metodologia, a par de uma consulta bibliográfica e comparação entre as várias obras que abordam a temática, não deixaremos de afirmar a nossa opinião em algumas áreas.

Com este nosso estudo, não se pretendem esgotar as fontes de informação que existem, já que não é possível abarcar todo o material disponível para a investigação, uma vez que o *Cibercrime* é um tema muito abrangente, que se desenvolve e muda muito rapidamente, pelo que esta dissertação pretende apenas ser mais um contributo.

Capítulo I - A Cibercriminalidade na nova Era Global

1.- Enquadramento

Quando surgiram os primeiros computadores (os chamados computadores de primeira geração – o *ENIAC*, o *EDVAC*, o *MARK 1*, o *UNIVAC*, entre outros) desenvolvidos entre 1943 e 1958, eram enormes máquinas que funcionavam através de milhares de válvulas tríodos, semelhantes às utilizadas nos velhos aparelhos recetores de rádio. Estes computadores conseguiam efetuar de forma rápida cálculos relativamente complexos, graças à programação dos seus circuitos elétricos. A sua programação era feita no momento da instalação dos computadores nos locais dos utilizadores.²

Os computadores de segunda geração (desenvolvidos entre 1959-1962) utilizavam o transístor, inventado em 1947, que substituiu as válvulas usadas nos computadores da primeira geração.

Foi graças ao uso de transístores que surgiram novas perspectivas, face à difusão dos computadores, o que permitiu reduzir substancialmente a sua dimensão (passou então a ser possível passar os computadores pelas portas, tendo estes começado a ser montados nas fábricas e, depois, transportados para casa dos utilizadores). No entanto, eram ainda máquinas frágeis, que necessitavam de algum espaço e ambientes cuidadosamente controlados.³

Os rápidos progressos da eletrónica conduziram a uma diminuição do tamanho dos computadores, e o transístor foi rapidamente substituído pelo circuito integrado, inventado em 1958, que conseguia ter várias centenas de transístores miniaturizados sobre uma placa.

Até finais da década de 60, os fabricantes de *hardware* informático produziam o seu próprio *software*, utilizado apenas nos computadores que construíam.⁴ Os computadores eram comercializados juntamente com os programas adaptados às necessidades específicas dos utilizadores (prática denominada *bundling*), pelo que a transferência de programas para terceiros não trazia qualquer preocupação, nem interesse, já que cada programa só funcionava no computador em que tinha sido instalado. Assim, era muito

² Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, p.42.

³ *Idem*, *Op. Cit.*, p. 43.

⁴ Correa, Carlos M. (*et.al.*), *Derecho informático*, Depalma, Buenos Aires, 1987, p.53.

difícil a possibilidade de duplicação ilícita ou a “pirataria” do *software* e a proteção jurídica destes casos ainda não era uma preocupação.

Tal preocupação surgiu a partir de 1970, quando o *software* passou a ser desenvolvido e comercializado como produto autónomo⁵, isto é, passou a ser desenvolvido e comercializado separadamente dos computadores (prática denominada *unbundling*). Foi a partir daqui que surgiu a necessidade de criar uma tutela jurídica, uma vez que os programas de computadores podiam ser copiados ilegalmente e, depois, utilizados em vários aparelhos informáticos. Foi também nesta altura que surgiram conceitos e tipos de crimes que ainda hoje existem, como é o caso da reprodução ilegítima de *software*, com uma mistura de reprodução casual e de pirataria em larga escala⁶.

Graças a esta nova fórmula de criação e comercialização do *software*, foi possível a expansão da informática para novos domínios como as escolas, centros de saúde, serviços públicos e privados, pequenas e médias empresas, e mesmo particulares. Os computadores tornaram-se assim mais modernos e mais presentes na sociedade.

No entanto, à medida que acontecia esta evolução tecnológica, cada operador ligado ao negócio do desenvolvimento de *software* pedia proteção jurídica⁷, de modo a evitar imitações e cópias não autorizadas, mas as lacunas jurídicas, quanto à proteção do *software*, ainda eram evidentes e o Direito tinha dificuldade em acompanhar e regular estas situações.

A evolução tecnológica aliada ao aparecimento da *Internet* foi sendo notória um pouco por todo o mundo, abrangeu os vários sectores de cada sociedade, e trouxe novos desafios para o Direito que ainda hoje persistem. No entanto, ninguém fazia prever a dimensão que esta viria a ter.

⁵ Considera-se que foi em 1969, mais concretamente a 23 de junho de 1969, que o *software* adquiriu a sua independência, quando uma das maiores empresas multinacionais do mercado informático, a *IBM* (*Industrial Business Machines*) anunciou a sua intenção de abandonar a prática de *bundling* a partir de 1970 e comercializar (pela primeira vez na história da informática) o *software* separado dos computadores. Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, p.44.

⁶ Gurnsey, John, *Copyright Theft*, Aslib Gower, Hampshire, 1995, p.112.

⁷ Sobre este assunto, ver Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, p.46 a 48.

“No século XIX, os seres humanos raramente produziam sinais eletrónicos. Agora todos emitem *bits*⁸ e *bytes*⁹.”¹⁰ Frases como esta exprimem as enormes mudanças que ocorreram na sociedade até aos dias de hoje. Atualmente podemos dizer que vivemos numa *Era* dominada e comandada pelas novas tecnologias.

Comparando os meios tecnológicos que hoje temos ao nosso dispor com os dos anos anteriores, vemos o longo caminho percorrido pelas tecnologias da informação e da comunicação. Um desses exemplos é o caso dos telemóveis, que são cada vez mais desenvolvidos.

Da mesma forma, as ferramentas digitais, tais como os computadores ou os novos *Tablet* (agora mais finos, leves e facilmente transportáveis), desempenham novas funções e possibilitam novas e rápidas formas de comunicação, através das salas de conversação (as chamadas salas de *chat*¹¹), o correio eletrónico e as mensagens eletrónicas: o que faz com que as relações interpessoais também mudem, sendo cada vez maiores, mais rápidas e mais reais.

Para além disso, as mudanças ocorridas nas tecnologias vieram alterar o modo como vivemos em sociedade, fazendo com que estejamos cada vez mais expostos. Por exemplo: os cartões de crédito mostram os nossos hábitos de consumo, os nossos gostos ou simplesmente as nossas compras do dia-a-dia. As bases de dados de tráfego regulam as nossas viagens e registam quando passamos numa ponte, numa portagem, entramos ou saímos do metro ou autocarro, ou quando viajamos de avião.

As tecnologias emergentes, tais como: os dispositivos de controlo de pulsação, as cada vez mais usadas câmaras de vigilância em rede (hoje em dia já dotadas com *software* de reconhecimento facial e praticamente utilizadas em todos os serviços públicos), os chamados *medidores inteligentes* que entre outras funções registam, por exemplo, a que hora se apaga a luz, à noite.

⁸*Bit*- dígitos binários. Um sistema é construído a partir de duas unidades de informação: 0 ou 1. Cada uma delas é um *bit*. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1031.

⁹*Byte*- Conjunto formado por oito *bits*. Bit é a menor unidade digital de informação, representada por 0 ou 1. *Idem*, *Ibidem*.

¹⁰ Scherer, Michael; Shuster, Simon, *Time Magazine*, Berlim, 2013, in revista *Visão*, 16 de dezembro de 2013, p.74.

¹¹ *Chat* - troca de mensagens em tempo real por utilizadores da *Internet*. Pereira, Joel Timóteo, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.1032.

Estes são alguns exemplos de aparelhos tecnológicos que permitem sempre saber onde estamos ou o que fazemos, a qualquer momento.

O que está a acontecer é uma mudança no modo como vivíamos, nomeadamente, no modo como lemos e escrevemos, no modo como nos entretemos e educamos, no modo como fazemos amizades e criamos comunidades, e no modo como desempenhamos os nossos papéis como cidadãos.¹² Podemos assim afirmar que já não vivemos sem as tecnologias de informação e comunicação e que estas assumiram um papel fundamental no nosso quotidiano. E é assim que nasce o conceito de *Era Global*, caracterizando uma sociedade totalmente interligada entre si e, dominada pelas novas tecnologias.

São infindáveis as mais-valias que podemos encontrar nesta *Era Global*. Desde o simples avanço das Comunicações, através das novas tecnologias, até à evolução do Comércio, veja-se o chamado *e-commerce*¹³, ao avanço da Ciência, da Saúde ou da Educação e também do Direito, por exemplo: a criação da *Intranet* ou do programa *Habilus*, utilizado nos tribunais.

No entanto, algumas destas vantagens podem ter um lado negativo quando usadas de má-fé e em detrimento dos outros. Muitas das preocupações desta *Era Global* estão ligadas ao Direito e dizem respeito à violação dos direitos fundamentais inerentes a cada um de nós, nomeadamente, aos casos de violação da privacidade, violação da propriedade intelectual (por exemplo, o direito de autor), difamação, injúria, entre outros.

A verdade é que a própria natureza e as características da rede digital, ou seja, a livre e global interconexão de computadores e sistemas, aliado ao uso informático de quase todos os setores, serviços e cidadãos, deixa-nos cada vez mais expostos e vulneráveis a ataques perante falhas de segurança, dando assim lugar à chamada “virtual criminal communities”.¹⁴

¹² Fiss, Owen, “In search of a new paradigm”, in *The Yale Law Journal*, vol. 104, n.º 7, maio, 1995, p.1615.

¹³ E-Commerce - comércio eletrónico. Forma de realizar negócios entre empresa e consumidor (B2C) ou entre empresas (B2B), usando a *Internet* como plataforma de troca de informações, encomenda e realização das transações financeiras. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1034.

¹⁴ EUROPOL, *High Tech Crimes Within the EU: Old Crimes New Tools, New Crimes New Tools, Threat Assessment* 2007, [Em linha], High Tech Crime Centre, 2007, p.36. Disponível em [http://www.europol.europa.eu/publications/Serious Crime Overviews/HTCThreatAssesment2007.pdf](http://www.europol.europa.eu/publications/Serious%20Crime%20Overviews/HTCThreatAssesment2007.pdf), (consultado em 20.11.2014).

Temos ainda preocupações no âmbito criminal, em que os casos mais comuns e mais preocupantes dizem respeito aos sistemas de segurança na *Internet*, ao acesso não autorizado a páginas, dados e documentos pessoais; ataques aos próprios servidores, quer dos cidadãos em geral, quer dos próprios órgãos públicos; páginas que oferecem, sem qualquer controlo, conteúdos ofensivos, impróprios: conteúdos obscenos, racistas ou homofóbicos, pornografia comum e pornografia infantil, prostituição de adultos e prostituição de menores.

O uso das novas tecnologias encontra-se também aliado à prática de crimes do chamado “mundo real”, isto é, desde furtos ou fraudes fiscais até aos crimes de coação e ameaças a terceiros, através de mensagens eletrónicas de ódio (*Cyberbullying*), ofensas e casos de perseguição *online* (*Cyberstalking*¹⁵).

Por fim, dadas as várias situações de conflito entre os Estados, tem sido cada vez mais comum o uso das novas tecnologias aliado à prática de atos de terrorismo, seja como meio de os perpetrar, seja como alvo destes ataques.

Como vimos nesta breve introdução, o caminho percorrido pelas tecnologias da informação e comunicação foi longo e a sua evolução foi sendo feita gradualmente desde os primeiros computadores até aos mais atuais. Mas foi, sem dúvida, com a revolução do *software* e o aparecimento da *Internet* que se deu um *boom* exponencial na área da tecnologia e a necessidade de regular cada vez mais questões jurídico-tecnológicas que ainda hoje persistem.

Em seguida iremos analisar a *Sociedade da Informação* e como a *Internet* influenciou as novas tecnologias que hoje conhecemos.

¹⁵ Mais à frente iremos abordar este tema (ver capítulo II). Por agora importa referir que *Cyberstalking* pode ser definido como um fenómeno que envolve ameaças e assédio doentio, em que alguém persegue, de uma maneira assustadora e constante, uma outra pessoa, através dos meios informáticos (seja através do telemóvel ou das redes informáticas). Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 513.

2.- A Sociedade da Informação

“Uma das características marcantes da sociedade em que vivemos é a penetração de novas tecnologias de base científica na vida económica e social”.¹⁶ É graças a esta interligação das novas tecnologias com a nossa sociedade que ouvimos falar da chamada *Sociedade da Informação*. Mas o que se entende por *Sociedade da Informação* e como surgiu este conceito?

Como refere Reginaldo Rodrigues de Almeida, “o conceito de *Sociedade da Informação* desenvolveu-se na Europa Comunitária, a partir da década de 90 do século passado. Inicialmente constituiu a resposta europeia a iniciativas de outros blocos económicos e políticos, como a do Canadá, “Super-Auto-Estradas da Informação”, a do Japão “Infra-Estruturas Avançadas de Informações” e, sobretudo, da norte-americana “Auto-Estradas da Informação”^{17,18}.

O conceito de *Sociedade da Informação* ou, como alguns autores chamam, *Cibersociedade*, traduz-se no facto de que a informação não é um recurso ou bem económico fundamental, mas sim a base do desenvolvimento social e económico atual. Desta forma, a informação é entendida como um bem que não se esgota com o seu consumo, mas é antes enriquecida através de um desenvolvimento ideal das suas funcionalidades, nascendo outra nova informação que cada vez produz mais informação,¹⁹ criando um ciclo. Podemos dizer que o que caracteriza esta Sociedade é o uso da informação de modo intensivo e o valor que ela representa.

¹⁶ Gonçalves, Maria Eduarda, *Direito da Informação*, Almedina, Coimbra, 1994, p.5.

¹⁷ Por “Auto-estrada da Informação” entende-se o “projecto de ligar em rede o maior número possível de sítios informatizados e de lares, para uma difusão personalizada e interactiva de aplicações multimédia de qualquer natureza”. Nora, Dominique, *Os conquistadores do ciberespaço*, tradução, colecção Actualidades, n.º4, Terramar, Lisboa, 1996, p.329. “Auto-estrada da informação” designará, assim, uma rede global, interligando, idealmente, todos os lares, escritórios, escolas e universidades, bem como outras instituições públicas e privadas. Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, p. 313.

Embora a maior e mais conhecida autoestrada da informação seja a *Internet* (Bauche, Gilles, *Tout savoir sur Internet*, Arléa, 1996, pp. 70 e ss.), pelas suas características e proporções, a verdade é que existem outras redes, tais como a *Fidonet* que não opera em tempo real, mas apenas estabelece ligações quando necessário; e a *Super Janet*, que interliga computadores instalados em muitas universidades britânicas. *Idem*, *Ibidem*.

Sobre as autoestradas da informação ver Théry, Gérard, *Les autoroutes de l'information*, Collection des Rapports Officiels, La Documentation Française, Paris, 1994; Baran Nicholas, *Desvendando a superestrada da informação*, Editora Campus, 1995.

¹⁸ Almeida, Reginaldo Rodrigues de, *Sociedade Bit, da Sociedade da Informação à Sociedade do Conhecimento*, 2ª ed., Quid Juris? Sociedade Editora, Lisboa, Setembro, 2004, p.221, *apud.*, Junqueiro, Raul, *A Idade do Conhecimento, A Nova Era Digital*, Editorial Notícias, 2002., p.170.

¹⁹ *Idem*, *Op. Cit.*, p.220.

A procura de informação adaptada às diversas necessidades de utilizadores quer privados quer públicos tem, por sua vez, estimulado a criação de uma gama virtualmente ilimitada de produtos de informação acessíveis em linha ou em suporte eletrónico, bem como de novas formas de processamento da mesma, determinando o desenvolvimento de uma nova indústria, a *indústria da informação*²⁰. Como notam Pedro Veiga e Marta Dias, graças a esta indústria “foi possível uma globalização no acesso à informação, que passou a estar cada vez mais sob a forma digital e que obrigou à mudança da forma como as pessoas e os agentes económicos interagem entre si e com a administração pública”²¹.

Em torno da utilização dos meios de processamento e comunicação da informação, bem como da sua produção, circulação e utilização, emergem novos interesses económicos e sociais que requerem proteção e/ou conciliação por normas de direito.²²

Por um lado, alargam-se tecnicamente as oportunidades de recolha, tratamento e comunicação da informação e da produção dos correspondentes bens e serviços e o direito é chamado a oferecer um quadro normativo capaz de proteger e incentivar o aproveitamento económico e social dessas oportunidades.

Por outro lado, apercebem-se os riscos que poderão acarretar os fluxos de informação, se incontrolados, para a defesa de determinados interesses públicos e privados e apela-se igualmente ao direito para que imponha condições ou restrições a esses fluxos.²³

E é assim, neste novo contexto, de troca de informação e interligação digital, que nasce a chamada *Sociedade da Informação*. Emerge, assim, um domínio onde impera a qualidade de vida, as condições de trabalho, a competitividade das empresas e o alargar do horizonte do conhecimento.²⁴

Como define Masuda, “a Sociedade da Informação é aquela em que a produção de valores de informação e não de valores materiais constitui a força motriz da formação e

²⁰ Gonçalves, Maria Eduarda, *Direito da Informação*, Almedina, Coimbra, 1994, p. 8.

²¹ Veiga, Pedro; Dias, Marta, *A Governação da Internet*, [Em linha], JANUS.NET e-journal of International Relations, nº1, Outono 2010, p.78. Disponível em http://janus.ual.pt/janus.net/pt/arquivo_pt/pt_vol1_n1_pdf/pt_vol1_n1.pdf (consultado em 18.11.2015).

²² Gonçalves, Maria Eduarda, *Direito da Informação*, Almedina, Coimbra, 1994, p. 9.

²³ *Idem, Ibidem*.

²⁴ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.893.

desenvolvimento social, aquela em que o sistema tecnológico computador/telecomunicação determina a natureza fundamental da sociedade”.²⁵

Esta época da Sociedade de Informação é representativa também do capital humano, essencialmente de carácter cognitivo, ou seja, a capacidade de criar valor.²⁶ Assim, na *Sociedade da Informação* os cidadãos passam a dispor de mais e melhores meios de expressão, criação, participação e de interação,²⁷ tendo também um papel mais ativo na própria sociedade.

Passámos, assim, de uma era onde a informação era processada e circulava em pequena escala para uma era onde a informação circula livre e rapidamente à escala global, sem qualquer tipo de controlo ou filtragem e, onde a própria informação adquire agora um outro valor. Transita-se, assim, de uma economia de base industrial, assente na matéria, para uma economia em que o fator imaterial, isto é, os dados, a informação, conhecimentos científicos e técnicos adquirem crescente utilidade e consequente valor económico.²⁸ Não se trata apenas de informação, no sentido *lato* da palavra, mas sim de um material de troca com valor económico.

Esta *Sociedade da Informação* não se caracteriza apenas pelo crescente uso e aparecimento das novas tecnologias, mas também pela crescente informação (por vezes errada e plagiada) que circula na rede digital e que cada vez mais é criada sem controlo²⁹. E este é um dos problemas que destacamos na *Sociedade da Informação*, a manipulação da informação presente na rede.

Por estar diretamente relacionado com este ponto do tema, abordamos aqui outro conceito importante, o de *Sociedade do Conhecimento*, e fazemos uma breve distinção entre *Sociedade da Informação* e *Sociedade do Conhecimento*. Embora pareçam conceitos similares, a verdade é que *Sociedade da Informação* não significa Sociedade

²⁵ Gonçalves, Maria Eduarda, *Direito da Informação*, Almedina, Coimbra, 1994, p. 9. *apud*. Y., Masuda, *The Information Society*, Tokyo: Institute for the Information Society, 1981, p.1.

²⁶ Freire, Vicente, “Cibersegurança e Ciberdefesa: A Inevitabilidade de adoção de uma estratégia nacional”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.56.

²⁷ Gonçalves, Maria Eduarda, *Direito da Informação*, Almedina, Coimbra, 1994, p.8.

²⁸ *Idem*, *Op. Cit.*, p.9.

²⁹ É cada vez maior a quantidade de informação que circula pelas redes e que é armazenada nos sistemas informáticos. Num estudo realizado pela Universidade de Berkeley, apurou-se que 92% de toda a informação armazenada pela humanidade está guardada em meios magnéticos, designadamente discos rígidos. Anualmente é compilada informação equivalente a meio milhão de novas bibliotecas, cada uma delas com o tamanho da biblioteca do Congresso dos Estados Unidos. Verdelho, Pedro, *Cibercrime e Segurança Informática*, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º6, Coimbra Editora, Julho-Dezembro 2005, p. 160.

do *Conhecimento*. Tal como refere Reginaldo Rodrigues de Almeida, na *Sociedade da Informação* estamos todos, mas não na *Sociedade do Conhecimento*.³⁰ Isto é, a *informação* disponibilizada no mundo digital tem vindo a aumentar e, por conseguinte, é fácil ter acesso a novas pesquisas, novos conhecimentos, novos estudos. No entanto, tem-se verificado um decréscimo no teor e na qualidade destes conteúdos. Embora haja uma maior facilidade de acesso e envio de informação, a verdade é que tal informação parece não se ter convertido em conhecimento, mas, pelo contrário, tem dado origem a um decréscimo de conhecimento.

A quantidade cada vez maior de informação presente na nossa sociedade torna não só difícil de a quantificar, como qualificar o seu bom uso, pelo que é preciso conhecer métodos para a conversão da informação selecionada em conhecimento útil e verdadeiro.

Estamos constantemente a receber e a produzir informação que, por vezes, nada de novo acrescenta aos temas que já foram debatidos, que circula e é consultada pelo mundo todo. E são muitos os exemplos que hoje encontramos na rede, principalmente a nível académico: trabalhos já feitos sem as devidas referências bibliográficas, ou feitos sem qualquer rigor académico, textos mal traduzidos, apontamentos pessoais com erros de conteúdo e de ortografia, resumos e notas bibliográficas que não correspondem às frases citadas, entre outros exemplos. Falamos aqui de todas as formas de alterar o conteúdo informacional, desde a omissão à distorção da informação, que comprovam o excesso de informação e falta de conhecimento científico que aqui mencionámos. Assim, é fundamental que se transforme a informação presente na nossa sociedade em conhecimento.

Como refere Reginaldo Rodrigues de Almeida, “sem conhecimento, as infra-estruturas digitais por muito sofisticadas e poderosas que possam ser, não terão a capacidade de proporcionar os serviços e os conteúdos em que terão de assentar as novas formas de produção e de consumo. Sem conhecimento, a mobilidade transformar-se-á em hábito e acção rotineira, insusceptível de provocar uma nova dinâmica económica e social”.³¹ Acrescenta ainda que, “o conhecimento tem que ver com as pessoas, com as suas qualificações e a sua preparação para lidar com a conectividade, a informação, a

³⁰ Entrevista a Reginaldo Rodrigues de Almeida, realizada no dia 19 de maio de 2014.

³¹ Almeida, Reginaldo Rodrigues de, *Sociedade Bit, Da sociedade da Informação à Sociedade do Conhecimento*, 2ª ed., Quid Juris? Sociedade Editora, Lisboa, Setembro, 2004, p.223.

convergência e a mobilidade”.³² Só assim poderemos atuar em todos os aspetos que nos possam lesar.

Existe, um excesso de informação que, na nossa opinião, é necessário reorganizar. Como tal, primeiro que tudo é preciso não deformar, mas sim informar os cidadãos. Transmitir-lhes conhecimentos específicos sobre o que é e como devem atuar nesta *Sociedade da Informação*, seja através de: palestras, conferências ou até nas salas de aulas das escolas, universidades, institutos..., abordando questões importantes como o direito de autor³³, o plágio, manipulação e falsificação de informação, entre outros temas.

Da mesma forma, é necessário informar os cidadãos de que o mundo digital, embora sendo um espaço vasto, com características próprias e, sem fronteiras, não é um espaço totalmente livre e que não está imune à atuação do Direito. Em nossa opinião, ainda é notória a infoexclusão³⁴ por parte dos utilizadores quanto às novas tecnologias, na maioria dos adultos e idosos. Quanto aos jovens, como estão entre os principais utilizadores da *Internet*, são extremamente vulneráveis a abordagens via *Ciberespaço* e encontram-se também muito pouco sensibilizados para os riscos daí decorrentes.

Depois de ter sido implementada a cultura e o incentivo à utilização da tecnologia, é atualmente necessário implementar uma cultura de segurança dos sistemas informáticos e das redes.

Outro dos problemas que destacamos na *Sociedade da Informação* é a possibilidade de converter os sistemas de informação e comunicação em autênticas armas quando são utilizadas para causar danos às infraestruturas de um Estado. Hoje em dia, assistimos a

³² Almeida, Reginaldo Rodrigues de, *Sociedade Bit, Da sociedade da Informação à Sociedade do Conhecimento*, 2ª ed., Quid Juris? Sociedade Editora, Lisboa, Setembro, 2004, p.223.

³³ Sobre este ponto importa referir que os direitos de autor “continuam a ter a sua própria vigência no mundo online, da mesma maneira que no mundo físico”. Gandelman, Henrique, *De Gutenberg à Internet: direitos autorais na era digital*, p. 154.

Quanto à titularidade do direito de autor, as obras previamente existentes não apresentam quaisquer problemas específicos no *ciberespaço*, pois os princípios tradicionais do Direito de Autor permitem identificar os seus autores ou titulares do direito de autor. Daí que, também as sanções civis e criminais previstas para as violações de direitos de autor da época em que as obras intelectuais apenas tinham o formato analógico continuam a ter aplicação válida para o novo mundo digital. Por exemplo, a distribuição/disponibilização, na rede de uma obra protegida por direito de autor, foi considerada pela jurisprudência como constituindo contrafação (artigos 196.º e 197.º do CDADC) – nesse sentido se pronunciou o Tribunal de Grande Instância de Paris, em Sentença de 14 de agosto de 1996, publicada com anotação de F. Olivier/ F. Barbry, em *La Semaine Juridique*, edição geral, *Juris-Classeur Périodique*, 1996, II, n.º22727, pp.441 e ss; e também o Tribunal de Primeira Instância de Bruxelas, em sentença de 16-10-96, in *Dalloz*, *Recueil*, 26 de junho de 1997, n.º25, 1997, caderno jurisprudência, pp.322 e ss.

³⁴ Neologismo não dicionarizado (junção das palavras informática + exclusão).

vários exemplos de ações de agressão às redes digitais, provenientes do território nacional ou estrangeiro, através da *Internet* ou de outros meios de comunicação, com o intuito de promover a rutura da ordem social e/ou a institucionalização constitucional de outro Estado, como acontece, por exemplo, no caso do Estado Islâmico que utiliza os sistemas de informação e comunicação, na grande maioria a *Internet*, para transmitir as suas mensagens e ameaças ao Mundo, ou para recrutar novos aliados.

Por outro lado, temos os casos de violação do espaço informático de um Estado ou a sua utilização para interesses contrários ao Estado, seja para prejudicar, paralisar ou causar danos nestes meios de comunicação (por exemplo, através do bloqueio ou eliminação de páginas da *Internet* dos órgãos do Estado, ou divulgação nestas páginas dos dados pessoais e informações confidências de magistrados e outros funcionários do Estado³⁵).

Por último, vemos o uso da *Sociedade da Informação* ligada aos crimes informáticos:

- Propagação de vírus informáticos;
- Implantação de sistemas radioelétricos de intercessão de informação nos meios técnicos;
- Utilização ilícita de sistemas de informação e telecomunicações ou de recursos informáticos;
- Implantação, informação falsa, entre outros exemplos.³⁶

É certo que a nova infraestrutura da informação (*Internet*), as denominadas autoestradas eletrónicas da informação, aliadas ao fim das fronteiras nacionais, trouxeram vários desafios, não só económicos, como jurídicos e sociais.³⁷

De entre todas as inovações tecnológicas, sem dúvida alguma que a *Internet* foi a que mais modificou a *Sociedade da Informação*³⁸. Com qualquer aparelho que disponha de

³⁵ Como aconteceu em 2014 (mais concretamente, no dia 25 de abril de 2014) com o sítio oficial do Ministério Público, onde foram revelados dados pessoais e informações confidências sobre os próprios Magistrados por um *hacker* anónimo.

³⁶ Augusto, Mário, *As Nações Unidas no Contexto do Direito Internacional*, Estudos e documentos, Novo Imbondeiro, Lisboa, 2004, p.99.

³⁷ Marques, Garcia; Martins, Lourenço, *Direito da Informática*, Lições de Direito da Comunicação, Almedina, Novembro, 2000, p.44.

³⁸ Mais de vinte anos após a criação da *Internet* (segundo estudos, terá sido no início de 1983 que o Departamento de Defesa dos Estados Unidos fez substituir a *ARPANet*, rede interna de comunicação entre departamentos militares, por uma rede aberta e mais alargada, utilizando o protocolo TCP/IP, ainda hoje usado), a *Sociedade da Informação* vive numa dependência existencial dos sistemas informáticos. O seu normal funcionamento e desenvolvimento dependem vitalmente daqueles sistemas. Verdelho, Pedro,

ligação à *Internet* é hoje possível em qualquer lugar expor a nossa opinião, ou simplesmente publicar textos, adquirir praticamente qualquer bem ou serviço, estar em contacto com qualquer pessoa ou instituição, em qualquer parte do mundo e até praticar atos criminosos ou terroristas contra os Estados.

Em face do exposto, conseguimos perceber como a *Sociedade da Informação* abarca vantagens e desvantagens. Por um lado, é um instrumento fundamental para a melhoria e desenvolvimento da qualidade de vida dos cidadãos e, para o desenvolvimento sustentável de uma sociedade; por outro, cria novos tipos de crimes e novas formas de os cometer.

Concluindo: a *Sociedade da Informação* necessita de mecanismos reguladores capazes de certificar o acesso à informação em condições de segurança, de forma a garantir os direitos dos Cidadãos, a inviolabilidade da privacidade nas comunicações e a funcionalidade em segurança dos sistemas e infraestruturas sensíveis.³⁹

É difícil fazermos um balanço sobre estas novas tecnologias e analisar o impacto que estão a ter e terão no futuro da nossa sociedade, visto que estamos em constante evolução. Mas a verdade é que tais ferramentas tecnológicas trazem mudanças para a nossa sociedade em todos os âmbitos, difíceis de acompanhar pelo Direito. E é neste contexto que este tema se torna tão interessante, pois são ainda muitas as questões levantadas face às poucas respostas.

Nos capítulos seguintes iremos analisar detalhadamente algumas destas temáticas e tentar esclarecer como devemos garantir certos direitos e deveres fundamentais que à partida parecem ser difíceis de conciliar.

“Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º6, Julho-Dezembro 2005, p. 160.

³⁹ Macedo, Miguel, “O Desafio da Cibersegurança”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.34.

3. O Ciberespaço

3.1.- Evolução

O que começou por ser um conjunto de cabos e interruptores que permitiam a comunicação e conectividade entre os computadores de investigadores e técnicos, rapidamente se tornou num símbolo de crescimento da economia nacional e vitalidade social.

No início da década de 80 quando começaram a surgir novos desenvolvimentos nas telecomunicações, incluindo o aparecimento da *Internet*, criou-se um espaço no mercado virtual ilimitado para a propagação e venda de ideias, bens e serviços a uma escala global. Ou seja, um mundo de seres, atividades, ambientes e códigos totalmente novos, aglomerados num novo termo *Ciberespaço*, que engloba as comunidades intangíveis e o espaço interativo, tornado possível pelo conjunto de redes da *Internet*.⁴⁰

Segundo a maioria dos autores, a expressão *Ciberespaço*⁴¹ surgiu pela primeira vez no romance de William Gibson, *Neuromancer*⁴² (“Neuromante” tradução portuguesa) de 1984, utilizado para descrever o espaço relacional de troca imaterial, onde os indivíduos podem interagir sem presença física, conversando e trocando dados através de terminais e redes interpostos.⁴³

O *Ciberespaço* é entendido como o “domínio⁴⁴ caracterizado pelo uso de equipamentos eletrónicos e do espectro eletromagnético para armazenar, modificar e trocar dados via sistemas em rede”. Dinamizado por um conjunto de políticas, ditas de *Sociedade da Informação*, o *Ciberespaço* tem vindo a oferecer um vasto conjunto de potencialidades,

⁴⁰ Akdeniz, Yaman; Walker, Clive; Wall, David, *The Internet, Law and Society*, Longman, Pearson Education, 2000, p.3.

⁴¹ “Ciber” deriva do termo grego *Kybernan*, que significa navegar ou controlar o “espaço”.

⁴² “Neuromancer é um livro de ficção científica que introduziu novos conceitos para a época, como a inteligência artificial avançada e um ciberespaço quase que “físico” (...).” Neto, Arnaldo Sobrinho de Moraes, *Cibercrime e Cooperação Penal Internacional: um enfoque à luz da Convenção de Budapeste*, Universidade Federal de Paraíba – UFPB, João Pessoa, 2009, p. 41.

⁴³ Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, p.322.

⁴⁴ Quando o *Ciberespaço* é perspetivado para a condução de Operações Militares; este é materializado pelo “domínio da Eletrónica, do Eletromagnetismo, das Redes e das Infraestruturas físicas que se lhe encontram associadas”, in *Visão Estratégica do Air Force Cyber Command*.

excepcionais contributos para as organizações e sua gestão, bem como para as infraestruturas e a cidadania.⁴⁵

De uma forma geral, o conceito *Ciberespaço* é utilizado para referir algo ligado à *Internet* e às novas práticas socioculturais que lhe estão associadas. Pela sua própria natureza complexa e multifacetada, o *Ciberespaço*, no sentido mais rigoroso do termo, é suscetível de uma abordagem multidimensional e de ser objeto de investigação a partir de variadas disciplinas.⁴⁶ Para o seu estudo, convergem, entre outras, a perspetiva tecnológica, sociológica, jurídica, política, estratégica e de segurança.⁴⁷

Em formulação simplificada, o *Ciberespaço* resume-se a um conjunto de computadores com ligação entre si. As ligações efetuadas podem ser por terra, por fio ou cabo, sem fio (ou seja, wireless – por ondas de rádio, infravermelhos, satélite) ou ambas. “De forma mais complexa, o ciberespaço é definido como a rede interdependente de infraestruturas de tecnologia de informação, incluindo a *Internet*, redes de comunicação, sistemas de computador e processadores e controladores parte de indústrias críticas”.⁴⁸ Acresce a estes elementos o ambiente virtual de informação e interações entre as pessoas.⁴⁹

A indústria tecnológica sofreu a sua primeira alteração quando passou de uma era de computadores individuais, em que o seu funcionamento e armazenamento estavam apenas condicionados a uma *mainframe*⁵⁰ isolada numa sala fechada, para uma era em que os computadores pessoais se interligam a redes informáticas, juntamente com outros tantos milhões de computadores espalhados pelo mundo, todos capazes de partilhar informações entre si.⁵¹ Da mesma forma, as atividades da vida real passaram a desenvolver-se no mundo digital, no chamado *Ciberespaço*.

⁴⁵ Freire, Vicente, “Cibersegurança e Ciberdefesa: A Inevitabilidade de adoção de uma estratégia nacional”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.53.

⁴⁶ Fernandes, José Pedro Teixeira, “Utopia, Liberdade e Soberania no Ciberespaço”, in *idn Nação e Defesa, Instituto de Defesa Nacional, Cibersegurança*, Revista Quadrimestral, n.º133, p.12.

⁴⁷ *Idem, Ibidem*.

⁴⁸ US National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23), *apud.*, Galdes, Ana Vaz, *Ciberterrorismo: cenário de materialização*, in Revista da Faculdade de Direito da Universidade de Lisboa, Coimbra, vol.53 n.º1-2, 2012, p.43

⁴⁹ *Idem, Ibidem*.

⁵⁰ Designa-se por *Mainframe*, um computador de grande porte, dedicado normalmente ao processamento de uma vasta quantidade de informação. Uma vez que são equipamentos que ocupam muito espaço e necessitam de muita manutenção, foram substituídos por servidores de computadores pessoais e servidores *Unix* (sistema operativo), com custos significativamente mais baixos e que necessitavam de menor manutenção.

⁵¹ Reynolds, George W., *Ethics in Information Technology*, Third Edition, Course Editions, USA, 2010, p.74.

Este *Ciberespaço* passou a englobar dois conceitos, os quais achamos importante definir e distinguir desde já. São eles o conceito de *Internet*⁵² e de *World Wide Web*⁵³ (também conhecida como *Web*).

O primeiro conceito, *Internet*, é a camada ou rede física composta por *switches*, *routers* e outros equipamentos que permitem o seu funcionamento. Esta tem como função primordial transportar informação de um ponto para outro de forma rápida e segura. Quanto ao segundo conceito, *World Wide Web*, é uma camada de dispositivos e aplicativos que opera sobre a *Internet*. Esta tem como função essencial oferecer uma ligação que transforme as informações que fluem pela *Internet* em algo utilizável.⁵⁴

Da mesma forma, também a evolução de cada uma teve fases distintas.

Quanto à *Web*, originalmente chamada de *ARPANET (Advanced Research Projects Agency Network)* manteve-se até à década de 80 com uma utilização exclusivamente académica (era utilizada para ligar a Universidade da Califórnia em Los Angeles, o Instituto de Investigação em Stanford, a Universidade da Califórnia em Santa Bárbara e a Universidade de Utah), altura em que se libertou e passou a ser uma estrutura sem proprietário, sem fronteiras e, como alguns pretendiam, sem limites. Após esse período, passou a ser chamada de *Panfetoware*, ao ficar reconhecida e caracterizada pela “luta” pelos nomes de domínio⁵⁵. Esta etapa concentrou-se na necessidade de quase todas as empresas partilharem informações na *Internet* para que as pessoas pudessem saber sobre os produtos e serviços que essas mesmas empresas disponibilizavam.⁵⁶

A terceira evolução da *Web* deu-se quando esta passou de um patamar de dados fixos para um patamar de informações transacionais, nas quais produtos e serviços podem ser comprados e vendidos, assim como era possível oferecer serviços. Foi nesta fase que

⁵² *Internet* - teve início em meados de 1969 pelo Departamento de Defesa dos Estados Unidos da América. É a interligação de computadores das mais variadas regiões numa mesma rede, possibilitando a comunicação em tempo real. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1036.

⁵³ *World Wide Web* (Rede de Alcance Mundial). Conjunto interligado de documentos e arquivos que fazem parte da *Internet* e se encontram armazenados em servidores [http](http://). *Idem*, *Op. Cit.*, p.1045.

⁵⁴ Evans, Dave, *A Internet das Coisas, como a próxima evolução da Internet está mudando tudo*, Cisco Internet Business Solutions Group (IBSG), abril 2011, p.3.

⁵⁵ “Se a função inicial dos nomes de domínio consistia em possibilitar a localização de informação na rede, a crescente utilização comercial desta, veio conferir-lhes outras funções ligadas a essa utilização, como a de distinguir produtos e serviços oferecidos em linha.” Gonçalves, Maria Eduarda, “Internet, Direito e Tribunais”, *Sub Judice, Justiça e Sociedade*, revista trimestral n.º35, Almedina, Setembro 2006, p.6.

⁵⁶ Evans, Dave, *A Internet das Coisas, como a próxima evolução da Internet está mudando tudo*, Cisco Internet Business Solutions Group (IBSG), abril 2011., p. 5.

surgiram empresas como o *eBay*, a *Amazon.com* e tiveram o seu *boom* exponencial. Foi também nesta altura que as chamadas “ponto com” (.com) tiveram um grande crescimento⁵⁷.

Por fim, a quarta etapa, é aquela em que nos encontramos agora e é chamada de *Web social* ou de *experiência*, graças a empresas como *Facebook*, *Twitter*, *Instagram*, que se tornaram famosas e rentáveis pela possibilidade de interação direta entre pessoas de todo o mundo, criando uma maior interação social. Esta etapa tem como distinção em relação à terceira, o facto de permitir que pessoas de todo o mundo interligadas pelas redes informáticas comuniquem, conectem e compartilhem informações por exemplo: textos, fotografias, vídeos sobre si mesmos com amigos, familiares, colegas ou até mesmo com desconhecidos.⁵⁸

Contrariamente à *Web*, a *Internet* teve uma evolução mais gradual, mantendo quase sempre o objetivo para a qual foi criada na era da *ARPANET*, ou seja, uma função educacional, académica.

Não obstante todos estes avanços tecnológicos, foi apenas em 1995 que se deu início ao crescimento da *Internet* junto do público em geral. Como notam Pedro Dias e Marta Veiga “houve a perceção de que a Internet poderia vir a ser muito importante como instrumento de desenvolvimento”⁵⁹. Imediatamente, foram colocadas várias questões, no âmbito da sua funcionalidade e das suas características. Destacando-se uma questão à qual ninguém parecia saber responder, “quem controla a *Internet*?”⁶⁰.

Particularmente e, face à questão apresentada, subsistiam dois tipos de recursos que se destacaram⁶¹: os chamados *nomes de domínio*⁶² e os *endereços de IP*⁶³ (*numbers*)

⁵⁷ Evans, Dave, *A Internet das Coisas, como a próxima evolução da Internet está mudando tudo*, Cisco Internet Business Solutions Group (IBSG), abril 2011., p.5.

⁵⁸ *Idem*, *Op. Cit.*, p.6.

⁵⁹ Veiga, Pedro; Dias, Marta, *A Governação da Internet*, [Em linha], JANUS.NET e-journal of International Relations, nº1, Outono 2010, p.78. Disponível em http://janus.ual.pt/janus.net/pt/arquivo_pt/pt_vol1_n1_pdf/pt_vol1_n1.pdf (consultado em 18.11.2015).

⁶⁰ *Idem*, *Ibidem*.

⁶¹ *Idem*, *Ibidem*.

⁶² *Nomes de Domínio* (ou também chamados de *Domain Names*). Nome como determinada entidade ou computador é identificado pelo servidor de nomes na *Internet* (exemplo: em www.quidjuris.pt, o domínio é “pt”. Por sua vez, “quid juris” é o subdomínio e “www” é a *World Wide Web*). Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1033. Os nomes de domínio constituem o primeiro e principal instrumento de referência na *Internet*, o modo como todos nos orientamos na sua geografia ou na sua cartografia. Sem um completo domínio da sua regulação e aplicação prática, torna-se difícil a navegação no *ciberespaço*.

usados pelos computadores para aceder à *Internet*. Os nomes de domínio, ou *domain names*, eram os que originavam mais problemas, verificando-se uma situação especial. Os domínios que terminassem com duas letras eram da responsabilidade de cada país (por exemplo, “pt” Portugal, “es” Espanha, “it” Itália), quanto aos “domínios globais (.com, .org, .net, .edu) eram geridos e comercializados em regime de monopólio, conferido via contrato, por uma empresa americana, a *NSI - Network Solutions International*”⁶⁴, que era quem detinha o domínio maioritário dos mesmos. Logo aí surgiu um problema, pois se cada país detinha um nome de domínio e cada empresa também (no caso dos domínios “.com”, “.org”, etc.), imagine-se a quantidade de possíveis reguladores da *Internet*.

Assim, e face aos diversos movimentos de tentativa de regulamentação da *Internet* e das relações estabelecidas através dela, o ativista norte-americano *Perry Barlow* proclamou em fevereiro de 1996 a “Declaração de Independência da *Internet*”, da qual constava a seguinte citação: “Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.”⁶⁵ Estávamos, assim, perante um novo espaço tecnológico sem fronteiras, sem um poder soberano e sem legislação.

Embora se refira que o *Ciberespaço* é um lugar sem um organismo central responsável pelo estabelecimento de regras jurídicas (com força impositiva e coativa), este sempre foi regulado por regras técnicas que ajudaram no cumprimento de um padrão lógico da tecnologia utilizada na ligação, na comunicação, e nas atividades na *Internet*.

Andrade, Miguel Almeida, *Nomes de Domínio na Internet, A Regulamentação dos Nomes de Domínio sob. PT*, CENTROATLANTICO.PT, Portugal, 2004.

⁶³ IP- Abreviatura de *Internet Protocol*. Uma das linguagens, ou protocolos, mais importantes da *Internet*, responsável pela identificação das máquinas e redes e pelo encaminhamento correto de mensagens entre elas. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.1036. O IP identifica o cliente. Serve para abrir e reforçar a prova.

⁶⁴ Veiga, Pedro; Dias, Marta, *A Governação da Internet*, [Em linha], JANUS.NET e-journal of *International Relations*, nº1, Outono 2010, p.78. Disponível em http://janus.ual.pt/janus.net/pt/arquivo_pt/pt_vol1_n1_pdf/pt_vol1_n1.pdf, (consultado em 3.4.2014).

⁶⁵ Perry Barlow “Declaration of the Independence of Cyberspace”. Disponível em <https://projects.eff.org/~barlow/Declaration-Final.html> (consultado em 23.11.2015).

A comunicação na *Internet* é feita através de uma “linguagem de comunicação” comum chamada TCP/IP⁶⁶ (*Transmission Control Protocol/ Internet Protocol*). Para que esta comunicação seja realizada com sucesso, é fundamental o sistema de desenvolvimento, de validação e de aprovação das especificações padrão estabelecidas pela chamada *Internet Society*⁶⁷ (ISOC), que é uma organização de utilizadores da *Internet* inteiramente composta por voluntários, com o único objetivo de promover uma troca universal da informação, através da mesma tecnologia utilizada na *Internet*.⁶⁸

Na *Internet Society*, existe o chamado *Internet Architecture Board* (IAB), constituído por um grupo de especialistas que supervisiona a evolução tecnológica da rede *Internet*.⁶⁹ O IAB é responsável pela orientação a longo prazo, por velar pela coerência da arquitetura e, mais genericamente, pela supervisão do processo.

Por outro lado, temos ainda um conjunto de regras não escritas, transmitidas e passadas entre os utilizadores denominadas de “netiquette”, traduzindo, assim, um conjunto de “boas maneiras” a adotar no *Ciberespaço*. O utilizador que transgrida as regras de *netiquette*, por exemplo: praticando atos de *flaming*⁷⁰, *shunning*⁷¹, *mailbombing*⁷², entre outros, pode ser sancionado pela comunidade de utilizadores.⁷³

⁶⁶ Na *Internet* o caminho seguido pelos pacotes de informação TCP/IP não é o mais curto, mas sim o menos congestionado. Descarregar uma página *web* alojada num servidor em Lisboa para um computador em Coimbra, ou ler em Coimbra uma mensagem de correio eletrónico da mesma proveniência, pode implicar uma viagem da informação através de um país situado fora da União Europeia. Castro, Catarina Sarmiento e, “Proteção de Dados Pessoais na Internet”, in Gonçalves, Maria Eduarda, *Internet, Direito e Tribunais, Sub Judice, Justiça e Sociedade*, revista trimestral n.º35, Almedina, Setembro 2006, p. 29.

⁶⁷ Sobre a estrutura da *Internet Society*, Dufour, Arnaud, *Internet*, 4ª ed., P.U.F., col. “Que Sais-Je?”, n.º3073, Paris, 1997. Tradução portuguesa, Dufour, Arnaud, *A Internet*, Publicações Europa-América, Coleção “Saber”, n.º235, 1997.

⁶⁸ Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, 326.

⁶⁹ Silva, Libório, Remoaldo, Pedro, *Introdução à Internet*, 2.ª ed., Editorial Presença, Lisboa, 1996, p.18.

⁷⁰ *Flaming* - O fenómeno *online* de *flaming* ocorre quando o utilizador perde o autocontrolo e escreve uma mensagem que emprega linguagem depreciativa, obscena ou indecorosa. Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, 327.

⁷¹ *Shunning* – Sucede quando um utilizador da *Internet* se recusa a receber mensagens de outra pessoa utilizadora da Net (ou, mais genericamente, quando utiliza um programa de computador conhecido como um “*kill file*” para automaticamente desviar qualquer mensagens de correio eletrónico de um endereço especificado). *Idem, Ibidem*.

⁷² *Mailbombing* – Um utilizador da *Internet* lança uma “*mailbomb*” a uma determinada vítima, enviando-lhe um elevado número de mensagens de correio eletrónico sem conteúdo útil, com o objetivo de sobrecarregar (ou, pelo menos, perturbar) o computador recetor. *Idem, Ibidem*.

⁷³ Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, 327.

Importa salientar que todas estas normas não têm força de lei; são apenas especificações, publicadas para prestar um serviço à comunidade virtual e aos próprios utilizadores.

É um facto que o *Ciberespaço*, por envolver tantas e valiosas transações de informação, não é um lugar harmonioso. Assim, à medida que aumenta o número de utilizadores no *Ciberespaço* aumentam também as expectativas de que as normas legais do mundo real sejam igualmente aplicáveis. Atualmente são cada vez mais os casos de advogados e magistrados que são chamados a acusar, defender ou decidir litígios emergentes das cibercomunidades.

Sempre que se criam novas oportunidades, surgem também novos riscos e novos desafios que tornam difícil garantir a segurança dos sistemas públicos e privados, e da própria sociedade.

Recentemente, o aumento dos fluxos de informação no *Ciberespaço* são de tal ordem numerosos e complexos que, em certos casos, é impossível determinar a sua origem geográfica, os agentes e as circunstâncias conexas.⁷⁴

A verdade é que a *Internet*, enquanto meio eletrónico que não conhece fronteiras geográficas, desestabilizou o Direito ao criar fenómenos totalmente novos que necessitam de ser objeto de normas jurídicas claras e coercivas. Dadas as suas características a *Internet* permite e/ou facilita a prática de numerosos tipos de crimes informáticos de cariz transnacional, o que dificulta ainda mais a aplicação do Direito. Não se trata apenas de ataques de *hackers*, de ações de propaganda extremistas e da criminalidade organizada, mas também do apoio a ataques terroristas (como sucedeu em

⁷⁴ Por exemplo, no seguimento de uma investigação do FBI, que encerrou o sítio de partilha de arquivos “Megaupload” sob a acusação de que este facilitava a troca indevida de conteúdos protegidos ao abrigo da legislação norte-americana de direitos de autor, ocorreu a maior represália de sempre do grupo *hacker* “Anonymous” que em poucas horas lançou um ataque aos sítios das associações norte-americanas de cinema e música (MPAA, RIAA), para além dos sítios oficiais do Departamento de Justiça dos Estados Unidos da América, do US Copyright Music e até do FBI. Tratou-se de um ataque do tipo DDOS (*distributed denial of service*) que consiste numa ordem transmitida a milhares de computadores dominados (zombies) por um ou mais computadores dominadores (master) no sentido daqueles “entupirem” um determinado sistema/servidor tornando-o indisponível aos seus legítimos utilizadores. Pereira, Júlio, “Cibersegurança, O Papel do Sistema de Informações da República Portuguesa”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.38.

Nova Iorque, Washington) e de ações ilegítimas de outras entidades estatais (como sucedeu recentemente na Estónia⁷⁵ e na Georgia).⁷⁶

A importância do *Ciberespaço* foi bem evidenciada por Barry Posen⁷⁷, ao considerar o *Ciberespaço* como um novo “Global Common⁷⁸”, a juntar aos tradicionais espaços comuns: as águas internacionais; o espaço aéreo internacional e o espaço exterior. Barry Posen define estes espaços comuns como “os espaços que não estão sob o controlo direto de qualquer Estado, mas que são vitais para o acesso e ligação a quaisquer pontos do mundo”.⁷⁹

Nestes espaços assentam todas as redes de telecomunicações vitais, de transporte e de distribuição de energia das quais depende o comércio global, a segurança energética e a prosperidade das sociedades modernas.⁸⁰

Desta forma, o *Ciberespaço*, ao ser considerado como o quinto espaço comum, a seguir à terra, mar, ar e o espaço exterior (atmosfera), necessita de ser regulado e coordenado de forma única por todos os Estados. É fundamental consciencializar as comunidades internacionais sobre a necessidade de criar um mecanismo de resposta global de combate a estas novas *ciberameaças*.

Sobre este assunto e face à falta de cooperação internacional tem sido várias vezes debatida a ideia da criação de um Tribunal Criminal Internacional ou a criação de um

⁷⁵ Em maio de 2007, na Estónia, um dos Estados mais avançados em termos de implementação da tecnologia de “governo eletrónico”, o chamado *e-government*, foi alvo de um ciberataque. Segundo as autoridades estónias, os ataques atingiram mais de um milhão de computadores no país, causando danos a inúmeros sítios governamentais, de partidos políticos, de grandes empresas, de dois grandes bancos e também a empresas na área da comunicação. Provenientes de endereços russos, alguns do governo, os ataques à Estónia manifestaram como principal característica os ataques de negação de serviço, tendo a NATO enviado posteriormente para aquele Estado Membro especialistas em terrorismo virtual para apuramento de responsabilidades. Os referidos especialistas analisaram os ataques e não conseguiram descartar totalmente tal possibilidade, avançada pela Federação Russa, de os endereços terem sido trocados ou falsificados. *Idem, Op. Cit.*, pp.38 e 39.

⁷⁶ Viana, Vítor Rodrigues, “Cibersegurança”, *idn Nação e Defesa, Instituto da Defesa Nacional, Revista Quadrimestral*, n.º133., p.6.

⁷⁷ Barry Posen, Professor de Ciência Política do MIT.

⁷⁸ Os *Global Commons* são os espaços comuns onde funcionam as interações que existem entre o processo de globalização.

⁷⁹ Viana, Vítor Rodrigues, “Cibersegurança”, *idn Nação e Defesa, Instituto da Defesa Nacional, Revista Quadrimestral*, n.º133., p.5.

⁸⁰ *Idem, Ibidem.*

Tribunal do Ciberespaço que permita tomar medidas contra estes ciberataques a nível global.⁸¹

A adoção de uma estratégia para enquadrar o que respeita ao uso seguro do *Ciberespaço* torna-se cada vez mais uma exigência⁸². À medida que aumenta o número de utilizadores da *Internet*, aumentam também as possibilidades de cometer novos crimes, de surgirem novos cibercriminosos e novas vítimas.

Por tudo isto, só será possível assegurar a plenitude das vantagens e oportunidades que o *Ciberespaço* nos proporciona, se garantirmos a confiança da sua fiabilidade e resiliência a ameaças externas.

⁸¹ Judge Schjolberg, Stein, *A presentation at the Europol – INTERPOL Cybercrime Conference*, The Hague, The Netherlands, September 24-25, 2013, p.8.

⁸² Como revelou Cecilia Malmström (Comissária Europeia para os Assuntos Internos) numa conferência ocorrida em Bruxelas, a 9 de novembro de 2011, intitulada “Defining Cyber Security”, “a negação acerca da escala das ameaças do *ciberespaço* é ingénuo. (...) Esta é uma batalha que talvez não consigamos vencer, mas o *ciberespaço* é um domínio em que temos de atuar e temos de proteger o mais rápido possível”. Acrescentando que “sem partilha de informação, são poucas as ações concretas que podemos tomar”. (Tradução livre)

3.2.- A Internet na Era Global

Quando foi criada a *Internet* na década de 60, mais concretamente em 1969, pelo governo norte-americano para fins militares⁸³, nada fazia prever a escala global e as capacidades que esta viria a alcançar.

Foi graças à *World Wide Web* que a *Internet* se tornou no fenómeno que é atualmente e adquiriu a maioria das suas capacidades. Atualmente a *Internet* permite: armazenar e partilhar ficheiros com computadores e pessoas de todo o mundo; obter informação em formato digital, de forma rápida, simples e acessível a todos, em qualquer parte; localizar de forma rápida e simples qualquer pessoa ou serviço; entre outros.

Como já vimos, um pouco por todo o mundo foram implementadas medidas de incentivo à utilização das novas tecnologias que rapidamente deram origem a um espaço sem fronteiras espaciais, terrestres, sociais, económicas, culturais, etárias, linguísticas e raciais, onde informação e leitores circulam e se cruzam diariamente. A própria União Europeia, com os vários planos de ação *eEurope*, veio incentivar o desenvolvimento de serviços, aplicações e conteúdos em banda larga securizada à *Internet*.⁸⁴

Dados revelam que de 1998 para 1999, o número de utilizadores da *Internet* a nível mundial aumentou 55% face a anos anteriores. E o número de *hosts*⁸⁵ na *Internet*

⁸³ A conceção da *Internet* resultou de um projeto de investigação aplicada, cujo objetivo era ligar entre si vários computadores das forças armadas dos Estados Unidos da América, de modo a que a rede criada tivesse uma grande tolerância, dado o ambiente político em que viviam, “Guerra-Fria”. O grande objetivo deste projeto era garantir que, após uma possível guerra, e consequente destruição de muitos equipamentos de comunicação, fosse possível manter os restantes sistemas ativos, nomeadamente, que auxiliassem “as operações logísticas militares”, no envio e receção de mensagens, não obstante alguma deterioração das mesmas. No entanto, a fraca capacidade de comunicação das redes existentes veio forçar o desenvolvimento das mesmas. Assim foi desenvolvida uma nova tecnologia que se previa que funcionasse “em ligações de baixa velocidade (à escala atual) e com vários meios de comunicação, tais como, circuitos terrestres de vários tipos e ligações terrestres”. Estes circuitos e ligações serviram de base para a criação da tecnologia, que se tornou na solução central da conexão dos principais sistemas de informação e, também, na tecnologia de comunicação, que é a base da sociedade da informação. Veiga, Pedro; Dias, Marta, *A Governação da Internet*, JANUS.NET *e-journal of International Relations*, [Em linha] n.º1, Outono 2010, p.78. Disponível em http://janus.ual.pt/janus.net/pt/arquivo_pt/pt_vol1_n1_pdf/pt_vol1_n1.pdf, (consultado em 7.2.2014).

⁸⁴ Macedo, Miguel, “O Desafio da Cibersegurança”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, pp.35 e 36.

⁸⁵ Host - computador ligado à *Internet* onde um *website* é alojado para poder ser acedido pelos internautas. Computador central, também designado por servidor, onde se encontra gravado (alojado) o conjunto de programas e ficheiros de um ou mais sítios. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.1036.

aumentou para 46%, bem como o número de servidores *Web* que aumentou para 128%.⁸⁶

O desenvolvimento e a crescente utilização das tecnologias da informação e das telecomunicações vieram facilitar a *obtenção*, o *processamento* e *transmissão* de forma automática de grandes quantidades de dados e informação.⁸⁷ Desta forma havia, em 2003, aproximadamente 6,3 bilhões de habitantes no planeta e 500 milhões de dispositivos conectados à *Internet*.⁸⁸ Embora estes dados não demonstrem um grande avanço no número de dispositivos tecnológicos (já que o resultado demonstra que existia menos de um dispositivo por pessoa, mais concretamente, 0,08), a verdade é que ainda não tinha ocorrido o *boom* nos avanços e descobertas tecnológicas. Este só viria a ocorrer anos mais tarde⁸⁹.

Foi em 2010 que o avanço tecnológico tomou outros contornos, graças ao aparecimento dos *smartphones* e *tablets*, e aumentou o número de dispositivos conectados à *Internet* para 12, 5 bilhões, numa altura em que a população era de 6,8 bilhões de pessoas, fazendo com que pela primeira vez na história, o número de dispositivos existentes e conectados à rede fosse superior ao número de habitantes no planeta (estes valores dão uma média superior a 1, exatamente 1,84).

Além disso, estes valores podem ser maiores se tivermos em conta os valores exatos da população que já existia. Por exemplo, sabendo que em 2010 existiam 2 bilhões de pessoas que já usavam a *Internet*, o número de dispositivos conectados passa para 6,25 em vez dos 1,84 supra referidos.⁹⁰

A partir daí, assistimos ao exponencial crescimento das novas tecnologias e dos dispositivos conectados e interligados entre si à rede. A indústria tecnológica evoluiu rapidamente para o chamado *e-commerce*, e para o *e-business*,⁹¹ para os serviços de

⁸⁶ Raínha, Paula; Vaz, Sónia Queiróz, *Guia Jurídico da Internet em Portugal*, ed., CENTROATLANTICO.PT, Portugal, 2001, p.7.

⁸⁷ Gonçalves, Maria Eduarda, *O Direito da Informação*, Almedina, Coimbra, 1994, p.7.

⁸⁸ Evans, Dave, *A Internet das Coisas, como a próxima evolução da Internet está mudando tudo*, Cisco Internet Business Solutions Group (IBSG), abril 2011, p.3.

⁸⁹ Por exemplo a famosa marca Apple só revelou o primeiro *Iphone* em 2007, mais concretamente, no dia 9 de janeiro de 2007 na conferência *Macworld*.

⁹⁰ Evans, Dave, *A Internet das Coisas, como a próxima evolução da Internet está mudando tudo*, Cisco Internet Business Solutions Group (IBSG), abril 2011, p.3.

⁹¹ *E-business* – qualquer empreendimento baseado na *Internet*. Transações comerciais ou financeiras efetuadas entre entidades via *Internet*. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1034.

computadores nos telemóveis, indústrias, negócios globais e serviços de informação organizacional. Bem como para áreas tão distintas como:

- Medicina, onde são conhecidos casos em que pacientes ingerem dispositivos ligados à *Internet* para ajudar a determinar certas doenças e verificar a evolução dos pacientes a certos medicamentos experimentais;
- Biologia, em que micro sensores são colocados em plantas, animais e em recursos geológicos que ao serem conectados à *Internet* ajudam no estudo destas espécies;
- Educação, veja-se por exemplo a criação do *e-learning*, uma plataforma digital interativa de ensino à distância através da *Internet*;
- Espaço, por exemplo o caso do programa *Internet Routing in Space*, *IRIS* da *Cisco*.

É facto que a revolução ocorrida na sociedade atual, impulsionada pelo fenómeno informativo e comunicacional, adquiriu rapidamente um carácter transversal e global, em grande parte graças à sua própria natureza e à expansão tecnológica que lhe está associada: a digitalização, os dados, informação, conhecimentos, imagens, entre outros.

Esta revolução, criada pelos meios tecnológicos da informação e da comunicação, marcou não só as mais recentes mutações históricas e sociais, mas também o mundo do Direito. Foi responsável também por grandes mudanças no plano social, económico e até no plano político, tendo criado novas oportunidades para os seus utilizadores, no convívio dos utilizadores uns com os outros, nas atividades intelectuais e profissionais e na participação política dos cidadãos.

Estamos numa Era em que o envio e receção de informação se fazem de forma rápida e à escala mundial. Um acontecimento que outrora poderia demorar dias ou semanas a chegar a um dado local, é atualmente comunicável em direto e à escala global. Vejamos os seguintes exemplos: “ A notícia do assassinato do presidente norte-americano Abraham Lincoln, em 1865, levou 13 dias para cruzar o Atlântico e chegar à Europa. A queda da bolsa de valores de Hong Kong, na semana passada⁹², levou 13 segundos para cair como um raio sobre São Paulo e Tóquio, Nova Iorque e Tel Aviv, Buenos Aires e

⁹² Outubro/novembro 1997.

Frankfurt (...) ”⁹³. Recentemente, acontecimentos como discursos no Parlamento Europeu ou nos Estados Unidos da América são agora transmitidos em direto e em simultâneo para todos os países, numa linguagem que, também graças à *Internet* é universal, o inglês.

No entanto, a *Internet* trouxe também uma série de ameaças e desafios criados por um novo grupo de criminosos que viu nesta rede digital a possibilidade de cometer novos crimes de forma rápida, eficiente, com baixo risco e custo, capaz de provocar avultados prejuízos aos utilizadores e entidades. É fácil transmitir em direto atentados e crimes contra os Estados, por exemplo, os atentados de 11 de setembro, ou mais recentemente, as execuções praticadas pelos rebeldes do Estado Islâmico contra cidadãos de vários Estados. Isto deve-se à sua vasta natureza transnacional, e, por isso, dificilmente controlável, facilitando, deste modo, a sua utilização para fins ilícitos. Se antigamente ir do Japão a Portugal, por exemplo, implicava uma viagem de vários dias ou mesmo meses de navegação e seria quase impensável que uma frota japonesa viesse atacar Portugal, atualmente graças à *Internet* um operador de um computador que esteja em Tóquio consegue chegar com facilidade a um servidor que esteja em Lisboa ou Washington, tal como a qualquer outro servidor.⁹⁴

Hoje em dia causa muito mais danos a um país e à sua economia atacar servidores de serviços fundamentais para o país, como os sistemas de distribuição de energia, de controlo de telecomunicações, de sistemas financeiros e/ou bolsas de valores, do que realizar um ataque militar a esse país⁹⁵, por mais grave que seja.

Como observa Catarina Sarmento e Castro, o poder da *Internet* apresenta-se como “simultaneamente magnífico – do ponto de vista da celeridade, circulação de informação e possibilidades de tratamento de dados – e assustador - do ponto de vista da privacidade”.⁹⁶

⁹³ Rossi, Clóvis, *Do Conselho Editorial da Folha de São Paulo*, [Em linha], 2 de novembro de 1997. Disponível em http://www1.folha.uol.com.br/fsp/1997/11/02/caderno_especial/1.html (consultado em 23.11.2015).

⁹⁴ Cordeiro, Raul, “Ataques de DDOS, Medidas Preventivas”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p. 52.

⁹⁵ *Idem, Ibidem*.

⁹⁶ Castro, Catarina Sarmento e, “Proteção de Dados Pessoais na Internet”, in Gonçalves, Maria Eduarda, *Internet, Direito e Tribunais, Sub Judice, Justiça e Sociedade*, revista trimestral n.º35, Almedina, Setembro 2006, p.5.

A *Internet* global vive graças a infraestruturas, equipamentos, instalações, pessoas de vários países repartidas pelos vários Estados com as suas constituições e leis, polícias e órgãos políticos, mas partilhando um espaço comum, sem fronteiras, onde todos têm de conviver e onde todos têm direitos e deveres próprios, tal como acontece no mundo real. Mas como podemos nós circular num espaço livre e sem dono? Será um espaço onde podemos fazer tudo? E será um espaço onde uns ganham direitos e outros os perdem? Como podemos definir o limite das nossas atuações? E como pode o Direito atuar e legislar nesta nova era? São perguntas como estas que nos parecem ser cada vez mais comuns e mais pertinentes.

Como defendem alguns autores, a teoria e a prática da regulação desta rede digital passa pelo conceito de “governança” (*governance*), envolvendo uma mistura de tutela estatal, de cooperação internacional e de auto regulação. Como refere Maria Eduarda Gonçalves, “é presumivelmente esse o caminho certo para conciliar o respeito por valores e princípios consolidados das nossas ordens jurídicas e as complicadas exigências de regulação daquele espaço “virtual”.”⁹⁷

As próprias características da *Internet*: anónima, global e transnacional, fazem com que seja adversa à atuação do Direito, concebido para atuar numa sociedade assente em bens tangíveis. A globalidade da *Internet* contraria também o alcance territorial do Direito de base estadual, levantando o problema de aplicabilidade deste a um vasto campo sem fronteiras, agravado pela dificuldade de vigiar e controlar efetivamente o que nela se passa.⁹⁸

A verdade é que a *Internet* é uma tecnologia diferente de todas as que foram criadas até hoje, pois permite, pela primeira vez, a comunicação de muitos para muitos em tempo real e à escala global. Alguns autores mostram o poder desta tecnologia da comunicação, tal como define *Manuel Castells* a “Galáxia Internet”, comparando-a com a difusão da imprensa no Ocidente, tal como denominou *McLuhan* a “Galáxia Gutenberg”.⁹⁹

⁹⁷ Gonçalves, Maria Eduarda, “Internet, Direito e Tribunais”, *Sub Judice, Justiça e Sociedade*, revista trimestral n.º35, Almedina, Setembro 2006, p.5.

⁹⁸ *Idem, Ibidem.*

⁹⁹ Castells, Manuel, *A Galáxia Internet, Reflexões sobre Internet, Negócios e Sociedade*, p.15.

Concluindo, nesta Era Global a *Internet* converteu-se numa fonte de informação inesgotável que trouxe enormes benefícios da mesma forma que trouxe consequências nefastas para o campo social, científico e jurídico.

3.3.- A Cibersegurança

No mundo global em que hoje vivemos, um dos desafios que mais prementemente se colocam aos Estados é o da segurança. O terrorismo internacional e a criminalidade organizada aliados às novas tecnologias põem em causa a segurança e perturbam o funcionamento dos Estados e da sociedade.

É fácil de perceber que sendo um gigantesco oceano mundial de *bytes*, a *Internet* é um lugar muito público, sem dúvida, mas não imune ao Direito (como já referimos). Menos ainda, deve ser visto como um lugar onde uns percam todos os direitos e outros conquistem a possibilidade de praticar impunemente todos os abusos.¹⁰⁰ Assim, mais do que nunca faz sentido a definição e atuação do conceito de *Cibersegurança*.

Não existe um conceito fixo de *Cibersegurança*, mas através das estratégias publicadas por alguns países é possível retirar algumas ideias da sua definição. Por exemplo, a Alemanha considera *Cibersegurança* como o objetivo desejado da situação de segurança das Tecnologias de Informação em que o risco tem sido reduzido ao mínimo aceitável. No caso da Nova Zelândia a *Cibersegurança* é tratada como a prática de tornar as redes que constituem o *Ciberespaço* as mais seguras possível contra intrusões, mantendo a confidencialidade, disponibilidade e integridade de informação, deteção de intrusões e incidentes que ocorram, responder-lhes e recuperar deles. A Espanha, em literatura relevante, ainda não tem uma estratégia definida de *Cibersegurança*. No entanto, considera-a como a proteção dos componentes das infraestruturas dos sistemas de informação e comunicação entre ameaças cibernéticas.¹⁰¹

De um modo genérico podemos referir que a *Cibersegurança* consiste na segurança eficaz e efetiva de sistemas informáticos, de modo a garantir a segurança dos dados neles contidos, ou seja, bloqueando a leitura e o acesso indevido a estes, e também não permitindo a sua adulteração.¹⁰²

¹⁰⁰ Magalhães, José, *Homo S@piens, Cenas da Vida no Ciberespaço*, Quetzal Editores, Lisboa, 2001, p. 3.

¹⁰¹ Freire, Vicente, “Cibersegurança e Ciberdefesa: A Inevitabilidade de Adoção de uma Estratégia Nacional”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012,

¹⁰² Cordeiro, Raul, “Ataques de DDOS, Medidas Preventivas”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p. 48.

Podemos ainda definir *Cibersegurança* como todo o tipo de atividade, a título preventivo ou repressivo, destinado a diminuir os incidentes de segurança e a perceber a sua autoria.¹⁰³

Quando falamos em *Cibersegurança* é importante também definir claramente o que queremos proteger, pois só assim conseguimos garantir bons resultados.

De uma forma geral podemos afirmar que a função de um sistema de *Cibersegurança* eficaz será o de proteger informação vital, confidencial e importante, bem como de evitar a manipulação e alteração não autorizada dos parâmetros de sistemas vitais para a segurança e para a sobrevivência¹⁰⁴ da sociedade.

A *Cibersegurança* estende-se, por isso, a todos os atos relativos à proteção da confidencialidade, integridade e disponibilidade da informação no *Ciberespaço*, independentemente da sua classificação e fins para os quais tenha sido criada.¹⁰⁵ A confidencialidade é a garantia de que os sistemas reservados apenas são acedidos pelos utilizadores que tiverem autorização para tal, sendo a eventual informação não pública neles registada negada a terceiros e ao público em geral.¹⁰⁶ Quanto à integridade, significa que pode confiar-se nos sistemas e na informação por eles processada. Por fim, a disponibilidade e a fiabilidade traduzem a garantia de que os sistemas, as redes, os programas e os dados armazenados estão acessíveis a quem legitimamente queira usá-los.¹⁰⁷

A prossecução destes objetivos na defesa de uma sociedade da informação segura impõe que se encarem três tipos de ameaças diferentes: as atividades ilícitas nas redes de computadores, o crime informático convencional e, por último, a ameaça física.¹⁰⁸

A universalidade que o *Ciberespaço* promove, constitui desde logo um problema para a segurança dos utilizadores. A verdade é que hoje em dia só os digitalmente cultos se conseguem defender e não cair nos perigos que as redes informáticas comportam. O que

¹⁰³ Entrevista a Rogério Bravo (Inspetor-Chefe, Polícia Judiciária de Lisboa), no dia 18 de fevereiro de 2014.

¹⁰⁴ Cordeiro, Raul, “Ataques de DDOS, Medidas Preventivas”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p. 48.

¹⁰⁵ Macedo, Miguel, “O Desafio da Cibersegurança”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.35.

¹⁰⁶ Verdelho, Pedro, “Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º6, Julho-Dezembro 2005, p. 162.

¹⁰⁷ *Idem, Ibidem.*

¹⁰⁸ *Idem, Ibidem.*

desde logo, deixa crianças, idosos e portadores de deficiência em considerável desvantagem, dadas as suas características. Por exemplo, *Cookies*¹⁰⁹, *Spam*¹¹⁰, *Malware*¹¹¹ e tantos outros nomes como estes, desconhecidos para a maioria dos *internautas*¹¹², referem-se a meios que os *Hackers*, *Crackers* ou chamados *piratas informáticos*, têm para invadir a nossa privacidade, destruir a nossa propriedade ou apenas deixar a sua marca no mundo digital. Diariamente recebemos mensagens de correio eletrónico, avisos informáticos, atualizações de serviços ou apenas imagens ou vídeos de amigos e familiares que, embora desconhecendo tal facto, comportam vírus informáticos ou mensagens *spam*, à espera de serem ativados pelo *hacker* ou pirata *informático* que os criou. Em particular, o envio de mensagens *spam*, também conhecido como *spamming*, tem tomado proporções preocupantes, que têm criado a necessidade de o regulamentar. A Comissão Europeia estima que mais de metade do fluxo mundial de mensagens de correio eletrónico corresponda a mensagens não solicitadas (*spam*).¹¹³

Existem ainda os casos mais graves, como a pornografia e pornografia infantil, casos de prostituição, fraudes e tantos outros crimes (que mais à frente iremos abordar detalhadamente) que ocorrem cada vez mais no mundo digital.

A verdade é que o *Ciberespaço*, dadas as suas características: anónimo, global, transnacional, dificulta a implementação de medidas de segurança e, permite e/ou

¹⁰⁹ *Cookie*- pequeno arquivo que fica armazenado no computador do utilizador e guarda todas as informações importantes sobre a sua navegação. O *cookie* permite que um sítio tenha um histórico da navegação do utilizador e, assim, personalize o conteúdo do sítio de acordo com o perfil de cada *Internauta*, mas também pode ser perigoso, na medida em que o responsável pelo sítio pode ficar a conhecer determinadas preferências e informações de carácter pessoal do utilizador. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.1032.

¹¹⁰ *Spam*- Toda e qualquer correspondência eletrónica não solicitada e/ou não autorizada. Embora o artigo 22.º do Decreto-Lei n.º7/2004, de 7 de janeiro enfoque as mensagens não solicitadas no âmbito de marketing direto, o *spam* é muito mais amplo, abrangendo toda a forma de receção de mensagens não solicitadas. *Idem*, *Op. Cit.*, p.1042.

¹¹¹ *Malware*- *malicious software*.

¹¹² *Internauta*- pessoa que navega, visita vários sítios, na *Internet*. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1036.

¹¹³ O recebimento destas mensagens, além do incómodo pessoal, tem provocado elevados custos, que, estima-se, poderão causar às empresas de todo o mundo prejuízos de cerca de 20 mil milhões de dólares, por afetarem a sua produtividade e as obrigarem a reforçar as ferramentas de segurança nos seus equipamentos. Verdelho, Pedro, “Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º6, Julho – Dezembro 2005, p. 170.

facilita a prática de crimes por parte de utilizadores que no mundo real, provavelmente, não cometeriam tais atos.¹¹⁴

Nada preparou as pessoas ou os juristas para este mundo e este avanço tecnológico apanhou muitos de surpresa. A *Internet* mudou, quer para o bem quer para o mal, a forma como os juristas interagem com a informática e as redes eletrónicas.¹¹⁵ E é necessária uma resposta rápida e assertiva para travar os constantes avanços daqueles que usam estes novos meios de telecomunicações para a prática de atos ilícitos.

Contrariamente ao que acontece com outras áreas do Direito, na Informática não existe uma regulação global deste fenómeno que é a *Internet* e que abarque o mundo todo. Existem sim, normas globais, na grande maioria sob a forma de *Soft Law*, recomendando em vez de obrigar. Há também Direito Europeu. Há diversos diplomas nacionais sobre temas e subtemas parcelares (como por exemplo, o regime dos operadores de telecomunicações, acesso aos mercados, proteção de dados, direitos de autor, nomes de domínio), que fazem com que não haja uma harmonização legislativa.

Segundo a posição adotada por alguns autores, “multiplicidade de ameaças exige multiplicidade de meios de combate. (...)”¹¹⁶. Em nossa opinião, tal facto irá apenas criar mais dúvidas e dificuldade de implementação destas normas. Defendemos que o ideal seria a adoção, por parte de todos os Estados (sem exceção), de uma única legislação, com carácter global, capaz de combater estes ataques, evitar a propagação de novas ameaças e reforçar as cooperações entre os Estados e entidades.

A *Agencia Europeia de Segurança das Redes e da Informação* (ENISA), criada em 2004, traduz exatamente a valorização da ciberameaça, visando assegurar um elevado e efetivo nível de segurança informática na União Europeia, através do desenvolvimento de estratégias de *cibersegurança* que espelham a prioridade de todos os Estados Membros da União, no sentido de uma política concertada nestes domínio.¹¹⁷ Recentemente, foi também proposta a criação de uma “Equipa de Resposta de

¹¹⁴ UNODC, United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, February 2013, United Nation, New York, 2013, p. 8.

¹¹⁵ Magalhães, José, *Homo S@piens, Cenas da Vida no Ciberespaço*, Quetzal Editores, Lisboa, 2001, p. 292.

¹¹⁶ *Idem*, *Op. Cit.*, p. 102.

¹¹⁷ Macedo, Miguel, “O Desafio da Cibersegurança”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.36.

Emergência Informática” no quadro da União Europeia, tendo em vista a proteção do sistema contra ciberataques.

Também o Conselho da Europa expressou a sua preocupação face à *Cibersegurança*, através da Convenção sobre Cibercrime, de 2001, onde se instou com os Estados Membros para adotar um conjunto de medidas legislativas com vista a impedir o acesso e utilização não autorizada de dados informáticos, medidas de prevenção e controlo da pornografia infantil na *internet*, de defesa da propriedade intelectual, entre outras.¹¹⁸

A verdade é que a velocidade com que estas mudanças tecnológicas ocorrem, aliada à globalidade deste fenómeno, não têm permitido ao mundo académico e ao legislador acompanhar as várias ameaças que vão surgindo, aumentando assim as lacunas jurídicas quanto a este tema.

Vários países assumem hoje a *Cibersegurança* como missão prioritária. Para tal, aprovam documentos estratégicos que não só traçam o quadro de ameaças em curso como definem os meios e os bens/instalações a proteger.¹¹⁹

Tem sido visto como modelo de abordagem o conceito de segurança dos Estados Unidos da América que, no seio do *US Department of Homeland Security*, criaram uma importante unidade, especificamente direcionada para a segurança informática, a *National Cyber Security Division – NCSD*.¹²⁰ Esta unidade dispõe de um quadro de 60 pessoas que, coordenando a sua ação com o sector privado, identificam e analisam os riscos e vulnerabilidades dos sistemas informáticos públicos, como forma de prever eventuais ataques. Assim, a NCSD produz informação que faz chegar aos serviços públicos, ao sector privado e aos consumidores em geral, tendo em vista prevenir ameaças e incidentes informáticos e, se ocorrerem, responder-lhes de imediato.¹²¹

Sendo este um departamento público necessita de envolver na sua atividade o sector privado. Para o efeito, criou o *United States – Computer Emergency Readiness Team*

¹¹⁸ Macedo, Miguel, “O Desafio da Cibersegurança”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.36.

¹¹⁹ Pereira, Júlio, “Cibersegurança, O Papel do Sistema de Informações da República Portuguesa”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.43.

¹²⁰ www.dhs.gov Este serviço governamental é o pilar essencial da Estratégia Nacional para um Ciberespaço Seguro, fixada pela Administração Bush. Verdelho, Pedro, “Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º 6, Julho-Dezembro 2005, p. 174.

¹²¹ *Idem, Ibidem.*

(US-CERT¹²²), composto por equipas de análise e de resposta a incidentes, por representantes de empresas privadas produtoras de sistemas de segurança, por representantes dos fornecedores de acesso *Internet* (ISP's¹²³) e por agentes operacionais da área da segurança. Esta estrutura pôs em funcionamento o National Cyber Alert System, um sistema de identificação, análise e valoração de vulnerabilidades e ameaças às redes e sistemas. Recolhendo informação de todos os utilizadores, este sistema dirige-se também a todos os internautas, a quem pretende fornecer dados e ferramentas essenciais para agir no Ciberespaço.¹²⁴

O Presidente Barack Obama identificou desde muito cedo a *Cibersegurança* como prioridade da sua Administração, começando por atualizar o “cyber assessment” norte-americano para de seguida aperfeiçoar as políticas e as estruturas de *Cibersegurança*.¹²⁵

No Reino Unido, o tema *Cibersegurança* é igualmente prioritário, tendo os riscos do *Ciberespaço* sido apontados como ameaça premente.

Em 25 de outubro de 2011, as autoridades britânicas publicaram o “Cybersecurity Strategy”, da responsabilidade do Gabinete do Primeiro Ministro, que alocou £ 650 milhões para um programa quadrienal denominado “National Cyber Security Programme”. Esta estratégia realça a centralidade das “intelligence agencies” e do Ministério da Defesa na compreensão do fenómeno e redução das vulnerabilidades e ameaças.¹²⁶

¹²² www.us-cert.gov

¹²³ ISP (*Internet Service Provider*) - Provedor de acesso à *Internet*. Entidade que faculta o acesso dos utilizadores à *Internet*. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1037. Os ISP's são prestadores intermediários de serviços em rede. Estes permitem o acesso à *Internet* e garantem a comunicação entre o computador do utilizador e o computador onde a página (*website*) se encontra alojada. Ao conjunto de computadores e equipamentos que permite que um *sítio* esteja disponível na *Internet* chama-se *servidor*. Existem fornecedores de serviço de alojamento de página gratuitos e os que alojam um *sítio* mediante contrapartida monetária. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 509.

¹²⁴ Verdelho, Pedro, “Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º 6, Julho-Dezembro 2005, pp. 174 e 175.

¹²⁵ Pereira, Júlio, “Cibersegurança, O Papel do Sistema de Informações da República Portuguesa”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.43.

¹²⁶ *Idem, Ibidem.*

Por fim, destacamos o modelo de *Cibersegurança* mais próximo de nós, Espanha, cuja estratégia de segurança destaca a questão da “Ciberseguridad” como eixo fundamental da sociedade e do sistema económico espanhol e não como mero aspeto técnico.¹²⁷

No âmbito nacional, a *Cibersegurança* encontra-se numa fase muito inicial, apesar de algumas conferências e palestras sobre o assunto, o caminho a percorrer nesta área ainda é longo. Na avaliação da ENISA publicada em maio de 2011, Portugal encontrava-se na fase inicial de definição de uma política nacional de segurança da informação.¹²⁸ Por exemplo, o domínio DNS de topo nacional (pt.) foi “atacado” no início de 2012, a partir de servidores da China e da Rússia, com vinte mil pedidos de acesso por segundo.¹²⁹

Não existe ainda nenhuma entidade responsável pela *Cibersegurança* em Portugal, apesar do papel atribuído ao Gabinete Nacional de Segurança (GNS), à UMIC – Agência para a Sociedade do Conhecimento, bem como à Fundação para a Computação Científica Nacional (FCCN) que está a desenvolver um ótimo trabalho nas áreas da investigação e do ensino.¹³⁰ E encontramos ainda entidades que regulam problemas ligados as bases de dados, como é o caso da Comissão Nacional de Proteção de Dados Pessoais (CNPDP¹³¹).

No trabalho desenvolvido nesta área no seio da União Europeia, concluído em 2010 com a aprovação da Estratégia de Segurança Interna da União Europeia, a *Cibercriminalidade* é reconhecida como uma ameaça à escala mundial, técnica, transfronteiriça e anónima para os sistemas de informação.¹³²

Quando se fala em *Cibercriminalidade*, nenhuma entidade ou organização está a salvo. Por exemplo, só em 2012 a NATO foi vítima de 2.500 significantes ciberataques. E segundo especialistas em *Cibersegurança*, estes números só tendem a aumentar.¹³³

¹²⁷ Pereira, Júlio, “Cibersegurança, O Papel do Sistema de Informações da República Portuguesa”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.43.

¹²⁸ *Idem*, *Op. Cit.*, p.38.

¹²⁹ *Idem*, *Ibidem*.

¹³⁰ *Idem*, *Op. Cit.*, p. 40.

¹³¹ A Comissão Nacional de Proteção de Dados Pessoais (CNPDP) é uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República (como dispõe o artigo 21.º n.º1 da Lei n.º67/98 de 26 de outubro - que diz respeito à Lei da Proteção de Dados Pessoais e à Livre Circulação desses dados). Esta tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais (tal como dispõe o artigo 22.º n.º 1 da mesma lei).

¹³² Macedo, Miguel, “O Desafio da Cibersegurança”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, pp.36 e 37.

¹³³ Gabinete Nacional de Segurança, *Cyber Newsletter*, n.º37/2014, 10 de outubro de 2014, [Em linha]. Disponível em <http://www.gns.gov.pt/new-ciberseguranca/newsletter.aspx>, p.6.

Através deste exemplo é fácil de perceber como a questão da *Cibersegurança* se tornou num problema global que atinge não só utilizadores comuns como entidades internacionais.

A problemática da *Cibersegurança* abarca uma série de questões importantes que devem ser atendidas quanto a este tema. Por exemplo, qual o limite do controlo de conteúdo permitido pela *Internet*? Como se define o campo da privacidade? E qual o lugar reservado à privacidade pessoal, ao anonimato, à cifragem de mensagens? Qual o papel da *Cibersegurança* e que força coativa tem esta?

A verdade é que os avanços tecnológicos têm influenciado várias áreas do direito, entre as quais destacamos a privacidade. Assim, entendemos que quanto maior forem os avanços tecnológicos, maior será a exposição e os riscos a que os cidadãos estarão expostos. Como revela Luís Filipe Antunes “os cidadãos estão a pagar com a sua privacidade supostos serviços gratuitos na *Internet*”. E este é um fenómeno que tende a aumentar; segundo o mesmo autor, no futuro a privacidade será uma palavra pouco usada quando relacionada com os meios tecnológicos: “O que me choca é que na próxima geração haverá empresas que têm disponível um conjunto de informação sobre o comportamento das pessoas *online* desde crianças”.¹³⁴

A utilização da *Internet* e dos serviços por estas disponíveis obriga a que os operadores de telecomunicações, os fornecedores de acesso à *Internet*, os fornecedores de serviços da *Internet* e os titulares de sítios *web*, recolham e tratem dados pessoais do utilizador/assinante.

Nos termos da Lei n.º67/98, de 26 de outubro, são Dados Pessoais quaisquer informações, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativas a uma pessoa singular identificada ou identificável, que será o titular dos dados. A Lei considera que é identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social. Excluem-se do âmbito de aplicação da Lei os tratamentos efetuados por pessoas singulares no exercício de atividades exclusivamente pessoais ou

¹³⁴ Luís Filipe Antunes, do Centro de Competências em Cibersegurança e Privacidade da Universidade do Porto. *Jornal Metro*, 5 de junho 2014, p. 15.

domésticas, por exemplo: as listas pessoais de endereços, de compras, de presentes, etc.¹³⁵

Assim, para além dos comuns dados, como o nome, morada, telefone são também considerados dados pessoais, os dados tratados para efeito do envio de uma comunicação através de uma rede de comunicações eletrónicas, designadamente, a sua duração o tempo ou o volume da comunicação, o protocolo utilizado, a localização do equipamento terminal do expedidor ou do destinatário, a rede de onde provém ou onde termina a comunicação, o início e o fim da duração da ligação, o formato em que a comunicação é enviada pela rede, em suma, todos os dados relativos ao tráfego¹³⁶, mas também o *IP* do computador, as sequências de “cliques” (*clickstreams*) estabelecidas durante a navegação na *Internet*, bem como os dados de localização.¹³⁷

Foram já adotadas algumas medidas relativas à *Cibersegurança* para garantir direitos fundamentais dos cidadãos. No âmbito da União Europeia, foi criado um sistema de consentimento prévio (*Opt-in*), no que diz respeito às mensagens *spam*. A Diretiva nº 2002/58/CE relativa à privacidade e às comunidades eletrónicas, transposta para o ordenamento jurídico português pelo Decreto-lei nº7/2004, estabelece como padrão a proibição do envio de mensagens comerciais não solicitadas por correio eletrónico ou outros sistemas de mensagens eletrónicas, como é o caso das mensagens escritas e de *Multimédia Messaging Service* sem o consentimento prévio do assinante desses serviços de comunicações eletrónicas, tal como dispõe o número 1 do artigo 13.º da Diretiva. O sistema *Opt-in* consiste assim no envio de mensagens, através de uma autorização ou de uma subscrição num *website* ou *banner*, por exemplo: como acontece no caso das *newsletters*¹³⁸. A partir do momento da assinatura, o endereço eletrónico do assinante

¹³⁵ Castro, Catarina Sarmento e, “Proteção de Dados Pessoais na Internet”, in Gonçalves, Maria Eduarda, *Internet, Direito e Tribunais*, Sub Judice, Justiça e Sociedade, revista trimestral n.º35, Almedina, Setembro 2006, p.14.

¹³⁶ Dados de tráfego – são “os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo de serviço subjacente”. Definição presente na alínea c), do artigo 2.º da Lei n.º109/2009, de 15 de setembro.

¹³⁷ Castro, Catarina Sarmento e, “Proteção de Dados Pessoais na Internet”, in Gonçalves, Maria Eduarda, *Internet, Direito e Tribunais*, Sub Judice, Justiça e Sociedade, revista trimestral n.º35, Almedina, Setembro 2006, p.14.

¹³⁸ *Newsletters* (ou *e-letter*) - notícias ou comunicações eletrónicas, por exemplo, boletins de atualização de *websites*, boletins periódicos, etc. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1039.

passa a fazer parte de uma lista de contactos, também chamada de *mailing list*¹³⁹ ou de uma base de dados (lista *Opt-in*) que, todavia pode ser removido a qualquer momento, por declaração ou solicitação do utilizador.¹⁴⁰

Este sistema traz grandes vantagens, já que garante a proteção dos dados pessoais dos utilizadores; assegura que estes só recebem *spam* ou outras mensagens indesejáveis, caso assim o desejem; valoriza a relação entre o anunciante e o destinatário; promove a certeza jurídica para os prestadores de serviços na sociedade da informação e incrementa um clima de confiança no comércio eletrónico e na sociedade da informação.¹⁴¹

Ainda no âmbito da União Europeia, temos como outro bom exemplo os *Princípios Chave da Agenda de Túnis* (2005), onde podemos salientar pela sua importância “a aposta num modelo *multi-stakeholder*¹⁴² para o desenvolvimento da Sociedade da Informação, pelo reconhecimento do papel crucial do sector privado na disponibilização das infraestruturas, no papel dos *media* numa sociedade baseada no conhecimento, na necessidade de uma maior cooperação entre entidades públicas e privadas para defrontar o facto de os problemas de segurança serem globais e críticos, para que os utilizadores tenham confiança no uso da *Internet* e nas tecnologias da informação”¹⁴³.

Os seguintes pontos são alguns dos vários exemplos que constam da referida Agenda de Túnis, que ajudam no desenvolvimento e segurança desta nova era:

- “O acesso à informação e ao conhecimento;
- A capacitação das pessoas para a sociedade da informação;
- A criação de ambientes seguros e confiáveis;
- A protecção dos direitos de propriedade intelectual;
- A necessidade de investir na investigação e desenvolvimento;

¹³⁹ *Mailing list* – “lista de distribuição de mensagens de correio electrónico. Lista de endereços de correio electrónico, cujos proprietários subscreveram, para trocarem mensagens de e-mail ou para receberem informações ou notificações de actualizações do sítio”. *Idem, Op. Cit.*, p. 1038.

¹⁴⁰ *Idem, Op. Cit.*, p. 915.

¹⁴¹ *Idem, Op. Cit.*, p. 916.

¹⁴² Modelo *Multi-stakeholder*, este modelo preconiza uma colaboração, intervenção e partilha de responsabilidades entre governos, o setor privado nas suas várias dimensões, a sociedade civil onde as *Organizações Não Governamentais* têm um papel chave e os cidadãos. Veiga, Pedro; Dias, Marta, *A Governação da Internet*, [Em linha], *JANUS.NET e-journal of International Relations*, nº1, Outono, 2010, p.81. Disponível em http://janus.ual.pt/janus.net/pt/arquivo_pt/pt_vol1_n1_pdf/pt_vol1_n1.pdf, (consultado em 8.4.2014).

¹⁴³ *Idem, Ibidem.*

- A possibilidade de uso das *TIC* em novos sectores como o da saúde mesmo praticada à distância, a preservação da multi-culturalidade da *Internet*, o seu uso para a preservação do património cultural.”¹⁴⁴

Depois de 2005, a agenda de Túnis realiza todos os anos um encontro, “o *Internet Governance Forum*”. Até agora, estas reuniões foram realizadas nos seguintes países: “Atenas (2006), Rio de Janeiro (2007), Hiderabad (2008), Sharm-el-Sheik (2009) e Vilnius (2010)”. Mais recentemente foram realizados em Nairobi (2011), em Baku (2012), em Bali (2013) e este ano será realizado em Istambul (nos dias 2-5 de setembro de 2014).

Dos trabalhos e reflexões já realizados importa destacar a área do *Cibercrime*, da privacidade, da liberdade de expressão, bem como dos recursos mais críticos da *Internet*.¹⁴⁵

Já no âmbito nacional, destacamos o memorando de entendimento celebrado em 3 de maio de 2011 entre o Gabinete Nacional de Segurança e a NATO, no âmbito da Ciberdefesa¹⁴⁶.

Destaque também para a Resolução do Conselho de Ministros (RCM n.º12/2012), de 7 de fevereiro de 2012, em que o Governo aprovou um Plano de Racionalização das Tecnologias de Informação e Comunicação na Administração Pública, que estabeleceu como 4.ª Medida – a Consolidação de uma Estratégia Nacional de Segurança da Informação (ENSI). Esta estratégia nacional compreende ainda, entre outras medidas, a criação, a instalação e a operacionalização de um Centro Nacional de Cibersegurança.¹⁴⁷

Também existem normas que regulam situações emergentes deste novo paradigma tecnológico. É o caso do aproveitamento ilegítimo de identidades, ou dos nomes de

¹⁴⁴ Veiga, Pedro; Dias, Marta, *A Governação da Internet*, [Em linha], *JANUS.NET e-journal of International Relations*, n.º1, Outono, 2010, pp. 81 e 82. Disponível em http://janus.ual.pt/janus.net/pt/arquivo_pt/pt_vol1_n1_pdf/pt_vol1_n1.pdf, (consultado em 8.4.2014).

¹⁴⁵ *Idem*, *Op. Cit.*, p.82.

¹⁴⁶ Como revela Miguel Macedo, “as conversações em torno do memorando denotaram a necessidade de o país criar com brevidade um grupo de trabalho destinado a desenvolver um Centro Nacional de Cibersegurança (CNC). Esse centro deverá assumir as responsabilidades inerentes a uma alta autoridade para a Ciberdefesa, e terá um relacionamento com a Nato e outras entidades internacionais. De entre os objetivos deste Centro destacamos o desenvolvimento de trabalho conjunto e concertado, a partilha de informações relativas a vulnerabilidades de sistemas, tipos de ataques e perfis de atacantes, melhoria dos conhecimentos, das capacidades e tomada de decisão atempada, a fim de garantir vantagem no ciberespaço. Pereira, Júlio, “Cibersegurança, O Papel do Sistema de Informações da República Portuguesa”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.40.

¹⁴⁷ *Idem*, *Ibidem*.

figuras públicas para a criação de domínios, como prevê o artigo 193.º do Código Penal, ou o caso da propagação de vírus informáticos ou de programas (*software*) malicioso ou de programas (*software*) de espionagem, *spyware*¹⁴⁸, só para nomear alguns exemplos.

As ações da polícia nacional em cooperação com a *Europol* são já visíveis e têm-se feito sentir pela sua presença nos meios tecnológicos, mais concretamente, nas salas de *chat* ou sítios de encontros, por serem um dos meios de atuação mais utilizados para o aliciamento de pessoas. Estas vigilâncias têm como objetivo tentar perceber quem frequenta estes espaços tecnológicos, como forma de passatempo ou divertimento, e quem os frequenta com motivos criminosos, de má-fé, com o intuito de aliciar crianças, jovens e adultos (na maioria mulheres) para as redes de tráfico de prostituição, pornografia ou tráfico de órgãos humanos.

Quanto ao tema *Cibersegurança*, defendemos que a proteção dos direitos fundamentais na *Internet* passa primeiro pela sensibilização do utilizador, sendo fundamental assegurar a partilha e distribuição de informação sobre ciberameaças. Pais, tutores, professores, educadores e órgãos de segurança pública devem cooperar e trabalhar lado a lado no combate a este tipo de ameaças informáticas, através da divulgação dos perigos que a *Internet* e todo o mundo digital comportam. Estas informações devem ser transmitidas desde as camadas mais jovens até aos próprios adultos. Não obstante, defendemos que as crianças, mulheres, idosos e portadores de deficiência, dadas as suas características, deverão ser objeto de medidas especiais de salvaguarda, uma vez que são mais vulneráveis a tais ameaças. Para tal, consideramos ser importante organizar palestras de sensibilização, conferências nacionais e internacionais sobre este tema e que informem e protejam os cidadãos, através de normas legislativas.

Por outro lado, é também importante, por exemplo, a mobilização dos fabricantes de *software*, que deverão, no desenvolvimento dos seus produtos, ter preocupações quanto à segurança dos mesmos. No fundo, trata-se de implementar a *literacia informática* dos utilizadores finais de computadores e redes.¹⁴⁹

¹⁴⁸ *Spyware*- são programas espiões que enviam informações do computador do utilizador. Inclusive, tudo o que for digitado no teclado do próprio computador, pode ser monitorizado pelos *spywares*, alguns dos quais têm um mecanismo que faz imediata conexão com o respetivo servidor logo que o internauta fique *online*. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.519.

¹⁴⁹ Verdelho, Pedro, “Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º 6, Julho-Dezembro 2005, p. 166.

Defendemos também a criação de um sítio eletrónico que não só reforce os perigos que se escondem na *Internet* e quais os meios de defesa contra estes, mas também, que ligue e seja um ponto de cooperação entre as várias entidades que lidam com estes casos, como é o caso da Polícia Judiciária, do Ministério Público e do Gabinete de Combate ao Cibercrime.

Quanto ao conteúdo das páginas informáticas, seria importante desenvolver sistemas de filtragem e de classificação de conteúdos, de modo a facilitar a identificação de conteúdos ilegais ou impróprios para menores, através de um sistema que possa avaliar os conteúdos dos sítios¹⁵⁰.

De igual forma é importante criar sistemas de filtragem ou bloqueio de informação, que permitam ao utilizador selecionar o conteúdo que pretenda receber. Embora existam já alguns *sítios* eletrónicos que dispõem desta função, a sua atuação é em pequena escala. Por exemplo: como acontece nos sítios que permitem o controlo parental e assim bloqueiam certos conteúdos impróprios para crianças, sítios protegidos por palavra passe ou, face ao conteúdo que apresentam, conteúdo para maiores de idade, requerem a utilização de um cartão de crédito.

Para combater este crescente problema, o conhecido sítio eletrónico de vídeos da empresa *Google*, o *Youtube*, está a desenvolver uma nova versão do mesmo sítio para crianças. Este irá apresentar mais filtros para vídeos e comentários agressivos. Desta forma, serão criados conteúdos especificamente para crianças, livres de vídeos e comentários inapropriados. Aliado a este novo avanço, a empresa *Youtube* criou ainda o *Youtube EDU*, uma variante educacional desenhada especificamente para as escolas.¹⁵¹

Neste contexto, é necessário desenvolver o entendimento e a troca de informação entre os sectores público e privado, pois só assim será possível responder rapidamente aos ataques informáticos, minimizar os seus efeitos e manter as redes globais a funcionar.

Esta perspetiva tem sido bem acolhida pelo sector empresarial internacional. Exemplo disso foi a criação do *GBDe* (*Global Business Dialogue on Electronic Commerce*), uma

¹⁵⁰ Em termos estatísticos, os números mostram que os conteúdos pornográficos ou eróticos, não infantis, são mais de metade dos conteúdos existentes na *Internet* de acesso livre ou pago, sendo facilmente visitados pelas crianças e jovens.

¹⁵¹ “YouTube para crianças”, *Jornal Metro*, 19 de março 2014, p. 7.

iniciativa mundial de líderes empresariais, com o intuito de apoiar a criação de uma rede de políticas de desenvolvimento da economia *online*.¹⁵²

Têm sido também anunciados programas de cooperação entre empresas produtoras de *software* e entidades públicas. Como exemplo desta colaboração, destacamos o programa de cooperação entre a Microsoft¹⁵³ e a Interpol, anunciado em finais de 2003, que pretendia a realização de ações de formação de agentes policiais na área da pedofilia e da pornografia infantil nas redes informáticas.¹⁵⁴

Por fim, devem ser assegurados regimes especiais de acesso para determinados tipos de cidadãos, com necessidades especiais, e de organizações, designadamente as organizações culturais, as escolas (desde o ensino primário até ao ensino superior), bem como instituições que desempenhem um papel ativo junto das camadas especialmente relevantes na expansão de novas ferramentas de comunicação. Da mesma forma, é preciso criar e inculcar nos utilizadores novas formas de uso da *Internet* e da informação que esta dispõe, mostrando não só os perigos que esta comporta, mas também as vantagens que esta pode oferecer.

Concluindo: a definição de uma política de *Cibersegurança* deverá estruturar-se em quatro pontos-chave de atuação:

1. Garantir a segurança e confidencialidade da infraestrutura de tecnologias de informação e da comunicação;
2. Definir estratégias políticas de segurança, assentes na análise e gestão de riscos;
3. Alinhamento e integração operacional das organizações no equilíbrio necessário entre o direito à privacidade e a necessidade de acesso à informação por parte das Forças e Serviços de Segurança em nome da defesa da segurança;

¹⁵² Verdelho, Pedro, “Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º 6, Julho-Dezembro 2005, p. 166.

¹⁵³ A *Microsoft*, por ser o mais importante produtor mundial de *software*, é regularmente vítima de muitos ataques informáticos. Segundo Diário Digital de 25 de novembro de 2003, a *Microsoft* revelou publicamente que sofria cerca de 100 mil ataques informáticos por mês, na sua rede interna, à qual estarão ligados cerca de 300 mil computadores em todo o mundo. De acordo com a mesma fonte, nestes computadores seriam recebidos por mês, por correio eletrónico, 125 mil mensagens infetadas com vírus. *Idem*, *Op. Cit.*, pp.167 e 168.

¹⁵⁴ *Idem*, *Op. Cit.*, p. 167.

4. E, por fim, a criação de uma relação de parceria entre o sector público e o sector privado em moldes aceites por todos, a funcionar em rede e de forma desburocratizada.¹⁵⁵

A implementação destas estratégias poderá beneficiar da criação de um Centro Nacional de Cibersegurança, como apontam alguns autores, entre os quais Miguel Macedo¹⁵⁶, que colabore e coopere com as entidades de cada Estado, pela melhoria das condições operacionais do Sistema de Certificação Eletrónica do Estado (SCEE), e que fundamentalmente, defenda os interesses e garantias dos cidadãos.

¹⁵⁵ Macedo, Miguel, “O Desafio da Cibersegurança”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.36.

¹⁵⁶ *Idem*, *Op. Cit.*, p.37.

3.4.- Os desafios e ameaças do Ciberespaço

Como temos vindo a analisar, a *Internet* e as novas tecnologias, mudaram por completo a forma como os agentes pensam ou atuam, o que se tornou num grande problema para o Direito, obrigando-o a evoluir e a acompanhar esta mudança tecnológica.

O Direito, sentindo-se ultrapassado pelo avanço tecnológico, tem tentado acompanhar estas mudanças. No entanto, a *Internet* trouxe consigo importantes fatores de “desestabilização jurídica”¹⁵⁷, como o aspeto transnacional de uma rede que não conhece fronteiras nacionais, e a desmaterialização da informação.¹⁵⁸

Qualquer sistema normativo assenta, entre outros, em dois princípios fundamentais: o Princípio da Territorialidade e o Princípio da Soberania.

O primeiro princípio traduz-se nas fronteiras territoriais (geográficas) que delimitam áreas, dentro das quais diversos conjuntos de normas são aplicáveis. O segundo princípio tem a ver com a necessidade de existência de uma autoridade investida de poderes para fiscalizar a aplicação de normas e, em caso de desrespeito, sancionar a infração.¹⁵⁹

No entanto, quando analisamos estes dois princípios e os tentamos relacionar com o *Ciberespaço* (com as suas características e com o modo como funciona), vemos que são incompatíveis e como é difícil para o Direito legislar sobre esta matéria.

O conceito de “soberania nacional” dos Estados depara-se com sérias dificuldades quando encontra uma rede planetária como a *Internet*, já que esta é composta por dados, fluxos monetários e vários documentos que circulam através das redes sem controlo nem fronteiras geográficas. O volume de comunicações eletrónicas que cruzam as fronteiras territoriais é demasiado grande em relação aos meios de que dispõem as autoridades governamentais. Perante o domínio digital e as novas realidades do *Ciberespaço*, os Estados sentem-se inoperantes na aplicação do seu Direito interno.¹⁶⁰ E este é um dos grandes problemas que o Direito enfrenta no *Ciberespaço*.

¹⁵⁷ Bauche, Gilles, *Tout savoir sur Internet*, Arléa, 1996, pp.90 e ss.

¹⁵⁸ Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, p.320.

¹⁵⁹ *Idem, Ibidem.*

¹⁶⁰ *Idem, Op. Cit.*, p.322.

Esta dificuldade, da aplicação efetiva das leis nacionais, é ainda mais notória quando percebemos a rapidez com que tudo funciona no *Ciberespaço*. Por exemplo, um servidor *web* que enfrente uma certa lei penal poderá ser deslocado pelo seu criador, em poucos minutos, para outro ponto do planeta ligado à rede, nomeadamente, para “paraísos cibernéticos”¹⁶¹, isto é, para países cuja lei seja mais benévola ou permissiva quanto a estes casos.¹⁶²

A *Internet* proporciona fluxos intermináveis de informação no *Ciberespaço*, à medida que os sistemas digitais de alta capacidade ligam todos os pontos do mundo. Esta revolução da tecnologia está a criar um novo paradigma nas vidas de cada um de nós.

Em certas mãos as novas tecnologias são um bom aliado, mas podem com a mesma facilidade ser usadas de má-fé e servir de base para a prática de crimes graves. A verdade é que as novas tecnologias e esta era digital oferecem muitas vantagens. Mas oferecem de igual forma, um vasto mundo de desafios e problemas ainda por explorar.

A *Internet* oferece oportunidades e desafios em vários temas críticos, entre os quais podemos citar os relacionados com a jurisdição e a legalidade dos documentos eletrónicos, da assinatura eletrónica e da *Cibercriminalidade*. Mas é cada vez mais difícil criar meios de defesa seguros e manter o ritmo a par das novas tecnologias, uma vez que tendem a aumentar os avanços tecnológicos presentes nestas novas áreas e no *Ciberespaço*. Do mesmo modo, as técnicas utilizadas pelos agentes são cada vez mais avançadas, fazendo com que os órgãos de justiça estejam sempre um passo atrás nesta nova demanda jurídica. Assim, atualmente existe uma grande preocupação sob o ponto de vista social e sobre os perigos que enfrenta a nossa sociedade no *Ciberespaço*.

É neste ambiente de rede que se integram as infraestruturas críticas nacionais, como as telecomunicações, a banca, os transportes, energia, água, saúde, serviços de emergência,

¹⁶¹ Bauche, Gilles, *Tout savoir sur Internet*, Arléa, 1996, pp.91.

¹⁶² Por exemplo, uma eventual decisão judicial (cautelar ou repressiva) de proibição de certos conteúdos em determinados sítios, seria inoperante caso os sítios com material proibido fossem (re) colocados noutro país onde não vigorasse essa proibição (*maxime*, quanto ao direito de autor, países não aderentes à Convenção de Berna, que tutela o Direito de Autor no plano internacional). Essas situações de evasão ou contorno da lei de um determinado Estado, poderão, no máximo, ser sancionadas por violação da ordem pública internacional, ou por fraude à lei (sobre este ponto ver Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, p.324, nota 812), desde que seja cometida por um nacional cuja lei é contornada (ou uma pessoa coletiva com sede efetiva nesse Estado). Piette-Coudol Thierry/ Bertrand André, *Internet et la loi*, Dalloz, Collection Dalloz Service, Paris, 1997, p.61. Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998, p.324, *apud.*, Dufour, Arnaud, *Internet*, 4ª ed., P.U.F., col. “Que Sais-Je?”, n. °3073, Paris, 1997, p.111.

entre tantos outros. Por isso, é importante lembrar que sendo um modelo de interdependências, estas infraestruturas, já de si críticas, se tornam ainda mais críticas.

É importante lembrar que a *Internet* é a base na qual assentam os sistemas de comunicação entre Governos, Forças Armadas, Serviços de Informações e Segurança. Assim, face ao espectro da ameaça, as infraestruturas críticas são um alvo potencial de ataques que, pela sua natureza disruptiva, poderão colocar em risco o normal funcionamento de um país e os interesses nacionais.¹⁶³

É este o ponto fundamental que torna indispensável a adoção, por parte dos Estados, de Estratégias de Informação devidamente enquadradas nas estratégias nacionais de segurança e defesa, que devem contemplar linhas de ação, visando garantir a liberdade de ação no ambiente de informação e fazer face aos desafios colocados pela utilização segura do *Ciberespaço*, com destaque para as relacionadas com a proteção das infraestruturas de informação críticas e com as estruturas e capacidades necessárias nos domínios da *Cibersegurança* e da *Ciberdefesa*.¹⁶⁴

Sem dúvida que outro dos vários desafios do direito no *Ciberespaço* será tentar acompanhar o contínuo desenvolvimento tecnológico. E, de igual forma, tentar acompanhar a crescente informação que surge e circula no *Ciberespaço*.

Os problemas que nos são apresentados são dos mais variados, desde os perigos do conteúdo de alguns sítios eletrónicos, até à própria linguagem tecnológica (na grande maioria escrita em inglês) que pode induzir em erro muitos dos internautas.

Outro dos desafios do *Ciberespaço* são os dados pessoais. Com a *Internet* surgem novas categorias de dados pessoais, como por exemplo o endereço de *IP*. Por outro lado, a própria navegação na *World Wide Web* deixa rasto, tornando visíveis os nossos gostos, as nossas pesquisas, os nossos dados, a nossa informação. Daí, é necessário que os regimes de proteção de dados pessoais estejam em constante evolução.

Da mesma forma é necessária uma contínua adaptação do Direito e dos Tribunais a esta nova realidade, para que reinterpretem os princípios e regras em vigor, à luz do

¹⁶³ Viana, Vítor Rodrigues, “Editorial”, in *idn Nação e Defesa, Cibersegurança*, Instituto da Defesa Nacional, n.º133, p.6.

¹⁶⁴ *Idem, Ibidem*.

desenvolvimento tecnológico; como exemplo destacamos a jurisprudência do Tribunal Europeu de Justiça, no caso Lindqvist.

Por permitir a identificação do respetivo utilizador, o *IP*¹⁶⁵ é assim considerado um dado pessoal. O *IP* possibilita a comunicação na *Internet*, isto é, quando queremos consultar uma página na *Internet* o nosso computador remete informação contendo o pedido, o nosso endereço *IP* (para que se saiba para onde enviar a resposta) e o *IP* do sítio na *Internet*, alojado num servidor.¹⁶⁶

À medida que o *Ciberespaço* e os endereços de *IP* crescem, assistimos ao aumento de tráfego de redes sem fios (*wireless*) comparativamente às redes com fios, *wired devices*. Quanto mais o tráfego da *Internet* provém de dispositivos exteriores ao computador, “non PC devices”, mais se torna difícil pensar num tipo de crime que não esteja diretamente ligado ao endereço de *IP*.¹⁶⁷

A rede *Wireless* é outra das ameaças do *Ciberespaço*, por ser um dos ambientes mais vulneráveis que pode haver numa rede interna, pois não permite um controlo muito restrito de todos os sistemas que lá se podem ligar. Por exemplo, se for uma rede *wireless* com acesso livre, as pessoas que passam ou estão na organização podem ligar os seus dispositivos, como computadores portáteis, telemóveis, *tablets*, a esta rede, não havendo qualquer controlo pelos gestores da rede. Estas redes *wireless* são, na verdade, um dos pontos mais perigosos de entrada de “malware” na rede, até mesmo de forma não intencional.

De acordo com um recente estudo, atualmente existem mais dispositivos tecnológicos por todo o mundo do que humanos. Como revelou um analista digital da *GSMA Intelligence* o número de dispositivos móveis ligados por todo o mundo é superior ao

¹⁶⁵ O *IP* (*Internet Protocol*) é um número que é atribuído a cada computador quando este se liga à *Internet*. O responsável pela atribuição de um endereço *IP* pode ser, por exemplo, um gestor de uma rede local ligada à *Internet* (como uma Universidade, uma empresa, um espaço público), ou um fornecedor de acesso à *Internet*.

¹⁶⁶ Castro, Catarina Sarmiento e, “Proteção de Dados Pessoais na Internet”, in Gonçalves, Maria Eduarda, *Internet, Direito e Tribunais, Sub Judice, Justiça e Sociedade*, revista trimestral n.º35, Almedina, Setembro 2006, p.15.

¹⁶⁷ UNODC, United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, February 2013, United Nation, New York, 2013, p.6.

total da população humana. O número de dispositivos móveis é atualmente de 7.22 bilhões, enquanto o número de pessoas no mundo ronda os 7.19 e 7.2 bilhões.¹⁶⁸

Em 2020, para uma população mundial de 7,6 bilhões de pessoas, calcula-se que haja 50 bilhões de dispositivos conectados¹⁶⁹, o que dá um número elevadíssimo de 6,58 dispositivos conectados por pessoa. Ou seja, calcula-se que em 2020, irão existir quase 7 dispositivos tecnológicos por cada pessoa no mundo. Sem mencionar os rápidos avanços dos dispositivos, da tecnologia e da própria *Internet*, que podem fazer com que estes números aumentem ainda mais.

Outro dos desafios ligado ao *Ciberespaço* é a proteção da privacidade dos cidadãos. Com um mundo tecnológico cada vez mais global, coloca-se hoje ao cidadão comum a questão de como pode este manter a sua vida privada quando existe um número de entidades (serviços, órgãos, organismos, empresas) que vai recolhendo e guardando, ao longo do tempo, todos os dados pessoais e também o seu percurso existencial?

Hospitais, bancos, polícias, seguradoras, empresas nacionais ou multinacionais, ou qualquer outra entidade que nos tenha prestado um serviço, têm guardado os nossos dados pessoais nas suas bases de dados. Não só por questões de segurança, mas também para garantir uma melhor qualidade de serviço aos seus utentes, podendo aceder de imediato aos seus dados. Mas se ao cruzarmos esses dados com os de outras bases, quer nacionais quer internacionais (operadoras telefónicas, portagens, transportes públicos, companhias aéreas), percebemos como esta realidade se pode transformar numa ameaça à nossa segurança e privacidade, dada a grande quantidade de dados que circulam nos sistemas informáticos. Assim, é fácil de avaliar como as instituições e empresas penetram hoje em dia em praticamente todos os setores da atividade humana, recolhendo todo o tipo de dados úteis aos seus fins organizacionais, de planificação e desenvolvimento.¹⁷⁰

Cada vez mais o acesso ilegítimo a redes e tráfico de dados pessoais tornam-se um problema grave, nomeadamente, porque podem partir, e partem (na grande maioria), de atuações de criminosos situados num ponto remoto do mundo. Na maioria dos casos

¹⁶⁸ Gabinete Nacional de Segurança, *Cyber Newsletter*, n.º37/2014, 10 de outubro de 2014, [Em linha]. Disponível em <http://www.gns.gov.pt/new-ciberseguranca/newsletter.aspx>, p. 11.

¹⁶⁹ Evans, Dave, *A Internet das Coisas, como a próxima evolução da Internet está mudando tudo*, Cisco Internet Business Solutions Group (IBSG), abril 2011, p.3.

¹⁷⁰ Raíña, Paula; Vaz, Sónia Queiróz, *Guia Jurídico da Internet em Portugal*, Centro Atlântico ed., Portugal, 2001, p. 43.

atuam com um endereço de *IP* oculto ou em nome de outrem. O que aumenta a gravidade destes ataques e diminui consideravelmente a hipótese de se achar o verdadeiro culpado.

Apesar de existirem algumas ferramentas que facilitam a navegação na *Internet* e o modo como os sítios nos oferecem os seus serviços, a verdade é que são igualmente uma das ameaças do *Ciberespaço*, já que se aproveitam da nossa privacidade. Por exemplo, os chamados *cookies*. Estes são ficheiros especiais que se auto instalam no disco rígido de um computador e que têm como função recolher informações acerca do utilizador daquele computador quando este se encontra ligado à *Internet*, assim como o tipo de computador utilizado e a forma de acesso. Posteriormente, enviam essas informações de volta ao sítio de origem.

Embora a utilização de *cookies*, possa ser desativada no próprio computador, a verdade é que alguns sítios não permitem a navegação a quem não aceite estes ficheiros. Assim, se o internauta pretender utilizar os referidos *cookies*, a sua navegação ficará facilitada, já que o sítio irá sugerir opções que lhe podem ser úteis. No entanto, haverá sempre uma intrusão à sua privacidade.¹⁷¹ Se não permitir estes *cookies*, também não poderá aceder à grande maioria dos sítios eletrónicos, já que hoje em dia, praticamente, todos usam esta ferramenta.

Assim, entendemos que a necessidade de proteger a privacidade dos cidadãos e os abusos do mundo digital será outro dos desafios face ao *Ciberespaço*.

A *Internet* não serve apenas para “navegar” em busca do conhecimento ou como ferramenta de lazer. Esta, foi criada e sedimentou-se como um espaço onde, de maneira pública ou com acesso reservado, é possível o estabelecimento de relações jurídicas, pessoais, de intercâmbio ou de puro convívio, através das ações dos utilizadores, sendo estes a parte ativa e importante desta tecnologia. Deste modo, e para prevenir que certos direitos não sejam lesados, o Direito é chamado a regular e a intervir nestas relações jurídicas quando necessário. E, embora em pequena escala, essa atuação do Direito começa já a ser visível. Como exemplo, temos em Portugal a primeira sentença de despedimento lícito por comentários na rede social *Facebook*. A sentença foi proferida pelo Tribunal do Trabalho de Matosinhos, dando razão à empresa *Esegur* por ter

¹⁷¹ Marques, Ana Margarida; Anjos, Mafalda; Vaz, Sónia Queiróz, *101 Perguntas e Respostas do Direito da Internet e da Informática*, CENTROATLANTICO.PT, Portugal, 2002, p. 38.

despedido, por justa causa, um trabalhador que fez comentários ofensivos à empresa, a alguns colegas e a alguns superiores na referida rede social. Na referida sentença, foi proferido pelo Juiz o seguinte argumento: “no mundo da Internet, em que as redes sociais e os *blogs* permitem a qualquer autor colocar as informações e fazer as afirmações que pretende, é inaceitável que a liberdade de expressão e de comunicação não tenha qualquer tipo de limites externos”.¹⁷²

Tal sentença só nos leva a crer que a *Internet* pode ter um âmbito virtual, mas é sustentada por pessoas ou entidades reais que, através das suas ações, interagem e comunicam umas com as outras. Como tal, enquanto plataforma de comunicação e informação, é suscetível de ser utilizada como instrumento de ofensa à honra, dignidade ou consideração social de uma pessoa em concreto, mediante imputação feita por outrem nesse sentido.¹⁷³ Da mesma forma acreditamos que é suscetível de ser sancionado pelo Direito o utilizador que através dela viole os direitos de terceiros.

Aliada à quantidade de informação disponível no *Ciberespaço*, surge outro desafio, a navegação e compreensão do mesmo. Como já referimos, este caracteriza-se por ser um espaço dominado, maioritariamente, pela língua inglesa e por ter conceitos e sistemas muito técnicos, próprios das novas tecnologias, mas pouco explorados pelos utilizadores comuns. Como Reginaldo Rodrigues de Almeida aponta, “os mecanismos de exclusão social passam pelos analfabetos em inglês. Palavras como *print screen*, *caps lock*, *enter*, *delete*, são de uso corrente entre os utilizadores de computadores e assiste-se à criação de verbos como *delitar*, *printar*, etc., palavras que, por um lado são entendidas por alguns dos que não recorrem a recursos informáticos diariamente e, por outro, são utilizadas, sabendo que correspondem a uma certa funcionalidade informática, mas sem que o utilizador saiba exatamente o que querem dizer, (...)”¹⁷⁴. Desta forma, como podem os utilizadores fazer uma simples pesquisa? Saber se é necessária uma atualização de algum programa? Que o seu computador tem um vírus informático ou que foi vítima de *Cibercrime*?

¹⁷² “Despedimento lícito por Comentários no Facebook”, OA – *Boletim da Ordem dos Advogados*, n.º111, fevereiro 2014, p.16.

¹⁷³ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade da Informação, Lisboa, Outubro, 2004, p.12.

¹⁷⁴ Almeida, Reginaldo Rodrigues de, *Sociedade Bit, Da Sociedade da Informação à Sociedade do Conhecimento*, 2ª ed., Quid Juris? Sociedade Editora, Lisboa, Setembro, 2004, p. 51.

A verdade é que atualmente, todos os utilizadores encontram dificuldades de navegação no *Ciberespaço*, inclusive os profissionais das mais variadas áreas. Por exemplo: advogados, médicos, biólogos, engenheiros são agora obrigados a adequar os seus conhecimentos e a sua profissão ao mundo digital e às novas tecnologias. Bill Gates chama a atenção para este assunto, focando precisamente as mudanças profissionais que aqui descrevemos, como por exemplo “a alteração das próprias formas de agir de um advogado na sua vida profissional, as vídeo conferências em tribunal.”¹⁷⁵ Temos como exemplo a criação da *Intranet*¹⁷⁶ utilizada nas organizações, nas empresas, nos tribunais, ou o programa *Habilus*¹⁷⁷ utilizado nas videoconferências em tribunal.

Para além da criação de grupos *online*, *blogues*, *sítios eletrónicos*¹⁷⁸, a *Internet* oferece também muitas *salas de chat* (as chamadas salas de conversação), onde se pode falar sobre tudo, em tempo real e de forma completamente anónima ou adotar outra identidade que não seja a nossa. “As salas organizam-se em torno das mais variadas temáticas, desde o cinema à economia, passando por questões ligadas a uma determinada cidade, a salas para pais, enfim, tudo o que se consiga imaginar. Contudo as que têm um maior sucesso e onde se encontra um número crescente de pessoas, são as salas de sexo.”¹⁷⁹ Dado o aumento destes espaços na *Internet* e face aos riscos que trazem para os utilizadores, tendem a ser alvo de inspeção por parte dos administradores das empresas que restringem o uso de certas páginas dos seus empregados; dos diretores “das escolas que tentam controlar o uso e abuso das novas tecnologias por parte dos seus alunos”¹⁸⁰ e, das próprias famílias que, cada vez mais, são alertadas para os perigos que os seus filhos correm ao entrarem neste sítios, onde são aliciados para encontros e a

¹⁷⁵ Almeida, Reginaldo Rodrigues de, *Sociedade Bit, Da Sociedade da Informação à Sociedade do Conhecimento*, 2ª ed., Quid Juris? Sociedade Editora, Lisboa, Setembro, 2004, p. 172, *apud.*, Gates, Bill, *A Estrada do Futuro*. Editora: Cia das Letras, 1995, p. 224.

¹⁷⁶ *Intranet* – Rede interna de informações baseada na tecnologia da *Internet*. É usada por qualquer tipo de organização (empresa, entidade ou órgão público) que deseje compartilhar informações apenas entre seus utilizadores registados, sem permitir o acesso de outras pessoas. O que o utilizador vê é um *interface* igual ao da *Internet*. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1036.

¹⁷⁷ *Habilus* – Na sequência da instalação da *intranet*, foi introduzido na rede informática dos Tribunais, um programa designado “*habilus*”, o qual tem simplificado o trabalho dos oficiais de justiça, com a padronização da maioria dos atos, designadamente com formulários redigidos pela DGAJ, com a automatização da distribuição, com a criação de bases de dados dos elementos identificativos de cada processo, seus intervenientes, residências e endereços de *email* de mandatários. É igualmente através deste sistema que é possível o acesso ao registo informático de execuções. *Idem*, *Op. Cit.*, p. 968.

¹⁷⁸ Sítio - conjunto de páginas eletrónicas reunidas num só endereço na *Internet*. *Idem*, *Op. Cit.*, p.1042.

¹⁷⁹ Almeida, Reginaldo Rodrigues de, *Sociedade Bit, Da Sociedade da Informação à Sociedade do Conhecimento*, 2ª ed., Quid Juris? Sociedade Editora, Lisboa, Setembro, 2004, p. 174.

¹⁸⁰ *Idem*, *Ibidem*.

fornecer informações pessoais como os seus dados, *passwords*, moradas, números de cartão de crédito, etc¹⁸¹.

Esta questão ganha outros contornos quando pensamos como a *Internet* é um espaço vasto, de dimensão global, sem fronteiras, onde numa *sala de chat* podem estar, simultaneamente, várias pessoas de todo o mundo, agindo de boa ou má-fé, adotando identidades verdadeiras ou falsas, sendo vítimas ou agressores.

Não obstante o facto de os pais serem continuamente alertados para os perigos que os filhos correm ao entrarem nestes ambientes tecnológicos, quer sejam as supra referidas salas de *chat* ou as famosas redes sociais, como o *Facebook*, *Twitter*, ou o *Instagram*¹⁸², a verdade é que são as crianças e os jovens os utilizadores mais assíduos e os alvos mais fáceis dos perigos que estes espaços comportam.

Nesta *Era*, a *Internet* revelou-se um excelente veículo para as organizações com interesses na pedofilia ou no tráfico de seres humanos, de prostituição, bem como de todos os tipos de seitas e negativismos.¹⁸³ Torna-se assim fácil para estas entidades conseguirem novos interessados e afiliados, sem serem descobertos pelas autoridades, uma vez que o conteúdo dos mesmos se encontra, na sua grande maioria, indisponível a qualquer um. É necessário ter uma senha de acesso e entrar numa *Internet* quase “secreta”, ou como é conhecida, *DarkNet*.

No entanto, também na *Internet* dita comum, a *Surface Web*, são divulgadas fotografias e imagens ou vídeos dos mais variados tipos, bem como os contactos para aceder a essas pessoas, bens e serviços legais ou ilegais.

Como já referimos, o fenómeno da *Globalização* faz com que não seja necessário procurar por certos serviços já que estes vêm até nós. Por exemplo: “são as facilidades bancárias para pedir empréstimos aos bancos, que são enviadas directamente para as nossas caixas de correio, mas são também as crianças que são levadas até aos pedófilos; são as compras on-line que nos possibilitam uma maior qualidade de vida, se pensarmos no desperdício de tempo que as levaríamos a fazer, proporcionando-nos tempo para

¹⁸¹ Almeida, Reginaldo Rodrigues de, *Sociedade Bit, Da Sociedade da Informação à Sociedade do Conhecimento*, 2ª ed., Quid Juris? Sociedade Editora, Lisboa, Setembro, 2004, p. 174.

¹⁸² *Facebook*, *Twitter* ou *Instagram* são exemplos de redes sociais de carácter público, que permitem a interação em tempo real com utilizadores de todo o mundo, sejam eles conhecidos ou não.

¹⁸³ Almeida, Reginaldo Rodrigues de, *Sociedade Bit, Da Sociedade da Informação à Sociedade do Conhecimento*, 2ª ed., Quid Juris? Sociedade Editora, Lisboa, Setembro, 2004, p. 177.

outras actividades, mas são também as mulheres que são levadas até aos clientes para exercerem a prostituição, em muitos casos, contra a vontade e sob ameaça de represálias”.¹⁸⁴

O tráfico de mulheres e a prostituição são outros dois desafios e ameaças do *Ciberespaço*, já que se tem verificado um grande aumento, dada à possibilidade de se chegar aos potenciais clientes através da *Internet*. O desemprego e as precárias condições de vida, aliadas à mobilidade das pessoas e facilidade em se viajar, especialmente entre os Estados Membros, graças ao espaço *Schengen*, dão uma nova logística a todo este fenómeno que antigamente não era possível.

De igual forma, o aumento da partilha de informação pessoal na *Internet* quer de imagens, fotografias, vídeos, relatos de atividades do dia-a-dia, através das redes sociais, têm gerado novos desafios para o Direito, já que são cada vez mais os casos de extravio desses dados pessoais, furto de identidade ou de casos mais graves, como o *Cyberstalking*.

Outro dos problemas que encontramos no *Ciberespaço* é à proteção dos cidadãos com necessidades especiais. E, embora existam já medidas neste domínio, como o *Programa Nacional para a Participação dos Cidadãos com Necessidades Especiais na Sociedade da Informação*, aprovado pelo Conselho de Ministros n.º 110/2003, de 12 de agosto, a verdade é que não possuem força vinculativa. Os cidadãos têm, como já dissemos, muita informação ao seu dispor, mas continuam a não ser informados sobre aspetos importantes, sobre os seus direitos e deveres. Continuam a faltar padrões mínimos de acesso dos cidadãos com necessidades especiais ao sistema de informação, assim como faltam ações de sensibilização, cooperação com empresas e entidades, bem como implementações práticas e incentivos à utilização das novas tecnologias da sociedade de informação por esses cidadãos.¹⁸⁵

Por fim, importa referir aquela que consideramos ser uma crescente ameaça do *Ciberespaço*: o *Ciberterrorismo*. Esta é uma ameaça cada vez mais comum e global que usa a *Internet* como meio de propaganda, para transmitir as suas mensagens, para causar o terror e como forma de recrutamento de novos afiliados, infiltrados e seguidores por

¹⁸⁴ Almeida, Reginaldo Rodrigues de, *Sociedade Bit, Da Sociedade da Informação à Sociedade do Conhecimento*, 2ª ed., Quid Juris? Sociedade Editora, Lisboa, Setembro, 2004, p. 178.

¹⁸⁵ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 33.

todo o mundo. O principal epicentro deste fenómeno e talvez o mais catastrófico de todos os tempos foi o atentado de 11 de setembro às torres gémeas nos Estados Unidos da América, que colocou o mundo em constante alerta, com transmissões em direto dos próprios atentados. Também “os massacres de *Littleton* provocaram nos Estados Unidos da América uma onda de alarme sobre os perigos, reais ou supostos, da Net, ampliados pela divulgação de números “bomba” sobre o crescimento em massa dos utilizadores”.¹⁸⁶

Não obstante estes ataques terem ocorrido nos Estados Unidos da América, a verdade é que as suas consequências foram também sentidas um pouco por todo o Mundo. As recentes guerras na Síria e no Líbano são também um forte exemplo disso. Paralelamente, os Estados Membros recebem de vários países vídeos com ameaças de atentados por parte de organizações radicais ou extremistas. Como revela José Magalhães, “Uma certeza muito confirmada pelo 11 de Setembro: se a Net pode ser usada por terroristas (tristemente pôde, pode e poderá!), é nas mãos dos que lutam pela liberdade, pela democracia e pela tolerância que ela releva o seu potencial sem paralelo”.¹⁸⁷

No quadro de guerra em curso, muitas medidas terão de ser adotadas para prevenir a apropriação da *Internet* para fins sinistros, sem a privar das suas mais preciosas características.¹⁸⁸

O grande desafio do Direito será certamente o combate a estas situações de risco do *Ciberespaço*, dado o seu crescimento ser cada vez maior e este fenómeno tomar proporções globais.

¹⁸⁶ Magalhães, José, *Homo S@piens, Cenas da Vida no Ciberespaço*, Quetzal Editores, Lisboa, 2001, p. 141.

¹⁸⁷ *Idem, Ibidem.*

¹⁸⁸ *Idem, Op. Cit.*, p. 318.

Capítulo II – Cibercrime

1- Noção

Desde que, em 1984, quando William Gibson utilizou pela primeira vez a palavra *Ciberespaço* na sua obra de ficção científica *Neuromancer*, surgiram várias expressões derivadas e com o mesmo prefixo daquela. Entre elas, *Ciberdireito* e *Cibercrime*.¹⁸⁹

Não obstante as várias alusões à palavra *Cibercrime*, a verdade é que não está doutrinariamente definido o seu conceito, ou seja, não existe nenhum dispositivo legal que use, refira ou defina este conceito. Do ponto de vista doutrinário também não existem teorizações nem delimitações metodológicas, não estando ainda assente se estamos perante um novo sector do direito penal ou se apenas se trata de um mero conjunto de normas penais que se referem ao ambiente digital.¹⁹⁰

No âmbito sociológico, o crime no *ciberambiente* está já autonomizado. Há investigações científicas e policiais sobre os crimes cometidos no *Ciberespaço* e as instâncias internacionais manifestam, cada vez mais, preocupação pelas consequências dos atos ilícitos cometidos nas redes, ou através das redes de computadores.¹⁹¹

Como refere o UNODC – *United Nations Office on Drugs and Crime* (Escritório das Nações Unidas sobre Drogas e Crime, uma agência especializada da Organização das Nações Unidas, criada em 1997, com sede em Viena), não existe uma definição única de “Cibercrime”, considerando mais adequado incluir neste conceito, não tanto um tipo de atos, mas um conjunto de atos ou condutas, que podem ser organizados em categorias com base no objeto do crime ou no *modus operandi*.¹⁹²

Também não existe consenso quanto à expressão utilizada para denominar este tipo de criminalidade emergente. Alguns autores utilizam o conceito de *Cibercrime*, outros utilizam a expressão de *Crime Informático* (adaptação da clássica expressão inglesa *computer crime*), enquanto outros apelidam de *Crime Tecnológico* (também uma adaptação do termo inglês *hightec crime*).

¹⁸⁹ Verdelho, Pedro, *Cibercrime*, in *Direito da Sociedade da Informação*, vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003, p. 347.

¹⁹⁰ *Idem*, *Ibidem*.

¹⁹¹ *Idem*, *Ibidem*.

¹⁹² UNODC – United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, [Em linha], fevereiro de 2013, p. 11. Disponível em http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Outra das definições utilizadas para definir este tipo de crimes é *Cibercriminalidade*. A *Cibercriminalidade* refere-se, geralmente, a um amplo leque de diferentes atividades criminosas que envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais.

A *Cibercriminalidade* inclui as infrações tradicionais, por exemplo: fraude, falsificação e roubo de identidade; infrações relativas aos conteúdos, por exemplo: distribuição de material pedo-pornográfico em linha ou incitamento ao ódio racial; e crimes respeitantes exclusivamente a computadores e sistemas informáticos, por exemplo: ataques contra os sistemas informáticos, recusa de serviço e *software* malicioso.¹⁹³

Como consta da própria definição de *Cibercriminalidade*, esta inclui três grupos de crimes:

1.- Abrange os crimes que embora sejam cometidos por via de computadores ou sistemas de computadores (ou seja, *on-line*), não se distinguem do mesmo tipo de crime cometido por outras vias. Isto é, dogmaticamente nada os distingue da sua forma tradicional, apenas têm de diferente o meio usado. Por exemplo: o abuso de liberdade de imprensa cometido num jornal *on-line*, ou as injúrias ou ameaças remetidas por correio eletrónico, ou o branqueamento de capitais utilizando um banco virtual.¹⁹⁴

2.- Distingue outros crimes, que têm de especial o ambiente em que são praticados. Estes são gerados no ambiente informático e só podem ocorrer pela especificidade do meio. Por exemplo: os crimes de burla informática ou de devassa por meio da informática.¹⁹⁵

3.- Define outra espécie de crimes, os quais se caracterizam por serem praticados contra o meio informático. São crimes contra computadores ou sistemas de computadores, ou seja, são os crimes informáticos propriamente ditos. São exemplos deste tipo de crimes o dano informático ou o acesso ilegítimo, ou ainda a sabotagem informática.¹⁹⁶

¹⁹³ (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013.,p.3.

¹⁹⁴ Verdelho, Pedro, *Cibercrime*, in *Direito da Sociedade da Informação*, vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003, p. 348.

¹⁹⁵ *Idem, Ibidem.*

¹⁹⁶ *Idem, Ibidem.*

Todos estes conceitos pretendem, no fundo, definir os vários tipos de crimes que podem ser praticados através do computador ou contra o computador.

Ainda quanto ao próprio conceito de *Cibercriminalidade*, pode ser analisado de duas ou três formas. Como revela Rui Batista, “numa primeira análise diria que há um conceito formal, em que *Cibercriminalidade* é o que a própria Lei do Cibercrime (Lei 109/2009, de 15 de setembro) assim o define, neste caso no seu artigo 11.º, n.º1, alíneas a), b) e c)”.¹⁹⁷ Nomeadamente, quando se refere aos crimes “previstos na presente lei” (alínea a); “cometidos por meio de um sistema informático” (alínea b); ou “em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico” (alínea c). Temos assim um primeiro conceito legal de *Cibercriminalidade*.

Numa segunda análise podemos considerar que existe um conceito pessoal de *Cibercriminalidade*,¹⁹⁸ isto é, um conceito que é defendido por cada autor, embora haja uma equiparação quanto aos conceitos adotados quer por um quer por outros. Por exemplo, Rogério Bravo refere que, de uma maneira geral, podemos definir *Cibercriminalidade* como a “criminalidade relacionada com o universo cibernético e as redes de comunicação entre computadores”.¹⁹⁹

Podemos ainda considerar uma terceira análise, em que a definição de *Cibercriminalidade* pode ser entendida como um conceito genérico, que foi dado a um novo e constante tipo de crime que foi surgindo, relacionado com os meios informáticos, abrangendo quer os crimes praticados contra a máquina (computadores), quer os crimes praticados através da máquina.²⁰⁰ Ou seja, de forma a criar um conceito genérico e universal que pudesse abarcar todos estes tipos de crimes já mencionados.

¹⁹⁷ Entrevista a Rui Batista, Procurador-Adjunto - Colaborador do Gabinete Cibercrime, realizada no dia 14 de julho de 2014.

¹⁹⁸ *Idem, Ibidem.*

¹⁹⁹ Entrevista a Rogério Bravo, Inspetor-Chefe, Polícia Judiciária de Lisboa, realizada no dia 17 de fevereiro de 2014.

²⁰⁰ Entrevista a Rui Batista, Procurador-Adjunto - Colaborador do Gabinete Cibercrime, realizada no dia 14 de julho de 2014.

2 - Aspetos fundamentais

Atualmente a *Internet* atinge proporções como nunca antes vistas, quer em termos de conteúdo quer em termos de número de utilizadores. E são precisamente os utilizadores quem mais sofre com o crescimento da *Internet* e com o consequente aumento dos perigos que esta comporta.

Um inquérito do *Eurobarómetro da Comissão Europeia* revela que 76% dos cidadãos concordam que o risco de se tornarem vítimas da criminalidade informática é maior comparativamente com os anos anteriores e, 12% revelam já terem sido vítimas de pirataria das suas contas de rede social ou de correio eletrónico.

O mesmo inquérito revela ainda que apesar de 70% dos utilizadores da *Internet* no conjunto da União Europeia se sentirem capazes de a utilizar nas tarefas do dia-a-dia (por exemplo, para fazer compras ou efetuar operações bancárias *online*), apenas 50% optam por fazê-lo realmente.²⁰¹ Já 37% dos inquiridos dizem ter receio da utilização abusiva de dados pessoais e 35% não confiam na segurança dos pagamentos feitos na *Internet*.²⁰²

Como declarou Cecilia Malmström²⁰³, este inquérito revela o impacto devastador que a *Cibercriminalidade* tem sobre a utilização da *Internet* - demasiadas pessoas optam por não tirar pleno partido de todas as possibilidades que a *Internet* nos proporciona. Isto prejudica o ambiente digital tanto da nossa economia como das nossas vidas. Necessitamos de reforçar a cooperação europeia, como base no trabalho do *Centro Europeu da Cibercriminalidade*, de forma a atingirmos a cúpula do crime organizado em linha.²⁰⁴

O inquérito revela que menos de metade dos utilizadores da *Internet* mudou a sua palavra-passe no computador durante o último ano e que 87% dos inquiridos não divulgam informações pessoais na rede, o que, de todo, não exclui a possibilidade de serem vítimas destes ou outros ataques informáticos. De acordo com o *Eurobarómetro*, a maioria dos inquiridos (52%) considera que não está bem informada sobre os riscos da

²⁰¹ Disponível em www.europa.eu/rapid/press-release_IP-12-751_pt.htm.

²⁰² *Idem, Ibidem.*

²⁰³ Comissária da União Europeia responsável pelos Assuntos Internos.

²⁰⁴ Comissária da União Europeia responsável pelos Assuntos Internos, comentário no âmbito do inquérito do Eurobarómetro. Disponível em www.europa.eu/rapid/press-release_IP-12-751_pt.htm.

Cibercriminalidade e 7% referem já ter sido vítimas de fraude através do cartão de crédito ou serviços bancários *online*.

Através da análise destes dados, vemos, mais uma vez, que a informação e a prevenção quanto a estes crimes são essenciais, já que este inquérito abrangeu mais de 27 mil pessoas em todos os Estados Membros, e a percentagem dos cidadãos que se consideram mal informados é de 52%, ou seja, um pouco mais de metade do total dos inquiridos. Pelos referidos dados e tendo em conta o número de inquiridos, podemos constatar que os resultados são números assustadores que revelam que o *Ciberespaço* não é um sítio onde os cidadãos se sentem seguros e que há uma grande preocupação e desconfiança quanto ao uso da *Internet*, especialmente quanto aos casos de *Cibercrime*.

A verdade é que os cibercriminosos utilizam métodos cada vez mais sofisticados para se introduzirem nos sistemas informáticos, desviarem dados críticos ou exigirem resgates às empresas. O aumento da espionagem económica e de atividades patrocinadas por Estados no mundo digital coloca os governos e as empresas dos países ocidentais e da União Europeia à mercê de uma nova categoria de ameaças. E num mundo global como o que hoje vivemos é, sem dúvida, um tema de extrema importância, ao qual deve ser dada a devida atenção.

Nos capítulos seguintes iremos abordar detalhadamente a problemática do *Cibercrime* e os vários tipos de criminalidade emergente.

3. - A Problemática do Cibercrime e os novos fenómenos criminais

O aparecimento das novas tecnologias e consequente crescimento da *Sociedade da Informação* um pouco por todo o mundo tem dado origem a um desenvolvimento tecnológico que modificou, de forma irreversível, todas as áreas (económica, política e social) quer pela positiva quer pela negativa. Assim, à medida que os benefícios desta nova *Era* iam surgindo, apareciam também novas formas de crime ligadas aos meios tecnológicos.

Em Portugal, o *Cibercrime* é ainda um tema pouco abordado, mas que merece toda a nossa atenção, dado o seu contínuo crescimento e características imprevisíveis. Calcula-se que em média por ano, são realizados mais de 800 mil ataques cibernéticos em todo o mundo. Só em Portugal 7% dos crimes de branqueamento de capitais estão ligados ao *Cibercrime*.²⁰⁵

Como evidenciam Pedro Veiga e Marta Dias, “O carácter global da *Internet*, a possibilidade de produzir e distribuir qualquer tipo de conteúdos sob a forma digital e a custos quase nulos, bem como o enorme número de pessoas que usam a rede, veio realçar a necessidade de novas formas de intervenção num sector em que há muitos tipos de intervenientes.”²⁰⁶

Além de global e inexplorado, o *ciberambiente* tem outra característica que o torna impenetrável à lógica normativista e disciplinadora do direito positivo: está em constante evolução.²⁰⁷ E estes são os dois primeiros problemas que destacamos no *Cibercrime*: o seu âmbito de atuação global e a sua constante evolução.

No primeiro caso, podemos afirmar que não se trata de um tipo de crime que ocorra mais num dado local ou país do que noutro, mas sim, trata-se de um crime transnacional, que não conhece fronteiras nem jurisdições. No segundo caso, o *Cibercrime* evolui à medida que surgem novos avanços na *Internet* e novas ferramentas tecnológicas.

²⁰⁵ Workshop “A Prevenção e o combate à cibercriminalidade – A experiência nacional, europeia e internacional”, Direcção Geral de Política de Justiça, 21 de novembro de 2013.

²⁰⁶ Veiga, Pedro; Dias, Marta, *A Governação da Internet*, [Em linha], JANUS.NET e-journal of International Relations, nº1, Outono 2010, p.76. Disponível em http://janus.ual.pt/janus.net/pt/arquivo_pt/pt_vol1_n1_pdf/pt_vol1_n1.pdf, (consultado em 5.6.2014).

²⁰⁷ Verdelho, Pedro, *Cibercrime*, in *Direito da Sociedade da Informação*, vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003, p.356.

Diretamente ligado aos avanços tecnológicos e aos consequentes novos tipos de crime, surge outro problema: traçar o perfil dos novos agentes cibercriminosos.

No início dos anos 70 e 80 o criminoso informático podia ser definido como alguém especialista em computadores e sistemas informáticos. Tradicionalmente, os agentes deste tipo de crimes tinham entre os 20 e os 30 anos. Em alguns casos ainda se enquadra este perfil, quando as motivações das ações ilícitas são o desafio ou a curiosidade. Nestas situações, a idade da generalidade dos agentes é mesmo próxima dos 20 anos.²⁰⁸ Pelo contrário, quando o que está em causa é o lucro ou interesses ideológicos, a idade dos agentes é maior. O mesmo acontece quando as redes são usadas para outras atividades socialmente condenáveis e penalmente reprimidas, por exemplo, no caso das burlas ou extorsões, já que se trata de crimes que exigem uma maior preparação e premeditação por parte do autor.²⁰⁹

Esta evolução do perfil dos agentes dos crimes informáticos leva-nos a concluir que a prevenção criminal neste sector não passa pela mera repressão, mas tem de ser encarada numa perspetiva global e envolvente, abrangendo o sistema educativo e a segurança social, em conjunto com as organizações representativas das famílias.²¹⁰ Desta forma, a criminalidade informática pode ser prevista e prevenida, a começar pelas camadas mais jovens.

Atualmente, graças à facilidade de acesso aos meios tecnológicos e à fácil compreensão dos mesmos, qualquer pessoa pode cometer um ato criminoso, a começar pelos jovens, já que são a maioria dos utilizadores da *Internet*. Por exemplo, o envio de uma mensagem de correio eletrónico com um vírus, ou envio de mensagens *spam* (também conhecidas como *mensagens corrente*, que são enviadas em massa por vários internautas), acesso a bases de dados, *phishing*, podem constituir atos de *Cibercrime*.

O facto de o *Ciberespaço* ser uma área global sem fronteiras, aliado à realidade social e cultural em que vivemos, faz com que seja ainda mais difícil conhecer estes agentes, já que os ataques por estes praticados (por exemplo, envio de vírus, ataques a servidores, acesso ilegítimo a redes, tráfico de dados pessoais, entre tantos outros), podem partir de

²⁰⁸ Verdelho, Pedro, “Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º6, Julho-Dezembro 2005, p. 165.

²⁰⁹ *Idem, Ibidem.*

²¹⁰ *Idem, Ibidem.*

agentes criminosos situados em qualquer ponto do mundo, agindo anonimamente ou adotando a identidade de terceiros.

A verdade é que quem queira praticar atividades ilícitas tem a sua ação facilitada graças à *Internet*, por duas razões:

- Se os serviços de alojamento ou de acesso à *Internet* forem proibidos de alojar essas atividades ou conteúdos ou permitir o acesso a determinados utilizadores, quer por via de publicação de legislação, decisão administrativa ou judicial, o infrator transfere o seu conteúdo ou pede o acesso a um servidor *offshore*.²¹¹
- Se, contrariamente, os servidores forem estrangeiros, é técnica e juridicamente difícil para as autoridades de outro Estado proibirem que esses servidores armazenem e difundam certo tipo de informações, ou prestem determinado tipo de serviços.²¹²

Como refere Joel Timóteo Ramos Pereira, os criminosos mais experientes nas novas tecnologias utilizam técnicas que lhes permitem ocultar a sua conduta, nomeadamente, tornando anónima a sua presença na *Internet* (por exemplo, utilizando alguns destes programas: *Anonymizer*²¹³; *Anonymicer*²¹⁴; *Freedom*; *IDzap*, entre outros²¹⁵) cifrando e codificando as mensagens e comandos eletrónicos.²¹⁶ Não é totalmente impossível descobrir a localização dos aparelhos tecnológicos, no entanto, estes programas dificultam, em certa parte, descobrir qual o ponto de acesso dos mesmos. Também o chamado *IP Spoofing*²¹⁷ serve para encobrir a localização de um dado endereço *IP*.

Os motivos destes agentes são dos mais variados, seja por divertimento, para mostrar o seu valor, por dinheiro, fama, por pura malícia, como forma de revelia a alguma entidade, órgão político ou sociedade, por vingança, aposta ou ordem de outro

²¹¹ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 499.

²¹² *Idem, Ibidem*.

²¹³ Anonymizer – “Permite ocultar o browser atrás do proxy do servidor ou atrás do proxy do próprio programa. <http://www.anonymizer.com>”. Pereira, Joel Timóteo Ramos, *Direito da Internet e Comércio Eletrónico*, Quid Juris?, Sociedade Editora, Lisboa, 2001, p.489.

²¹⁴ Anonymicer – “Programa alemão para a navegação anónima. É semelhante ao Anonymizer, com a particularidade de ser totalmente grátis, permitindo ainda remeter mensagens de email de forma anónima”. *Idem, Ibidem*.

²¹⁵ O autor Joel Timóteo Ramos Pereira refere e define alguns exemplos de programas que permitem tornar anónima a nossa navegação na *Internet*, entre outras formas de privacidade. a 491.

²¹⁶ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 499.

²¹⁷ *IP Spoofing*- ataque em que um sistema assume ilicitamente a personalidade de outro sistema usando o seu endereço de identificação na *Internet*. *Idem, Op. Cit.*, p. 1037.

cibercriminal numa posição superior (no caso de pertencer a um grupo), entre outros casos. Da mesma forma, os meios pelos quais atuam são dos mais variados: *Spam*, *Cookies*, *Spyware*, *Trojans Horses*²¹⁸, *Hoaxes*²¹⁹, *Sniffers*²²⁰. Os vírus informáticos²²¹ dividem-se em vírus de *arquivos ou programas*²²², vírus de *Boot*²²³, vírus de *macro*²²⁴, vírus de *Stealth*²²⁵ e vírus *Polimórficos*²²⁶, só para nomear os mais comuns.

Ainda quanto aos cibercriminosos, os agentes mais conhecidos dividem-se em dois tipos: *Hackers* e *Crackers*. O *Hacker* é uma pessoa que procura aceder a sistemas sem autorização, usando técnicas próprias, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros.²²⁷ O *Cracker* é um *Hacker* que, ilegalmente,

²¹⁸ *Trojans Horses*- Cavalos de Tróia não são vírus, mas programas que são instalados em computadores com intenções maliciosas e utilizados para abrir portas para que o computador possa ser atacado remotamente. O seu objetivo é causar algum dano ao computador onde esteja instalado, apagando arquivos, pastas ou prejudicando a sua funcionalidade. Na sua maioria, os *trojans* não são detetados pelos programas de antivírus. Uma vez instalado, o *trojan* pode capturar informações: nomes de bancos, números de contas, senhas, números de cartões de crédito, certificados digitais e outros códigos utilizados em transações. Após colher essas informações, pode remeter as informações para o seu criador e/ou auto-destruir-se, eliminando todos os vestígios da sua passagem.” Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1043.

²¹⁹ *Hoaxes* - são *emails* (mensagens de correio eletrónico), na maioria dos casos com remetente de empresas conhecidas ou de órgãos governamentais, mas que na verdade comportam mensagens falsas, carregadas de vírus.

²²⁰ *Sniffers* - são programas que monitorizam o tráfego em rede. Os *hackers* usam os *Sniffers* para capturar dados transmitidos na rede. A esta técnica também é dado o nome de *Sniffing*: programa ou dispositivo que analisa o tráfego na rede. Os *Sniffers* são úteis para a administração de redes, mas, sendo utilizados por *Hackers* ou *Crackers*, permitem obter palavras passe (*password's*) e quaisquer outras informações ou conteúdos. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1042.

²²¹ *Vírus informáticos*- são um *software* malicioso que tem a função de auto-replicar-se e infetar partes do sistema operativo ou dos programas de aplicação, com o objetivo de causar a perda ou dano nos dados guardados nos computadores. *Idem, Op. Cit.*, p. 1044.

²²² *Vírus de arquivos ou programas*- são aqueles que infetam ficheiros de programas. São arquivos que têm em regra as extensões *COM*; *EXE*; *OVL*; *DLL*; *DVR*; *SYS*; *BIN* e *BAT*. *Idem, Ibidem*.

²²³ *Vírus de Boot*- são vírus que infetam a área de sistema de um disco. *Idem, Ibidem*.

²²⁴ *Vírus de Macro*- são vírus que infetam os arquivos dos programas *Microsoft Office*, *Word*, *Excel*, *PowerPoint* e *Access*. Todos estes vírus usam a linguagem de programação interna do programa, que foi criada para permitir que os utilizadores automatizem determinadas tarefas. *Idem, Ibidem*.

²²⁵ *Vírus de Stealth*- utiliza técnicas para ocultar as alterações executadas, e enganar o antivírus, como por exemplo, fazendo um *backup* dos arquivos alterados, isto é, fazendo uma cópia de segurança de dados e programas, feita em diferentes formatos (como disquete, fita magnética, disco *Zip* ou *CD-R*). *Idem, Ibidem*.

²²⁶ *Vírus Polimórficos*- utilizam técnicas de criptografia para construir a sequência de *bytes* (conjunto formado por oito *bits*. *Bit* é a menor unidade digital de informação, representada por 0 ou 1). A cada cópia gerada, uma nova combinação é utilizada para criptografar essa sequência, de forma que um único vírus pode ter inúmeras formas diferentes, que são decodificadas por chaves contidas numa pequena parte do vírus, sempre que necessário. *Idem, Ibidem*.

²²⁷ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1035.

entra, altera, apaga ou introduz informação distinta, programas ou vírus, em sistemas protegidos da *Internet*.²²⁸

Para além das diferenças em termos de conceito, estes dois cibercriminosos distinguem-se também pelo âmbito da sua atuação. Enquanto um procura aceder a sistemas sem autorização, mas adotando uma conduta menos lesiva (*Hacker*), o outro adota uma conduta não ética, invadindo sistemas com interesses patrimoniais ou danosos (*Cracker*). Não obstante, ambos praticam condutas lesivas, puníveis por lei.

É impossível avaliar a magnitude do problema do *Cibercrime*, dadas as suas próprias características e a dos seus agentes. No entanto, estima-se que o número de casos deste crime seja cada vez maior.

Não obstante, são já alguns os aspetos legislados quanto a esta matéria pelo Direito nacional e europeu: “A proteção dos dados pessoais, a defesa dos direitos de propriedade intelectual e direitos conexos, a luta contra a cibercriminalidade, a proteção dos menores a quem é reconhecida especial debilidade no âmbito da utilização diária dos recursos da Rede, em particular as redes sociais, os direitos dos consumidores em geral, os eventuais constrangimentos no acesso comercial aos serviços *Internet* e a respectiva regulação pelas autoridades competentes em cada país”²²⁹, entre outros casos que também iremos abordar nos capítulos seguintes.

Por fim, outro dos problemas que destacamos quanto à temática do *Cibercrime* é o elevado custo financeiro que este tem para a sociedade. Como revela o 5.º Estudo Anual da HP com o *Ponemon Institute*, está a aumentar o custo, a frequência com que ocorrem e o tempo de resolução dos ciberataques. De acordo com organizações americanas o valor atual é de \$ 12.7 m. Desde que este estudo começou houve um aumento de 96%.²³⁰

²²⁸ Pereira, Joel Timóteo Ramos, *Direito da Internet e Comércio Electrónico*, Quid Juris?, Sociedade Editora, Lisboa, 2001, p.474.

²²⁹ Veiga, Pedro; Dias, Marta, *A Governação da Internet*, [Em linha], JANUS.NET e-journal of *International Relations*, nº1, Outono 2010, pp. 82 e 83. Disponível em http://janus.ual.pt/janus.net/pt/arquivo_pt/pt_vol1_n1_pdf/pt_vol1_n1.pdf, (consultado em 5.6.2014).

²³⁰ Gabinete Nacional de Segurança, *Cyber Newsletter*, n.º38/2014, 17 de outubro de 2014, [Em linha]. Disponível em <http://www.gns.gov.pt/new-ciberseguranca/newsletter.aspx>, p. 8.

O tempo que se demora a resolver um caso de *Cibercrime* também aumentou 33%, durante o mesmo período, regra geral, com um custo de mais de \$1,6 m só para resolver um único ataque.²³¹

Face à constante evolução tecnológica, é imperativo que o Direito regule estas matérias, de maneira a inibir todas as formas de criminalidade tecnológica e a proteger os cidadãos, nomeadamente, através da proteção dos seus bens jurídicos, quer os já existentes, quer os que possam surgir com o avanço das novas tecnologias.

Da problemática do *Cibercrime* resultam ainda três fenómenos criminais que se entrecruzam e são cada vez mais imprevisíveis. Dadas as suas características, achamos importante abordar em capítulos separados: o Hactivismo; a Ciberespionagem e a Ciberguerra/Ciberterrorismo.

²³¹ *Idem, Ibidem.*

3.1. - Hacktivismo

O *Hacktivismo*: é um fenómeno com várias décadas e várias fases. A primeira fase foi marcada por três momentos:

- A emergência dos primeiros computadores, nos anos 50 e 60 do século passado, trouxe consigo alguns experimentalistas, na maioria estudantes universitários (no próprio MIT) que se dedicavam a testar as debilidades dos sistemas informáticos. Estes são considerados os “hackers originais”.
- O segundo momento ocorreu no início dos anos 70, quando surgiram diversos cérebros informáticos que se encarregaram de disseminar e descentralizar o *hardware* informático; entre eles, alguns atuais magnatas da indústria. Estes são apelidados de “hackers de hardware”.
- O último momento surgiu, sobretudo a partir dos anos 80, os “hackers de software”, que se dedicaram essencialmente a mudar ou a recriar programas sobre o *hardware* já existente.²³²

A segunda fase surge com a década de 90, mais politizada e como forma de contra cultura materializada no “hacking” (infiltrar) e no “cracking” (sabotar). Esta fase assemelhava-se mais a uma espécie de vandalismo informático, muitas vezes com o objetivo de colocar em causa os sistemas informáticos (nomeadamente, os níveis de segurança destes) e negociar posteriormente uma eventual contratação do *hacker* por parte das empresas informáticas. Noutros casos, o *hacker* era visto como um agente que solitariamente lutava com o seu conhecimento e inteligência, contra as grandes organizações, quebrando e subvertendo as barreiras defensivas, em nome da liberdade da *Internet*.²³³

A partir de meados dos anos 90 surge a terceira fase. Nesta fase houve uma alteração do papel do *hacker*; deixou de ser uma atuação individual e passou a ser uma atuação em grupo, de âmbito ciberglobal. Quanto à sua eficácia, em termos de dano, não resulta

²³² Esteves, Pedro, “Hacktivismo, Transpondo a Fronteira entre a Liberdade de Expressão e o Cibercrime”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.46.

²³³ *Idem, Ibidem.*

tanto da técnica dos agentes, mas, sim, pelo seu número e pela natureza massiva com que ocorrem os ciberataques.²³⁴

Da massificação deste fenómeno resultou, assim, o aparecimento do “Hactivismo”, um movimento multipolar de contornos estruturalmente anárquicos e que se procurou auto-legitimar através de declarações de princípios e de ensaios doutrinários.²³⁵

O conceito de “Hacktivismo” pode ser definido, utilizando a própria definição do termo desde que surgiu em 1995: *hacking*, ou seja, a infiltração não autorizada em sistemas de informação, e *activismo* (vertente política), isto é, a ação militante, tendo em vista alcançar um objeto político ou social.²³⁶

Quanto à sua definição tecnológica, o *modus operandi* do *hacktivismo* traduz-se na capacidade de romper e manipular a infraestrutura de tecnologias de informação digital e de comunicações, sistemas computacionais e processadores, ou seja, o *Ciberespaço*, protegidos, visando 5 objetivos centrais:

- 1- “O acesso a uma tecnologia ou conteúdos;
- 2- O reforço do poder dos utilizadores, em prejuízo do poder dos gestores do sistema;
- 3- A descentralização do controlo sobre a informação;
- 4- A introdução de soluções criativas, excedendo os limites previstos nos sistemas, colocando em causa os fins para os quais esse mesmo sistema foi criado;
- 5- A sabotagem e manipulação, através de ataques de negação de serviço, falsificação de sites, “phishing”, “password Crackers”²³⁷, vírus, troianos²³⁸, etc.”²³⁹

²³⁴ Esteves, Pedro, “Hacktivismo, Transpondo a Fronteira entre a Liberdade de Expressão e o Cibercrime”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.46.

²³⁵ *Idem, Ibidem.*

²³⁶ *Idem, Op. Cit.*, p.45.

²³⁷ *Password Crackers* ou *Cracking* – Consiste em fazer correr aplicações dentro de um determinado servidor que vão descodificando as passwords de acesso aos vários níveis de segurança do sistema. Cordeiro, Raul, “Ataques de DDOS, Medidas Preventivas”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p. 49.

²³⁸ Troianos (conhecidos como *trojans*) – São programas construídos para permitir abrir portas (canais de comunicação de dados de um protocolo específico) e assim enviar dados para o exterior, a partir da rede interna, e que podem eventualmente ser dados classificados. *Idem, Ibidem.*

²³⁹ Esteves, Pedro, “Hacktivismo, Transpondo a Fronteira entre a Liberdade de Expressão e o Cibercrime”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.45.

No plano político, o *hacktivismo* ficou conhecido em finais de 2010, quando o grupo “Anonymous” iniciou uma série de ciberataques, entre os quais vários ataques de negação de serviço através de uma série de solicitações sobre um determinado sítio eletrónico, provocando uma sobrecarga e paralisando o sistema, contra grandes corporações que se recusaram a apoiar o sítio eletrónico *Wikileaks*.²⁴⁰

O autor Pedro Esteves²⁴¹ faz alusão a dez critérios caracterizadores do “Hackerismo”, os quais achamos importante citar:

- 1- “O acesso à informação é um direito universal – citação frequente do Artigo 19.º da Declaração Universal dos Direitos do Homem (Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão);
- 2- A informação e expressão deve ser toda livre; consequentemente todo o controlo da informação é considerado “censura”;
- 3- “A informação quer ser livre” é uma das máximas do “Hacktivismo”.
- 4- A exigência de acesso ilimitado e total aos sistemas computadorizados;
- 5- A criação cibernética constitui uma arte tão digna como as artes (chamemos) clássicas;
- 6- A definição e imposição de condições limitativas (legais ou tecnológicas) no acesso à informação são atos ilegítimos e devem ser combatidos;
- 7- A autoridade (pública ou privada) exercida sobre os ciber-sistemas constitui uma ameaça;
- 8- A promoção da descentralização constitui um *modus operandi* permanente (não há um cérebro mas uma rede com uma multiplicidade de cérebros) – uma espécie de Al-Qaeda do *Ciberespaço*;
- 9- O *Hackerismo* constitui um movimento internacionalista militante – numa entrevista recente, um dos porta-vozes do movimento chamou-lhe as “Nações Unidas do Hacking”;

²⁴⁰ Esteves, Pedro, “Hacktivismo, Transpondo a Fronteira entre a Liberdade de Expressão e o Cibercrime”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.45.

²⁴¹ Pedro Esteves, Adjunto do Ministro da Administração Interna.

10- O *Hackerismo* assume-se como um movimento necessariamente radical – não há tréguas nem cedências.

11- A horizontalidade da rede e a liberdade individual são princípios dominantes.”²⁴²

De uma forma geral, o *Hacktivismo* rejeita a ideia da defesa da “desobediência civil” e opta antes pelo termo “disruptive compliance” (conformidade perturbadora/ disruptiva). Ou seja, defende a utilização de tecnologias intrusivas compatíveis com o espírito original da *Internet*, que consideram ter-se desviado dos fins para a qual foi criada.²⁴³

Uma das principais consequências do *hacktivismo*, o potencial comprometimento de informação, resultou, no ano de 2011, em perda de informação sensível por parte de algumas entidades públicas.²⁴⁴

No caso português, existem algumas debilidades quanto a este tema, as quais podem ser resumidas em três pontos:

1. Diversificação excessiva das infraestruturas públicas, redes e sistemas de informação e das soluções escolhidas na sua implementação, que tornam difícil a adoção de soluções defensivas comuns e que transformam o sistema pouco eficiente e dependente do mercado de segurança informática e da proteção de sistemas;
2. Inexistência de uma estrutura permanente que permita potenciar um mecanismo de coordenação e de monitorização contínua entre as infraestruturas do Estado e as infraestruturas privadas;
3. Por fim, destaque para uma cultura excessivamente descuidada em matéria de segurança das comunicações eletrónicas.²⁴⁵

Em conclusão, o “Hactivismo” é um dos fenómenos criminais cuja ação intencional, intrusiva e destrutiva no plano operacional constitui um fator de risco para a segurança e fiabilidade das comunicações e dos sistemas de informação sobre os quais assenta o

²⁴² Esteves, Pedro, “Hacktivismo, Transpondo a Fronteira entre a Liberdade de Expressão e o Cibercrime”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.46.

²⁴³ *Idem, Ibidem.*

²⁴⁴ Pereira, Júlio, “Cibersegurança, O Papel do Sistema de Informações da República Portuguesa”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.41.

²⁴⁵ Esteves, Pedro, “Hacktivismo, Transpondo a Fronteira entre a Liberdade de Expressão e o Cibercrime”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p. 47.

funcionamento da nossa sociedade pública e privada, transformando-os numa “infraestrutura crítica” nacional.²⁴⁶

Cabe às autoridades públicas, em conjunto com as entidades privadas (coletivas e individuais) o combate a este fenómeno criminal.

Desta forma, é necessário reduzir as oportunidades de afirmação e de disseminação do ideal militante do “hacker” através da contenção deste tipo de “crime de oportunidade”. A eliminação de oportunidades de sucesso resultará, como noutros domínios da segurança, no gradual esgotamento político do fenómeno do “Hacktivismo”.²⁴⁷

²⁴⁶ *Idem, Ibidem.*

²⁴⁷ Esteves, Pedro, “Hacktivismo, Transpondo a Fronteira entre a Liberdade de Expressão e o Cibercrime”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p. 47.

3.2. – Ciberespionagem

A *Ciberespionagem* é para alguns Estados uma ferramenta essencial para atingir a segurança nacional e a prosperidade económica, combinando os seus programas de recolha de informações de fonte aberta (HUMINT), inteligência de sinais (SIGINT) e operações de *Ciberespionagem* (que incluem intrusões em redes e exploração de acessos privilegiados em redes corporativas e proprietárias) no sentido de adquirir informação que pode dar a esses Estados uma verdadeira vantagem competitiva.²⁴⁸

Embora os casos de *Ciberespionagem* ainda não sejam muito comuns, ou pelo menos são pouco conhecidos do público em geral, a verdade é que este é um tema preocupante para alguns Estados.

Pela quantidade de informação importante, dados pessoais e poder (económico, político, social e até militar) que têm, um dos alvos mais comuns destes ataques são os Estados Unidos da América.

O Congresso norte-americano recebeu, em novembro de 2011, do *Office of the National Counterintelligence Executive*, um relatório intitulado “Espões estrangeiros roubam segredos económicos americanos no ciberespaço” que acusa diretamente a China e a Rússia de utilizarem técnicas de *Ciberespionagem* para “roubar” segredos económicos a entidades norte americanas.

Nesse relatório afirma-se que os chineses são os “agentes de espionagem económica mais ativos e persistente do mundo” e que os serviços de informações russos executam “um leque de atividades para recolher informação económica e tecnológica de alvos americanos”.²⁴⁹

Esse documento garante que a maior parte destes “roubos de informação” está a ocorrer no *Ciberespaço*, numa tendência que se agravará ao longo dos próximos anos. O que nos leva a crer que nenhum Estado está imune a estes ataques.

À medida que a informação referente às áreas económica, política e social dos Estados emerge no *Ciberespaço* é fácil de perceber o seu valor não só material, mas também político, militar, já que certas informações podem consubstanciar atos terroristas.

²⁴⁸ Pereira, Júlio, “Cibersegurança, O Papel do Sistema de Informações da República Portuguesa”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p. 41.

²⁴⁹ *Idem*, *Op. Cit.*, p.42.

Como tal, será fundamental assegurar, por um lado, que a transferência de informação do “mundo real” para o “mundo virtual” é feita de forma segura, por outro que existem meios de defesa coercivos que impedem o seu uso para atividades criminosas ou terroristas.

3.3. – Ciberguerra/Ciberterrorismo

O fenómeno da *Internet* tem possibilitado uma multiplicidade de serviços e recursos que, como temos vindo a analisar, trazem vantagens e desvantagens para a nossa sociedade, bem como para as infraestruturas e organismos que a compõem.

A partilha eletrónica assume uma importância tão vital que o acesso à *Internet* consubstancia um verdadeiro direito fundamental para os seus utilizadores.²⁵⁰

O impacto que a *Internet* tem na nossa sociedade é ainda mais determinante se pensarmos que os sistemas interligados em rede constituem e integram as estruturas de informação dos Estados, criando um autêntico mundo virtual, o *Ciberespaço*.

Dentro deste *Ciberespaço* existe uma categoria à parte na utilização da *Internet*, um núcleo de informações importante e privilegiado, apenas ao alcance de algumas organizações e instituições. É neste contexto que temos assistido à proliferação de ataques maliciosos destinados a colocar em causa a sobrevivência das sociedades virtuais e em última instância dos próprios Estados, encerrando, em si mesmo, a realização de verdadeiros atos terroristas.²⁵¹ Atendendo à sua natureza, estes atos poderão configurar cenários de materialização de *Ciberterrorismo*.²⁵²

A primeira referência ao conceito *Ciberterrorismo* surgiu em 1996 num artigo escrito por Barry Collin, um investigador sénior do *Institute for Security and Intelligence* na Califórnia, onde referia: “The physical and virtual worlds are inherently disparate worlds. It is now the intersection, the convergence, of these two worlds that forms the vehicle of Cyber Terrorism, the new weapon that we face.”²⁵³

Em 1999, o Major Bill Nelson da Força Área dos Estados Unidos da América definiu *Ciberterrorismo* como: “Cyber-terrorism is the calculated use of unlawful violence

²⁵⁰ Alguns estados reconhecem o acesso à *Internet* como um direito humano: Espanha, Estónia, Finlândia, França e Grécia. Galdes, Ana Vaz, “Ciberterrorismo: cenário de materialização”, in *Revista da Faculdade de Direito da Universidade de Lisboa*, Coimbra, vol.53 n.º1-2, 2012, p.42, *apud.*, Eksted, V./Parkhouse, T./Clemente, D., *Commitments, mechanisms & governance*, 2012, in Ed. Klimburg, A., *NATO National Cyber Security Framework Manual*. p. 164, nota 516.

²⁵¹ Galdes, Ana Vaz, “Ciberterrorismo: cenário de materialização”, in *Revista da Faculdade de Direito da Universidade de Lisboa*, Coimbra, vol.53 n.º1-2, 2012, p.43.

²⁵² *Idem*, *Ibidem*.

²⁵³ Gelbstein, Eduardo, “The War of Attrition in Cyber-Space or “Cyber-Attacks”, “Cyber-War” and “Cyber-Terrorism”, in “Conselho de Segurança da ONU”, *idn Nação e Defesa*, Instituto de Defesa Nacional, n.º135, p. 118, *apud.* Collin, Barry, *The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge*, 1996.

against digital property to intimidate or coerce governments or societies in the pursuit of goals that are political, religious or ideological.”²⁵⁴

Atualmente, o conceito de *Ciberterrorismo* é facilmente definido como a atividade terrorista praticada através do *Ciberespaço*, sendo este usado como meio ou como fim.²⁵⁵

O *Ciberespaço* pode ser utilizado de duas formas, na prática de terrorismo:

- A primeira é como meio auxiliar, isto é, as chamadas *ciberactividades*, auxiliares à prática de terrorismo, como a propaganda, recrutamento, comunicações, recolha de dados, divulgação de informação, operações bancárias e de financiamento, transações comerciais, aquisição e fornecimento de bens e serviços, transporte de pessoas e bens, entre outros exemplos;
- A segunda, como meio ou objeto direto de ataque terrorista^{256 257}.

Da mesma forma, a conceptualização do *Ciberterrorismo* resulta da conjugação de dois elementos, objetivo e subjetivo, havendo uma dupla vertente no elemento objetivo: primeiro trata-se de um ato praticado por via informática, lícito ou ilícito, o qual pode conduzir, ou não, a uma segunda vertente objetiva, caso ocorra: tomada de reféns, atos criminosos cometidos com a intenção de causar morte, destruição de infraestruturas críticas, entre outros exemplos.²⁵⁸

Quanto ao elemento subjetivo, é necessário que tenha como propósito fundamental desestabilizar gravemente ou destruir as estruturas fundamentais políticas, constitucionais, económicas ou sociais de um país ou de uma organização internacional.²⁵⁹

²⁵⁴ Nelson, Bill, et al., *Cyberterror, Prospects and Implications*, Center for the Study of Terrorism and Irregular Warfare, 1999.

²⁵⁵ Gerald, Ana Vaz, “Ciberterrorismo: cenário de materialização”, in *Revista da Faculdade de Direito da Universidade de Lisboa*, Coimbra, vol.53 n.º1-2, 2012, p.55.

²⁵⁶ Sobre as opções que o *ciberespaço* oferece aos terroristas, Kamal, A., *The Law of Cyberspace an invitation to the table of negotiations*, United Nations Institute of Training and Research, October, 2005, pp. 67-69.

²⁵⁷ Gerald, Ana Vaz, “Ciberterrorismo: cenário de materialização”, in *Revista da Faculdade de Direito da Universidade de Lisboa*, Coimbra, vol.53 n.º1-2, 2012, p.55.

²⁵⁷ *Idem, Ibidem.*

²⁵⁸ *Idem, Op. Cit.*, p. 56.

²⁵⁹ *Idem, Ibidem.*

Como refere Dorothy Denning, o “Ciberterrorismo é a convergência de terrorismo e de ciberespaço. É geralmente entendido como significando ataques ilícitos e ameaças de ataques, contra computadores, redes e a informação aí armazenada, quando feito para intimidar ou coagir um governo, ou as pessoas, na prossecução de objectivos políticos ou sociais. Para além disso, para qualificar um ataque como ciberterrorismo, este deve resultar em violência contra pessoas ou propriedade, ou pelo menos, causar dano suficiente para gerar medo. Ataques que levem à morte ou dano físico, explosões, quedas de aviões, contaminação de água, ou graves perdas económicas serão exemplos. Ataques sérios contra infraestruturas críticas podem ser ataques de ciberterrorismo, dependendo do seu impacto. Ataques que afectem serviços não essenciais, ou que constituíam apenas prejuízo sem outra gravidade que a material, não o são.”²⁶⁰

Não obstante as várias definições do conceito de *Ciberterrorismo*, não existe neste domínio enquadramento jurídico específico para a definição e criminalização de atos terroristas praticados através do *Ciberespaço*, quer em instrumentos nacionais quer em internacionais.

A *Internet* tem uma grande influência no aumento destes ataques, já que facilita a divulgação da oferta de serviços de pirataria mercenária, por exemplo, por parte de *crackers* russos, especializados na realização de ataques que consigam bloquear páginas na rede, os chamados ataques de negação de serviço (*Denial of Service*).²⁶¹

De igual forma, a *Internet* tem sido usada como elo de ligação entre os vários grupos de terroristas espalhados pelo mundo, como forma de transmitir as suas mensagens, recrutar aliados e definir estratégias.

Noutra perspetiva, foi divulgado que o governo da Coreia do Norte deu formação a centenas de *hackers*, tendo em vista a sua participação em eventuais guerras virtuais contra países estrangeiros, na maioria dos casos contra os Estados Unidos da América. Segundo a mesma fonte, esta formação foi de nível universitário, com componentes

²⁶⁰ Denning, Dorothy, *Cyberterrorism, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services*, US House of Representatives, 23 May 2000. The Terrorism Research Center, p. 1, <http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf> Neste sentido, cf. O’ Hara, T.F., *Cyber warfare/Cyber Terrorism*, U.S. Army War College Strategic Research Project, p. 14. Em sentido diverso, cf. Gabriel Weimann entende que *Ciberterrorismo* significa apenas: “a utilização de instrumentos de redes de computadores para fechar, ou danificar, infraestruturas críticas nacionais (como energia, transportes, operações governamentais)”. Weimann, Gabriel, *Cyberterrorism: The sun of all fears?*, 28 Studies, in conflict and Terrorism 129, pp.132-133.

²⁶¹ Verdelho, Pedro, “Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º 6, Julho-Dezembro 2005, p.161.

especificamente dirigidos à prática de atos de intrusão em sistemas informáticos estrangeiros.²⁶²

Perante estes desenvolvimentos, alguns Estados criaram “cyber armies” com capacidades defensivas e ofensivas, isto é, grupos militares especializados em ciberataques.

Face à utilização de armas informáticas para a condução de planos de defesa e segurança refere-se, na estratégia de *cibersegurança* da Austrália, o seguinte: “Estão a ser contemplados ataques a sistemas críticos de computadores, tanto no sector público como no privado, como uma forma alternativa de condução de guerra e um meio através do qual criminosos, grupos terroristas e serviços de *intelligence* hostis poderão causar danos aos interesses nacionais.”²⁶³

Os especialistas indicam que um ataque estruturado a uma infraestrutura crítica requer entre dois a quatro anos de preparação. Contudo, e apesar dos custos inerentes a estas operações, atualmente há uma geração ativa de novos terroristas já familiarizados com as tecnologias informáticas. Por outro lado, há nações identificadas como patrocinadoras de atividades terroristas, que poderão querer também intervir.²⁶⁴

O âmbito e o grau dos danos causados por um ciberataque são indicativos das capacidades e objetivos dos *ciberterroristas*. Na análise técnica desta matéria, são habitualmente categorizados três níveis de ataque:

1. Ataques básicos - intentados a partir de um ponto único, contra sistemas individuais, através de instrumentos criados por outras pessoas. Nestes casos, o ataque é limitado em duração e consequências;
2. Ataques estruturados - que implicam a capacidade de atacar sequencialmente múltiplos sistemas, a partir de diferentes localizações, e de modificar ou criar

²⁶² Diário Digital de 7 de outubro de 2004.

²⁶³ Geraldine, Ana Vaz, “Ciberterrorismo: cenário de materialização”, in *Revista da Faculdade de Direito da Universidade de Lisboa*, Coimbra, vol.53 n.º1-2, 2012, p.62, *apud*. Australian Government, *Cyber Security Strategy*, Commonwealth of Australia, 2009, p. 3. Sobre a utilização da informática como arma de guerra ver: Owen, R.S., *Infrastructures of Cyber Warfare*, 2007, in Janczewski, L./Andrew, M.C., *Cyberwarfare and Cyberterrorism*, USA/UK: IGI, pp. 35-41; Nugent, J.H./Raisinghani, M., *Bites and Bytes vs. Bullets and Bombs: A New Form of Warfare*, in Janczewski, L./Andrew, M.C., *Cyberwarfare and Cyberterrorism*, USA/UK: IGI, pp. 26-34.

²⁶⁴ Em outubro de 2004 foram identificados pelo Departamento de Estado Norte Americano, os seguintes países patrocinadores de atividades terroristas: Cuba, Irão, Iraque, Líbia, Coreia do Norte, Síria, Sudão. Council of Europe, *Cyberterrorism – the use of the Internet for terrorist purposes*, 2007, pp.44 e 45.

instrumentos para esse efeito. Nestes casos, o ataque terá como alvo vulnerabilidades específicas e objetivos específicos. Estes ataques requerem organização e recursos. A recuperação e defesa dependerão de peritos na matéria.

3. Ataques coordenados - são perpetrados a partir de diferentes localizações, com danos muito elevados. Este tipo de ataque requer organização estruturada, sofisticação, capacidade de análise das vulnerabilidades dos alvos, de suplantar sistemas de defesa heterogêneos e de criar instrumentos de ataque únicos e específicos para os fins pretendidos.²⁶⁵

O ciberataque de negação de serviço, *Distributed Denial of Service*, que a Estónia sofreu em abril de 2007, tem sido enquadrado no âmbito da *Ciberguerra* e do *Ciberterrorismo*²⁶⁶ e é um exemplo de um ataque estruturado.

O ataque foi efetuado através de *botnets*, localizadas em diversos países, que durante semanas enviaram comandos simultâneos de acesso a *websites* governamentais da Estónia, por volta das 2000 visitas por segundo, em vez das usuais 1000 por dia. Como consequência houve uma paralisação dos sistemas informáticos das instituições do Estado e de computadores pessoais de particulares. Apesar de existirem suspeitas do envolvimento da Rússia neste ataque, a investigação efetuada pelas autoridades levou apenas à condenação de um indivíduo de nacionalidade russo-estoniana, que teria operado um ataque através do seu computador pessoal na Estónia. A motivação deste ataque terá sido política e relacionada com a alteração da localização de um monumento russo na Estónia, que consagrava o combate da Rússia aos nazis na II Guerra Mundial.²⁶⁷

²⁶⁵ Geraldine, Ana Vaz, “Ciberterrorismo: cenário de materialização”, in *Revista da Faculdade de Direito da Universidade de Lisboa*, Coimbra, vol.53 n.º1-2, 2012, pp.59 e 60. Sobre as categorias de ataque, O’Hara, T.F., *Cyber warfare/Cyber terrorism*, U.S. Army War College Strategic Research Project, 2004, pp. 14-16.

²⁶⁶ Outro exemplo é o caso do ataque que a Geórgia sofreu em agosto de 2008. E ainda os ataques à Bielorrússia. Geers, K., *Strategic Cyber Security*, NATO Cooperative Cyber Defence Centre of Excellence, 2011, pp. 72-80; e entre os Estados Unidos da América e a China. *Idem*, *Op. Cit.*, p. 83. Com referências a outros exemplos, Walker, C., *Cyber terrorism: legal principle and law in the United Kingdom*, Center for Criminal Justice Studies, School of Law, University of Leeds, 2006, p.635.

²⁶⁷ Geraldine, Ana Vaz, “Ciberterrorismo: cenário de materialização”, in *Revista da Faculdade de Direito da Universidade de Lisboa*, Coimbra, vol.53 n.º1-2, 2012, pp.63 e 64. A este propósito a estratégia de Cibersegurança da Estónia, em Estonia Ministry of Defence, *Cyber Security Strategy*, 2008. Tallinn: *Cyber Security Strategy Committee*; e Wilson, C., *CRS Report for Congress, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Police Issues for Congress*, January 2008, pp. 7 e 8.

Nos últimos anos tornou-se óbvio que o *Ciberespaço* tem um lado negro que pode e tem vindo a ser usado para a prática de novos atos criminosos, desde o envio de vírus informáticos até aos casos mais graves de criminalidade organizada.

Empresas, governos e outras entidades são os alvos preferidos de ataques de terceiros com o intuito de penetrarem nas suas redes de dados e sistemas de informação. Estes grupos de cibercriminosos vão desde os adolescentes a grupos de criminalidade organizada extremamente competentes.

Para além das vulnerabilidades e das fraquezas informáticas de carácter técnico, o *Ciberespaço*, dadas as suas características, é propício à prática de atividades terroristas, já que se trata de um meio onde se pode agir anonimamente ou adotando uma outra identidade, com baixo custo, e sem fronteiras ou barreiras físicas.

Ao longo dos anos têm acontecido vários ataques potencialmente ligados ao *Ciberterrorismo*:

- A 14 de agosto de 2003, ocorreu um enorme apagão que abrangeu 65 milhões de pessoas no Canadá e no Leste dos Estados Unidos. Relatos oficiais revelaram que “a causa deste acontecimento não se deveu a ataques terroristas”, mas sim a uma combinação de fatores, incluindo erros informáticos.²⁶⁸
- A 28 de agosto de 2003, um apagão afetou o sul de Londres e Northwest Kent. A explicação oficial referia a ocorrência de duas falhas independentes com um espaço de 7 segundos entre elas.²⁶⁹
- A 28 de setembro de 2003, ocorreu um enorme apagão que afetou toda a Itália (com exceção das ilhas Sardenha e Capri) e prejudicou 56 milhões de pessoas.²⁷⁰ Também uma parte da Suíça foi afetada durante várias horas. A explicação oficial referia falhas resultantes de uma tempestade.²⁷¹

Para todos estes casos foi afastada a ligação ao *Ciberterrorismo*. No entanto, são um bom exemplo de como este tipo de ataques pode ter um impacto extremamente negativo na sociedade e nas suas infraestruturas. Importa referir que caso se tratasse de

²⁶⁸ Gelbstein, Eduardo, “The War of Attrition in Cyber-Space or “Cyber-Attacks”, “Cyber-War” and “Cyber-Terrorism”, in “Conselho de Segurança da ONU”, *idn Nação e Defesa, Instituto de Defesa Nacional*, n.º135, p.126.

²⁶⁹ *Idem, Ibidem.*

²⁷⁰ *Idem, Ibidem.*

²⁷¹ *Idem, Ibidem.*

ciberataques, envolvendo sofisticado *malware*, seria muito mais difícil de diagnosticar e reparar os danos causados.

Segundo a Unidade Nacional Contra o Crime de Alta Tecnologia, do Reino Unido, ainda não foi possível estabelecer qualquer ligação entre a produção e difusão de vírus informáticos e as atividades de terrorismo. Não obstante, a possibilidade existe.²⁷²

Sabe-se, também, que os terroristas que desviaram os aviões que provocaram os atentados de 11 de setembro de 2001, comunicaram entre eles por via de contas de correio eletrónico, abertas em servidores de *webmail*.

A possibilidade de intrusões terroristas em centros ou infraestruturas militares, resultando no controlo de forças militares e de armas²⁷³, é outra das preocupações em termos de *Ciberguerra* e *Ciberterrorismo*.

Não existem dados estatísticos que determinem a efetiva dimensão da utilização do *Ciberespaço* por terroristas²⁷⁴ e qual a proporção desta atuação. Podemos apenas confirmar o aumento dos casos de *Cibercrime*, bem como o aumento dos custos para a sociedade, que ultrapassa, a nível global, os custos do crime tradicional.

Legisladores, políticos e diplomatas têm procurado estabelecer conceitos e definições sobre este tema, mas, apesar da assinatura da Convenção do Conselho da Europa sobre Cibercrime em 2001 por vários Estados, não foram criados novos desenvolvimentos desde então.²⁷⁵

Face ao exposto e perante este novo tipo de criminalidade, é importante colocar uma questão: “pode um ciberataque ser considerado um ato de guerra?”²⁷⁶ A resposta a esta questão dependerá dos futuros desenvolvimentos tecnológicos. Por um lado, os efeitos

²⁷² Verdelho, Pedro, “Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º 6, Julho-Dezembro 2005, p.160.

²⁷³ Por exemplo, o lançamento de um míssil ou o bloqueio de comunicações militares em situação de guerra. Galdes, Ana Vaz, “Ciberterrorismo: cenário de materialização”, in *Revista da Faculdade de Direito da Universidade de Lisboa*, Coimbra, vol.53 n.º1-2, 2012, p. 61.

²⁷⁴ Galdes, Ana Vaz, “Ciberterrorismo: cenário de materialização”, in *Revista da Faculdade de Direito da Universidade de Lisboa*, Coimbra, vol.53 n.º1-2, 2012, p. 57, *apud*. Cf. A referência a um programa de *software* designado “o programa eletrónico da jihad informática”, divulgado por diversas plataformas informáticas de organizações jihadistas, em Council of Europe, *Cyberterrorism – the use of the Internet for terrorist purposes*, 2007, p. 34, nota 88.

²⁷⁵ Gelbstein, Eduardo, *The War of Attrition in Cyber-Space or “Cyber-Attacks”, “Cyber-War” and “Cyber-Terrorism”*, in “Conselho de Segurança da ONU”, *idn Nação e Defesa*, Instituto de Defesa Nacional, n.º135, p.116.

²⁷⁶ Freire, Vicente, “Cibersegurança e Ciberdefesa: A Inevitabilidade de Adoção de uma Estratégia Nacional”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p. 62.

de um ciberataque tenderão a aumentar o nível de sofrimento humano e os danos económicos que provocarão. No entanto, não é claro dizer que um ciberataque é um ato de guerra, pois as ferramentas e técnicas da *Ciberspionagem* são na maioria das vezes as mesmas que as de um ciberataque. As diferenças entre ambos estão na motivação: num caso, roubar; no outro, é um prelúdio para guerra.²⁷⁷

²⁷⁷ Freire, Vicente, “Cibersegurança e Ciberdefesa: A Inevitabilidade de Adoção de uma Estratégia Nacional”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p. 62.

4. – Tipologia

O fenómeno da criminalidade informática foi, em primeiro lugar, associado à questão da compatibilização do direito dos cidadãos exercerem as suas liberdades e de verem respeitados os seus direitos, nomeadamente, o direito à privacidade, com a necessidade da sociedade recolher informações sobre os indivíduos que a compõem, com vista ao seu melhor funcionamento e segurança.²⁷⁸

Como pudemos verificar pelo exposto nos pontos anteriores, não existe um conceito de criminalidade informática expressamente consagrado na legislação, ou uniformemente sedimentado na doutrina e jurisprudência. Não obstante, entendem alguns autores, como Garcia Marques e Lourenço Martins²⁷⁹, que “é frequente encarar a criminalidade informática como todo o acto em que o computador serve de meio para atingir um objectivo criminoso ou em que o computador é o alvo simbólico desse acto ou em que o computador é objecto do crime.”²⁸⁰

Ainda sobre este assunto, Garcia Marques e Lourenço Martins, interpretam o conceito de criminalidade informática em sentido amplo e em sentido estrito. Assim, “Em sentido amplo, então, a criminalidade informática englobará toda a panóplia de actividade criminosa que pode ser levada a cabo por meios informáticos, ainda que estes não sejam mais que um instrumento para a sua prática, mas que não integra o seu tipo legal, pelo que o mesmo crime poderá ser praticado por recurso a outros meios. Em sentido estrito, entenderemos nós que a criminalidade informática abarcará apenas aqueles crimes em que o elemento digital surge como parte integrador do tipo legal ou mesmo como seu objecto de protecção.”²⁸¹

Nos pontos seguintes iremos desenvolver alguns tipos de crimes ligados à criminalidade informática que merecem destaque, quer pela sua frequência, quer pela sua gravidade.

²⁷⁸ Venâncio, Pedro Dias, *Lei do Cibercrime, Anotada e Comentada*, Coimbra Editora, grupo Wolters Kluwer, Portugal, 2010, p.13.

²⁷⁹ Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2ª ed., Refundida e Actualizada, Almedina, Coimbra, 2006, pp.639 e ss.

²⁸⁰ Venâncio, Pedro Dias, *Lei do Cibercrime, Anotada e Comentada*, Coimbra Editora, grupo Wolters Kluwer, Portugal, 2010, p.16.

²⁸¹ *Idem, Op. Cit.*, p. 17.

4.1. - Criminalidade contra a privacidade

Como vimos supra, as características do *Ciberespaço*, anónimo, global e transnacional, têm uma influência negativa em vários aspetos da sociedade, entre eles, na privacidade dos cidadãos.

Se outrora se protegia a todo o custo o “direito à reserva da vida privada”, hoje em dia, tal já não acontece. Graças ao uso das novas tecnologias, assistimos, cada vez mais, ao excesso de partilha de informação pessoal e privada, pondo em causa um conceito que será cada vez mais escasso, o *direito ao anonimato*. Embora não se trate de um Direito propriamente dito, podemos considerar que se trata de um direito pessoal que a todos é conferido, como uma opção por resguardar a sua vida privada.

A navegação pela *Internet* exige sempre um acesso identificado, pelo que é difícil navegar no espaço digital sem que se seja reconhecido. É, contudo, lícito o recurso ao anonimato, quando usado para proteger determinadas informações e prevenir e garantir que não caiam nas mãos erradas ou que certa informação seja usada de forma indevida, pondo em causa a segurança das pessoas.

Na *Internet*, o direito de não ser reconhecido, o direito de não se identificar e nem ser identificado é constantemente violado com a adição de pequenos ficheiros, presentes nos sítios, denominados *cookies*, que registam e gravam a atividade do utilizador. Estes ficheiros permitem conhecer o rasto de navegação, as preferências, as consultas efetuadas, o período de permanência na *Internet*, o local de acesso (endereço de *IP*, número de telefone usado para aceder, entre outros). Por outro lado, estas informações podem e são manipuladas por empresas de marketing e de recursos humanos para fins comerciais, mas também por organismos estatais e utilizadores com objetivos ilícitos.²⁸²

O mesmo sucede com o “*sistema de chips*” que permite armazenar dados pessoais dos cidadãos, suscetíveis de serem lidos por qualquer aparelho próprio para o efeito²⁸³.

²⁸² Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 519.

²⁸³ Gomes, Mário M. Varges, *O Código da Privacidade e da Protecção de Dados Pessoais na Lei e na Jurisprudência (Nacional e Internacional)*, Coleção direito das novas tecnologias, Centro Atlântico, Portugal, 2006, p.5.

Sendo a *Internet* um lugar onde estamos constantemente a ser observados, consideramos constituir o anonimato um direito inalienável²⁸⁴, sendo suscetível de responsabilidade civil quem divulgar ou utilizar sem autorização todas as informações de caráter pessoal e particularmente do foro íntimo, tais como dados pessoais ou as preferências de cada utilizador, guardadas pelos ficheiros *cookies* nos computadores e que posteriormente são enviados aos gestores dos sítios eletrónicos.

Existem métodos para minimizar a aparência de navegação na *Internet*, nomeadamente programas que protegem e evitam a revelação de dados pessoais a terceiros²⁸⁵. No entanto, estes programas bloqueiam certas funcionalidades dos sítios, não sendo possível visualizar todo o conteúdo e informação disponível.

Como comenta Mário Gomes: “bem necessária e oportuna é esta chamada de atenção para direitos fundamentais da pessoa humana num tempo em que as derivas securitárias decorrentes do 11 de setembro e dos atentados terroristas que se lhe têm seguido perturbam os espíritos e ameaçam destruir uma das mais importantes conquistas da civilização dos nossos dias, fazendo alterar perigosamente o equilíbrio deste binómio sensível: segurança-privacidade.”²⁸⁶

Estas novas e poderosas ameaças surgiram com o desenvolvimento e difusão das tecnologias da informação, com destaque aqui para as grandes bases de dados pessoais (constituídas por informações da mais variada natureza, a que é cada vez mais fácil aceder), para a *Internet* e para os sistemas de videovigilância eletrónica.

A proteção da privacidade e dos dados pessoais é ainda mais importante no que toca à transferência desses dados para países terceiros, nomeadamente, para aqueles países que não ofereçam garantias de um nível de proteção adequada, no contexto da globalização.

²⁸⁴ Parecer n.º13/96 do Conselho Consultivo da Procuradoria Geral da República, publicado no DR, II, n.º286, de 12.12.97, p.15247 ss: “No cruzamento do direito à identidade pessoal, que inclui fundamentalmente o direito à intimidade da vida privada, poder-se-á extrair uma proteção constitucional do anonimato”.

²⁸⁵ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 21.

²⁸⁶ Gomes, Mário M. Varges, *O Código da Privacidade e da Protecção de Dados Pessoais na Lei e na Jurisprudência (Nacional e Internacional)*, Colecção direito das novas tecnologias, Centro Atlântico, Portugal, 2006, p.5.

Hoje em dia, de uma forma constante e mais ou menos minuciosa, são seguidos os nossos passos na *Internet*, procedem-se a escutas “globais” das nossas comunicações²⁸⁷, para além de, diária e constantemente, nos vigiarem ainda nos mais diversos locais e situações²⁸⁸. Por exemplo, os aparelhos de videovigilância são utilizados com a desculpa de ser um meio de proteção, mas são cada vez mais uma ameaça à proteção da vida privada. Sabe-se, publicamente, que quem passeia por Londres, será gravado por uma câmara de videovigilância, em média, a cada cinco minutos²⁸⁹, mas também em espaços fechados, quer seja através de câmaras de vídeo, detetores de som, sensores de consumo de fluidos no interior dos lares (água, eletricidade ou gás), conservação e interceção de comunicações, ou ainda pela localização de pessoas ou veículos, através do *GPS*²⁹⁰.

Também, graças aos desenvolvimentos tecnológicos é possível localizar qualquer aparelho que esteja ligado à *Internet*, já que a maioria dos sítios eletrónicos utiliza a identificação por tecnologias de geo-localização, isto é, trata-se de uma ferramenta que consegue localizar de forma precisa a nossa localização.

Todos estes exemplos demonstram como a sociedade está cada vez mais exposta e a facilidade com que se pode aceder a dados pessoais e informação confidencial. Por conseguinte, é fundamental garantir sanções para o tratamento e a utilização abusiva de dados pessoais informatizados.

Sobre este ponto, o artigo 35.º da Constituição da República Portuguesa prevê a “Utilização da Informática”, onde, de uma forma global, consagra a proteção dos

²⁸⁷ Veja-se o caso mais recente das declarações proferidas por Edward Snowden relativamente às escutas telefónicas feitas pelos Estados Unidos da América a cidadãos e organismos mundiais; o caso do *ECHELON* - uma potente e sofisticada rede de escutas de língua inglesa, ligando os Estados Unidos da América, o Canadá, o Reino Unido, a Austrália e Nova Zelândia, levada a cabo através de vários satélites de comunicações, implantada pelo denominado “*pacto UKUSA*”, permitindo que as escutas relativas a determinadas pessoas (terroristas, por exemplo) sejam ouvidas, quer sejam escutas globais quer sejam escutas sistemáticas - e o *CARNIVORE* - um sistema de escuta do *FBI* que permite intercetar, por filtragem, todo o tráfego da *Internet* que passa pelos fornecedores de acesso. Gomes, Mário M. Varges, *O Código da Privacidade e da Protecção de Dados Pessoais na Lei e na Jurisprudência (Nacional e Internacional)*, Coleção direito das novas tecnologias, Centro Atlântico, Portugal, 2006, p.24.

²⁸⁸ Publicamente reconhecida a impossibilidade de qualquer organismo oficial fornecer dados concretos e rigorosos nesta área, calcula-se que nas ruas, no metropolitano e em estabelecimentos comerciais de França existem cerca de um milhão de câmaras de videovigilância. *Idem, Op. Cit.*, p.25.

²⁸⁹ *Idem, Ibidem.*

²⁹⁰ *GPS* - (*Global Positioning System*) nascido nos Estados Unidos da América, durante a Guerra Fria, para fins militares e destinado a guiar aeronaves e mísseis, é composto por 24 satélites *Navstar*, em seis órbitas diferentes, percorrendo a órbita da Terra em cada 12 horas. O *GPS* é hoje utilizado em múltiplos sistemas de navegação e orientação, da navegação aérea à automóvel e às bombas, sendo agora também utilizado na localização de chamadas de telemóveis. *Idem, Ibidem.*

cidadãos perante o tratamento de dados pessoais informatizados. Da análise deste artigo destacamos a forma abrangente da palavra *tratamento* já que, a mesma engloba não apenas a individualização, fixação e recolha de dados, mas também a sua conexão, transmissão, utilização e publicação; veja-se o exposto no n.º2 do supra referido artigo. Já quanto ao conceito de *dados*²⁹¹, aparece como uma representação convencional de informação, sob a forma analógica ou digital, que possibilita o seu tratamento automático (através da introdução, organização, gestão e processamento de dados). Quanto aos dados pessoais, o enunciado exprime logo a estreita conexão entre estes direitos e o respetivo tratamento informático. Desta forma, podemos afirmar que, quanto mais os dados relacionam a dignidade, a personalidade e a autodeterminação das pessoas, tanto mais se impõem restrições quanto à sua utilização e recolha, nomeadamente, o caso dos bancos de dados.

A Constituição da República Portuguesa, a Carta dos Direitos Fundamentais da União Europeia, as diretivas comunitárias e variada legislação avulsa, têm-se esforçado por confirmar e garantir o cumprimento da proteção da privacidade e dos dados pessoais como um direito fundamental: o uso, e muitas vezes o abuso das novas tecnologias, sempre em nome da segurança, tornam urgente o cumprimento rigoroso das normas que definem os limites de cada um dos valores fundamentais em presença, permitindo assim restabelecer, uma vez mais, o justo equilíbrio no binómio segurança-privacidade.²⁹²

A relação da área da informática com o Direito é inquestionável, já que engloba uma série de direitos, liberdades e garantias que o Direito deve proteger, nomeadamente, o desenvolvimento da personalidade, a dignidade da pessoa humana e a intimidade da vida privada. E é precisamente nestes tipos de direitos que os casos de *Cibercriminalidade* mais se têm feito sentir.

Falamos aqui de uma *Cibercriminalidade* mais comum, se assim pudermos falar, já que são casos ligados aos crimes de difamação e injúria, como por exemplo: devassa e/ou

²⁹¹ Dados informáticos - “qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função”. Definição presente na alínea b), do artigo 2.º da Lei n.º109/2009, de 15 de setembro.

Da mesma forma podemos aqui enquadrar os *dados de tráfego*, são “os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente”. Definição presente na alínea c), do artigo 2.º da Lei n.º109/2009, de 15 de setembro.

²⁹² *Idem, Ibidem.*

exposição da vida privada na *Internet*, calúnias ou furto de identidade. Não obstante, serem considerados casos de menor relevo, a frequência e a amplitude com que começam a ocorrer é motivo de preocupação para o legislador e para o Direito.

Da mesma forma surgem novos tipos de crimes, aliados quer aos meios informáticos quer à amplitude da *Internet*. São o caso do assédio virtual, também conhecido por *Cyberstalking* e as ameaças ou *bulling* virtual, o chamado *Cyberbulling*. Em ambos os casos os agentes atuam através dos meios informáticos: computadores, telemóveis, ou qualquer outro dispositivo com acesso à *Internet* ou possibilidade de enviar e receber mensagens de texto escritas. No entanto, com diferenças significativas.

O *Cyberstalking* é um conceito de origem recente para o qual ainda não existe uma definição certa. No entanto, pode ser definido como um abuso que envolve ameaças e assédio doentio, em que alguém persegue, de uma maneira assustadora e constante, uma outra pessoa através dos meios informáticos.²⁹³

Neste caso, assistimos a um tipo de crime que, apesar de aparentemente inofensivo, já que a vítima não está frente a frente com o agressor e, como tal, pode defender-se ou “fugir” se assim o entender, tem características e contornos que o tornam insuportável para a vítima. À medida que os aparelhos tecnológicos (telemóveis, *tablets*, computadores, etc.) emergem cada vez mais no nosso quotidiano, tornam-se também verdadeiras armas, já que possibilitam saber onde estamos ou o que fazemos a qualquer hora. Assim, enquanto a vítima utiliza os aparelhos tecnológicos no seu dia-a-dia, é constantemente vigiada pelo agressor (na maioria dos casos sem saber).

Em Portugal, ainda são poucos os casos conhecidos de *Cyberstalking*. Contrariamente, nos Estados Unidos da América, o *Cyberstalking* já é mais comum²⁹⁴ e em última instância, chega a consubstanciar verdadeiros atos de rapto.

²⁹³ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 513.

²⁹⁴ *Idem*, *Op. Cit.*, p.514. Um dos primeiros casos de *Cyberstalking* publicitados ocorreu em 1999, em Massachusetts (EUA). “Nancy” entrou numa sala de *chat* de assuntos gerais, onde um dos internautas comentou dizendo que não gostava do *username* escolhido por esta, começando a trocar do mesmo. Nanci defendeu-se e os dois começaram de imediato a discutir nos limites da argumentação. Todas as vezes que Nanci entrava na sala de *chat*, o seu interlocutor estava presente, esperando-a e dirigindo-se a esta sempre de forma agressiva. Numa certa altura, este disse-lhe que tinha contratado uma outra pessoa, também habitual na sala de *chat*, para saber quando a mesma ali entrasse. Mais, tarde começou a revelar informações cada vez mais pessoais sobre Nanci, como quem era o seu pai e onde a mesma vivia e fazendo ameaças à mesma (“não descansaria enquanto ela não tivesse 6 passos de baixo de terra”).

Do ponto de vista jurídico, este é um crime contra a autodeterminação pessoal, que pode ser enquadrado na lei penal portuguesa (embora sem a total abrangência), no crime de ameaça. As páginas *web*, as mensagens de *email*, ou os programas de *chat* podem servir de meio para a prática do crime de ameaça. Nos termos do n.º1 do artigo 153.º do Código Penal, “quem ameaçar outra pessoa com a prática de crime contra a vida, a integridade física, a liberdade pessoal, a liberdade e autodeterminação sexual ou bens patrimoniais de considerável valor, de forma adequada a provocar-lhe medo ou inquietação ou a prejudicar a sua liberdade de determinação, é punido com pena de prisão até um ano ou com pena de multa até 120 dias”.²⁹⁵ Em Portugal, “o procedimento criminal depende de queixa da pessoa ameaçada”, tal como dispõe o n.º2 do supra referido artigo.

O crime de ameaças através da *Internet (Cyberstalking)* é praticado, em regra, por indivíduos que pretendem intimidar, ameaçar ou perturbar outras pessoas, utilizando para tal, os meios tecnológicos e um disfarce de um nome fictício, de um pseudónimo ou de terceiros, por vezes, até de conhecidos da vítima para ganhar a confiança desta. O *stalker* é precisamente o indivíduo que assedia de uma forma persistente a sua vítima, causando-lhe embaraço e/ou medo.²⁹⁶

Dado o aumento de casos quanto a este tipo de crime, é-nos possível traçar alguns factos importantes:

- Os *Cyberstalkers* julgam que atuam sob absoluto anonimato e que nunca serão descobertos;
- Os autores, quando descobertos, a maioria diz que não quiseram dizer o que disseram ou provocar qualquer receio ou medo na vítima;

Horrorizada, Nanci deslocou-se à polícia local, contando o sucedido. No entanto, os polícias não fizeram nada, limitando-se a rir efusivamente, ignorando a própria ameaça de morte.

O agente tornou-se ainda mais agressivo e passou a remeter as mensagens de correio eletrónico dizendo-lhe que tipo de automóvel a mesma conduzia, onde tinha estado naquele dia e o nome da sua mãe. Nanci dirigiu-se à Polícia Estadual, ao Procurador do Distrito e ao Procurador-Geral do Estado. Mas todos apontavam o dedo para os outros, dizendo não podendo ajudá-la.

Finalmente, Nanci contratou um advogado e a imprensa local. Quando apareceu nos canais de Televisão o Procurador Distrital passou a acompanhar o caso, tendo finalmente deduzido a acusação contra o *Cyberstalker*. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 514.

²⁹⁵ *Acórdão RC, 24.04.1996, BMJ, 456*, p.511- “Só a pessoa a quem se comina um mal futuro se pode considerar vítima de um crime de ameaças”.

²⁹⁶ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 515.

- A maioria dos casos não sucede entre pessoas conhecidas, mas entre pessoas completamente desconhecidas;
- O maior número de vítimas é do sexo feminino (mais de 80%);
- O *Cyberstalking* atinge 5% dos utilizadores de salas de *chat-room* ou de serviços de mensagens instantâneas.²⁹⁷

Assim, para evitar o assédio ou ameaças pela *Internet*, é conveniente que os utilizadores se previnam e transmitam o mínimo de informação pessoal na *Internet*. Da mesma forma, será importante fazer referência a algumas sugestões (nossas e de alguns autores²⁹⁸), para evitar este tipo de ameaça:

- Use a sua conta de *correio eletrónico* apenas para mensagens dirigidas ou a receber de pessoas em quem conheça e tenha confiança;
- Obtenha uma conta de correio eletrónico gratuita, mas certificada, por exemplo: *Hotmail.com*, *Gmail.com*, etc., já que oferecem uma maior segurança quanto ao seu conteúdo e à informação que é partilhada/recebida e utilize-a para as suas atividades e contatos pela *Internet*.
- Apague a sua conta caso suspeite que esteja a ser usada indevidamente por outrem (por exemplo: normalmente quando foi vítima de uso indevido começa a receber várias mensagens de *spam*²⁹⁹ ou mensagens de proveniência duvidosa; as mensagens que envia não são entregues ou não recebe as mensagens que lhe enviam, entre outras situações anómalas). De preferência crie uma conta nova com nome e palavra-passe completamente diferentes da anterior;
- Mude a sua palavra-passe de tempos-a-tempos (por exemplo, de 4 em 4 meses) e utilize letras maiúsculas e minúsculas, bem como números e caracteres, para que seja mais difícil descobrirem a sua palavra-passe e aceder à sua conta.
- Utilize, de preferência, uma palavra-passe diferente para cada conta que tenha.

²⁹⁷ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 515.

²⁹⁸ Com algumas alterações nossas, estas sugestões encontram-se presentes no *Compêndio Jurídico da Sociedade da Informação. Idem, Op. Cit.*, p.56.

²⁹⁹ *Spam* - Toda e qualquer correspondência eletrónica não solicitada e/ou não autorizada. *Idem, Op. Cit.*, p. 1042.

- Evite utilizar o seu nome ou data de nascimento na palavra-passe, pois são elementos fáceis de descobrir por parte dos cibercriminosos;
- Defenda a sua conta não preenchendo os campos de identificação secundários tais como: data de nascimento, telefone, morada, local de trabalho, ou outras informações mais pessoais, que possam dar acesso ao seu dia-a-dia;
- Opte por um *nickname*, pseudónimo, alcunha, etc., nas salas de conversação *online* (salas de chat);
- Evite o uso de *webcams* com utilizadores que não conhece e sempre que possível tape a lente da câmara³⁰⁰, principalmente se tiver crianças;
- Utilize programas de bloqueio de informação não solicitada ou proceda à filtragem manual de mensagens indesejadas;
- Caso seja provocado numa sala de conversação ou comunidade virtual, não responda, pois é exatamente essa a reação que o provocador pretende.
- Se a provocação continuar procure seguir os seguintes passos:
 1. Dirija-se ao provocador, solicitando que deixe de o contactar, em virtude de não pretender qualquer conflito entre ambos;
 2. Contacte o provedor de acesso ao provocador (*ISP* de acesso à *Internet*, serviço de email ou de *chat*) e reencaminhe as mensagens da autoria do provocador, solicitando uma ação em conformidade;
 3. Se a provocação continuar ou se tornar mais obsessiva, contacte a Polícia ou a Guarda Nacional Republicana local. Em casos mais graves, contacte a Polícia Judiciária ou o Ministério Público.
 4. Por fim contacte um advogado.³⁰¹

Quanto ao *Cyberbullying* é um fenómeno em que alguém, através dos meios tecnológicos, humilha e critica outro de forma sistemática e constante, a ponto de trazer consequências para a saúde mental e física dessa vítima, nomeadamente: problemas de

³⁰⁰ Atualmente existem programas que conseguem aceder e ligar remotamente as câmaras dos computadores dos utilizadores, filmando-os enquanto estão ao computador, sem o seu consentimento.

³⁰¹ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 516.

autoestima, depressão, doenças como anorexia e bulimia, e em casos extremos, tentativas ou mesmo atos de suicídio.

A palavra *Cyberbullying* divide-se em duas partes:

- *Cyber* porque o fenómeno acontece num meio tecnológico;
- *Bullying* ocorre “quando se pensa existir perseguição e humilhação prolongada por parte de uma ou mais pessoas que se servem do seu poder para intimidar outro mais fraco que passa a ser vítima num relacionamento em que, precisamente o poder e a desigualdade dificultam que a última se proteja”³⁰².

Em Portugal, e um pouco por toda a Europa, o conceito de *Cyberbullying* começa já a ser conhecido, tornando-se cada vez mais comuns os casos deste fenómeno nos mais jovens. Nos Estados Unidos da América, este conceito apresenta proporções extremas, sendo tão comum que vários estados norte-americanos estão a aprovar legislação para o criminalizar.

Há várias situações que consubstanciam crimes e isso é algo que muitas pessoas, na grande maioria os jovens, não sabem. O que pode começar numa simples brincadeira, um simples comentário pode rapidamente dar origem a algo sério, um crime até. Por exemplo: um simples comentário numa página do *Facebook* pode hoje em dia, desencadear vários outros comentários, boatos, ameaças, perseguições, que em casos extremos podem levar ao homicídio/suicídio de alguém. E é precisamente neste ponto que se centra a grande questão do *Cyberbullying*.

Com o aparecimento e uso das novas tecnologias, nomeadamente das redes sociais, fenómenos como o *Cyberbullying*, tornam-se muito frequentes.

A *Internet* traz uma realidade diferente, pois, contrariamente aos *media* tradicionais em que os jovens eram meros recetores, agora são eles os criadores de conteúdos, falsos ou verdadeiros. Muitas vezes pensam que atuam impunemente e que, ao entrarem numa conta de terceiros, ao tirarem e usarem sem autorização a fotografia ou a página pessoal de uma pessoa, ou ao criarem um perfil falso, não cometem qualquer crime, o que não é verdade.

³⁰² Ana Tomás de Almeida, Psicóloga, “Cyberbullying” [Em linha]. Disponível em <http://pplware.sapo.pt/informacao/cyberbullying-o-que-como-combater/> (consultado em 2.11.2015).

Os casos mais preocupantes são os de vingança, cada vez mais comuns, de colocação de imagens íntimas na *Internet*, comentários proferindo verdadeiras humilhações que, graças ao carácter global da *Internet*, tomam proporções extremas.

“Cyberbullying é, segundo Belsey, o uso e difusão de uma informação para fins difamatórios, em formato electrónico, através de meios de comunicação como e-mail, SMS, MSN ou Redes Sociais (FaceBook, Hi5, etc.), em plataformas electrónicas, de difusão de conteúdos, onde um indivíduo ou grupo pretendem, de forma deliberada e repetida, causar mal-estar a outro.”³⁰³

A grande diferença entre o *Bullying* e o *Cyberbullying* é que neste último caso o agressor profere as ofensas no anonimato, através do uso do computador, adotando a identidade de qualquer pessoa, enquanto no *Bullying*, as ofensas são proferidas cara a cara. No entanto, em ambos os casos, as crianças e jovens são os alvos mais suscetíveis a tais ameaças.

Nas palavras de Ana Tomás de Almeida, alguns dos possíveis sinais são:

- “Isolamento;
- Decréscimo no rendimento académico ou profissional, ou aumento das horas de estudo (atenção virada para uma tarefa);
- Não querer estar com amigos e colegas;
- Não querer sair de casa;
- Não atender o telefone;
- Outros.”³⁰⁴

Perante a presença de algum destes sinais, os responsáveis pelas crianças e jovens devem ser avisados para que possam tomar as medidas necessárias.

Destacamos também o portal do *Bullying*, que disponibiliza toda a informação necessária sobre este tema: <http://www.portalbullying.com.pt/>.

Existem medidas, sugeridas por psicólogos e por agentes de segurança nacional, que se podem realizar para combater este tipo de agressão, que, ao mais pequeno sinal, devem ser de imediato acionadas. São elas:

³⁰³ Ana Tomás de Almeida, Psicóloga, “Cyberbullying” [Em linha]. Disponível em <http://pplware.sapo.pt/informacao/cyberbullying-o-que-como-combater/> (consultado em 2.11.2015).

³⁰⁴ *Idem, Ibidem.*

- *Reportar a agressão*, disponibilizada em quase todos os sítios; esta opção permite comunicar com a entidade que criou o sítio que algum conteúdo é difamatório, ou que algo não está de acordo com os termos e regras estabelecidas;
- *Colocar o computador num local comum*; não evita de todo os riscos, mas faz com que consiga perceber por que sítios os seus filhos navegam;
- *Não partilhar dados pessoais*, como já referimos; a *Internet* é um lugar muito público, a que todas as pessoas, bem ou mal intencionadas, têm acesso. Como tal, a partilha de informação deve cingir-se ao indispensável;
- *Guardar as mensagens de Cyberbullying*; embora seja difícil guardar mensagens desagradáveis e com ofensas, devem ser guardadas para que possam servir, futuramente, como prova;
- *Mudar de email ou de conta da sua rede social*; quando sentir que estão a usar a sua conta de correio eletrónico, ou alguma das suas redes sociais, mude as palavras-passe das mesmas para nomes completamente diferentes.
- *Utilizar programas de bloqueio de informação não solicitada* ou proceder à filtragem manual de mensagens indesejadas;
- Tal como no *Cyberstalking*, não se mostrar através de *webcams* com utilizadores que não conhece e sempre que possível tapar a lente da câmara, principalmente se tiver crianças/jovens.

Como utilizadores da *Internet*, somos todos potenciais vítimas. Temos como exemplo as revelações do antigo analista informático norte-americano Edward Snowden de que a Agência de Segurança Nacional dos Estados Unidos da América realizava e continua a realizar escutas e controla *emails*, violando a privacidade de milhões de pessoas em todo o mundo.

De igual forma, somos também potenciais criminosos, por exemplo: furto de identidade, envio de mensagens *spam*, envio de vírus informáticos, etc. E são várias as tentativas com que todos os dias somos confrontados: falsos *emails* que anunciam prémios, ofertas de viagens, confirmações de contas bancárias, confirmações de compras *online*, entre outros exemplos.

Em conclusão, podemos dizer que a proteção da privacidade passa em primeiro lugar pela sensibilização do utilizador. Para todas estas situações, só depende de nós próprios

tomar uma posição defensiva quanto à *Internet* e, para tal, é preciso estar bem informado, sabendo os perigos que esta comporta e como atuar ou se defender em cada situação, sem descurar as vantagens que a *Internet* nos pode oferecer.

4.2. - Crimes Informáticos

É certo que a *Internet*, enquanto meio de comunicação e transmissão de informação a que temos feito referência, expande-se a um ritmo alucinante e pode ser usada para fins proveitosos e pacíficos, mas também criminosos.

Face a determinados atos, podem ser postos em risco desde os interesses fundamentais de um país, por exemplo, através da preparação de atentados aos seus governantes e instituições, passando pelas infrações à moral pública ou à boa reputação das pessoas, ou como meio para a prática de criminalidade internacional organizada, até aos casos de fraudes informáticas e violação da propriedade intelectual.³⁰⁵

Os crimes informáticos são cada vez mais frequentes e diversificados. A esta categoria pertence uma série de tipos de crime, como por exemplo: a burla informática, falsidade informática, *blackboxing* e *blueboxing*, “carding”, transmissão de vírus pela *Internet*, acesso ilegítimo, interceção ilegítima e espionagem, bem como pirataria informática.

Estes crimes têm como característica comum a conduta lesiva, a qual não necessita corresponder à obtenção de uma vantagem ilícita. Nestes casos, o bem jurídico protegido são os dados e recursos oferecidos por um sistema de processamento de dados, (compilação, armazenamento ou transmissão dos mesmos). Assim, estes crimes pressupõem dois elementos indivisíveis: por um lado, que sejam praticados contra os dados que estejam preparados as operações do computador e, por outro, através do computador, utilizando o *software* e o *hardware* do mesmo para os praticar.³⁰⁶

Vários tipos legais de crimes previstos no Código Penal, nomeadamente nos artigos 180.º a 188.º, podem entrar ainda em conexão com a informática, como é o caso da difamação e injúria contra pessoas singulares ou a ofensa à memória de pessoa falecida ou a pessoa colectiva, organismo ou serviço, podem ser feitas verbalmente, mas também por escrito, gestos, imagens ou qualquer outro meio de expressão.³⁰⁷

Como destacam Garcia Marques e Lourenço Martins, ainda que não se considerasse meio escrito, o correio eletrónico, a inscrição num sítio, num *blog*, num grupo de

³⁰⁵ Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2.ª ed. Refundida e Actualizada, Almedina, Coimbra, 2006, p.656.

³⁰⁶ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 519.

³⁰⁷ Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2.ª ed. Refundida e Actualizada, Almedina, Coimbra, 2006, p.679.

discussão ou numa Base de Dados, entre outros, não poderia deixar de ser entendido como uma outra forma ou meio de expressão.³⁰⁸

Uma injúria pode também manifestar-se através da imagem, e a ofensa resultará normalmente agravada se for transmitida através de um sistema informático ou de uma rede informática, ambiente especialmente propício a facilitar a sua divulgação, tal como prevê o artigo 183.º, n.º1, alínea a) do Código Penal.³⁰⁹

Também o uso da mensagem pela via informática pode ser idóneo, por si só ou acompanhado de outros elementos, para integrar a prática do crime de ameaça simples, ou até de coação, como consagram os artigos 153.º a 155.º do Código Penal.³¹⁰

O aumento das realidades criminais no ciberambiente é o resultado de múltiplos fatores. Por um lado, paradoxalmente, é fator criminógeno a complexidade e sofisticação dos sistemas de segurança, o que leva a que os procedimentos de segurança não sejam devidamente observados ou sejam aligeirados. Por outro lado, é fator criminógeno a multiplicidade e incompatibilidade dos sistemas operativos ativos nas redes. O mesmo acontece com a falta de conhecimentos técnicos por parte da generalidade dos operadores.³¹¹

Potenciam também as más utilizações das redes a grande possibilidade de anonimato na *Internet*, a facilidade de encriptação e a vasta mobilidade internacional. É também um fator de incentivo a facilidade técnica em praticar certos atos criminosos. Por exemplo, é rápido e fácil realizar ilegalmente cópias de *software* que podem também ser rapidamente compactadas e transmitidas à distância.³¹² A juntar à facilidade técnica, é igualmente fator criminógeno a provável impunidade dos agentes resultante, sobretudo, da dificuldade que os tribunais têm de impor as suas decisões no estrangeiro.³¹³

³⁰⁸ Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2.ª ed. Refundida e Actualizada, Almedina, Coimbra, 2006, p.679.

³⁰⁹ *Idem, Ibidem, apud.* Astier, Stéphane, *Rumeurs sur internet*, in *legalis.net*, Jun.2005, 2, pp.63/75, “onde também se dá conta do primeiro julgamento em França de um caso de difamação através de um *blog*”.

³¹⁰ Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2.ª ed. Refundida e Actualizada, Almedina, Coimbra, 2006, p.679.

³¹¹ Verdelho, Pedro, *Cibercrime*, in *Direito da Sociedade da Informação*, vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003, p.353.

³¹² *Idem, Ibidem.*

³¹³ *Idem, Ibidem.*

É importante salientar que, regra geral, a motivação destes agentes, na maioria *hackers*³¹⁴, não consiste em obter um benefício ou vantagem ilegítima, mas sim em testar a segurança dos sistemas, o que, em alguns casos, pode ser vantajoso para o servidor visado, de forma a criar a segurança devida. Outras vezes, o agente atua com o simples propósito de se desafiar a si próprio, pelo prazer da infiltração e da glória pessoal pelo feito; nestes casos, não há qualquer prática de crime de acesso ilegítimo. Se para alguns *hackers* o único intuito é protestar, outros aproveitam-se das ações/intrusões dos primeiros para ilegitimamente se apropriarem de dados relativos a interesses nacionais, nomeadamente ficheiros privativos das autoridades.³¹⁵ Contrariamente, o *cracker*, regra geral, atua com o objetivo de alterar ou remover dados.³¹⁶

A atual crise económica que atravessamos aliada à fácil e rápida mobilidade do espaço digital podem também ser apontadas como dois fatores responsáveis pelo aumento deste tipo de criminalidade.

Nos pontos seguintes iremos analisar alguns destes tipos de crime.

³¹⁴ *Hacker* - é alguém que tem um elevado conhecimento de computadores, comunicação e programação. Em regra é autodidata e conhece várias linguagens de programação, faz os seus próprios programas ou adapta os existentes. O seu principal objetivo e lema é invadir computadores, olhar e sair sem neles mexer ou deixar qualquer rasto da sua presença. No caso de a vítima ter algum programa ou ficheiro que lhe interesse, o *Hacker* copia-o. Por vezes até “conserta” o computador do “hackeado”. É um “pensamento-livre”. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 526 e 527.

Os *Hackers* podem ainda ser divididos em três tipos, conforme o seu nível de conhecimentos e perícia. Os primeiros são os chamados “*script kiddies*”, também conhecidos por *losers* (perdedores), *short-pants* ou *lammers*, nomes que os caracterizam por serem os mais novos e inexperientes. Estes têm um nível baixo de conhecimentos informáticos, são normalmente jovens curiosos que tentam aprender algumas técnicas e “*modus operandi*” através da *Internet*. Os segundos são os chamados *Hackers de nível médio* e já têm mais experiência do que os “*script kiddies*”. “Estes hackers estudam as vulnerabilidades da rede informática e identificam os potenciais alvos, conquistando o controlo dum sistema de informação.”

Por fim, temos “os *Hackers* de nível alto, também conhecidos por “Elite” ou “Gurus”. Estes são conhecidos como génios informáticos e os responsáveis pelos ensinamentos às camadas inferiores. “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.” Dias, Vera, *A Problemática da Investigação do Cibercrime*, Faculdade de Direito, IDPCC, Lisboa, novembro 2010, p.8, *apud.*, Sieber, Ulrich, *Criminalidad Informática: Peligro y Prevención*, Delincuencia Informática, IURA-7, PPU, Barcenona, 1998, p.77; Santos, Paulo, Bessa, Ricardo et.al, *CYBERWAR o fenómeno, as tecnologias e os actores*, FCA, Editora de Informática, Lda., 2008, pp. 59 e 60; Sieber, Ulrich, *Documentación para una aproximación al Delito Informático*, Delincuencia Informática, IURA, Barcenona, 1992, p. 78; Rovira, Enrique Del Canto, *Delincuencia Informática y Fraudes Informáticos*, Estudios de Derecho Penal, 33 Editorial Comares, Granada, 2002, pp.109-114.

³¹⁵ Pereira, Júlio, “Cibersegurança, O Papel do Sistema de Informações da República Portuguesa”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.39.

³¹⁶ *Idem*, *Op. Cit.*, p. 526.

4.2.1. - Burla Informática

Nos Estados Unidos da América, no decurso do ano de 2001, as burlas cometidas através da *Internet* superaram, em prejuízo patrimonial, o valor das burlas tradicionais.³¹⁷ Face a estes dados, o FBI estima que durante aquele ano tenham sido burlados através da *Internet* cerca de 10 mil utilizadores.³¹⁸

Esta evolução do número de casos de *burlas informáticas* não foi só sentida nos Estados Unidos da América, mas também um pouco por toda a Europa. Com efeito, na Europa, apenas no segundo semestre de 2001, o número de crimes informáticos aumentou 10%.³¹⁹

Em Portugal, existe um número significativo de *burlas informáticas*. Em regra, são processos de factualidade extremamente complexa que implicam perícias tecnologicamente exigentes e envolvem, com frequência, um grande número de arguidos. Alguns dos casos abrangem também factos consubstanciadores de crime de *abuso de cartão de garantia* ou de *crédito*, previstos no artigo 225.º do Código Penal.³²⁰

É o facto de a *burla informática* ser praticada através da utilização dos meios informáticos que a torna específica.³²¹

A conexão do crime de burla com a informática estabelece-se pelo modo como a ação é executada, ou seja, por interferência “no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático – recordem-se alguns dos *modi operandi* acima mencionados –, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizado no processamento...”³²².

³¹⁷ É o que resulta de um programa de pesquisa de tecnologia e mercado, realizado pela sociedade *Gartner*, citado pelo *Diário Digital* de 6 de março de 2002. Segundo este mesmo estudo, os prejuízos das burlas *online* representam mais de 1% do valor das vendas *online* realizadas. Verdelho, Pedro, *Cibercrime*, in *Direito da Sociedade da Informação*, vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003, p. 352.

³¹⁸ *Idem*, *Ibidem*, *apud*. Relatório Anual de 2001, citado pelo *Diário Digital* de 15 de maio de 2002.

³¹⁹ Dados revelados por um estudo da consultora IDC.

³²⁰ Verdelho, Pedro, *Cibercrime*, in *Direito da Sociedade da Informação*, vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003, p. 354.

³²¹ Ascensão, José de Oliveira, *Criminalidade Informática*, Direito da Sociedade de Informação, Coimbra: Coimbra Editora, 2001, p. 216.

³²² Por acórdão do Supremo Tribunal de Justiça, de 30.03.2000, in www.dgsi.pt, foi entendido que “o arguido, que se apoderou ilicitamente de vários cartões de crédito da ofendida e a obrigou a revelar-lhe os respectivos códigos de acesso, comete um crime continuado de burla informática se, como se provou,

Como descrevem alguns autores, estamos perante uma criminalidade económico-informática.³²³

A *burla informática* consubstancia um crime contra o património, sendo esse o bem jurídico protegido, embora com natureza mista, já que visa a proteção do património individual e do património abstrato, coletivo, das telecomunicações, enquanto meio de telecomunicação³²⁴, integrando um crime de dano, cuja consumação depende da efetiva ocorrência de um prejuízo patrimonial de outra pessoa. Este é ainda considerado um delito material ou de resultado, que só existe quando se verifica a saída dos bens ou valores da esfera de disponibilidade fáctica da vítima.³²⁵

Alguns autores entendem que este visa igualmente proteger o correto funcionamento e a inviolabilidade dos sistemas informáticos e de informação.³²⁶

Segundo Oliveira Ascensão, a burla informática “surge no desenvolvimento da disciplina geral da burla e participa dos elementos delimitadores gerais do artigo 217.º: a intenção de obter para si ou para terceiro enriquecimento ilegítimo e a causação a outra pessoa de prejuízo patrimonial. A especificidade está no processo utilizado”.³²⁷

Desta forma, a *burla informática* foi enquadrada no próprio Código Penal português, no artigo 221.º, por se considerar que tinha o mesmo significado que a burla em geral. Assim, prevê o n.º1 do supra referido artigo: “Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizado no processamento, é punido com pena de prisão até 3 anos ou com pena de multa”.

utilizando os cartões e os códigos, em caixas Multibanco, procedeu a diversos levantamentos, ... uma vez que a sua conduta integra um dos modos de execução típicos de tal crime: “aproveitamento de dados sem autorização”. II – No crime de burla informática, p.p. pelo artigo 221.º, do Código Penal, o bem jurídico protegido é não só o património – mas concretamente, a integridade patrimonial – como, ainda, a fiabilidade dos dados e a sua protecção”. Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2ª ed. Refundida e Atualizada, Almedina, Coimbra, 2006, p. 676.

³²³ Costa, José de Faria, Moniz, Helena, *Algumas reflexões sobre a criminalidade informática em Portugal*, Boletim da Faculdade de Direito, Coimbra, Vol.73, 1997, p.322.

³²⁴ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 520.

³²⁵ *Idem, Ibidem*

³²⁶ Graça, Pires da, (relatora), Acórdão no processo 78/07.6JAFAR.E2.S1, 3.ª Secção, Supremo Tribunal de Justiça, Lisboa 20-10-2010.

³²⁷ Ascensão, José de Oliveira, *Criminalidade Informática, Direito da Sociedade da Informação*, II, Coimbra, 2001, p.216.

Nestes casos encontra-se ainda previsto o crime *furto de tempo* de acesso à *Internet*. Este ocorre, quando alguém descobre o nome de utilizador (*login*) e palavra-passe de outrem e usa esses dados para aceder ao provedor de serviços de *Internet*, sendo este acesso pago, de modo a utilizar a *Internet* à conta do utilizador.³²⁸ Ou seja, nestes casos o autor do ataque não paga a mensalidade e usufrui do serviço de *Internet* grátis, à custa do verdadeiro utilizador.

Este tipo de crime encontra-se tipificado no número 2 do artigo 221.º do Código Penal, com pena de prisão até 3 anos: “A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.”

Em ambos os casos, a mera tentativa é punível e o procedimento criminal depende de queixa, tal como preveem os números 3 e 4 do artigo 221.º do Código Penal, respetivamente.

³²⁸ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 520.

4.2.2. – Falsidade Informática

O crime de *falsidade informática* destina-se a proteger interesses semelhantes aos que tradicionalmente são tutelados através dos delitos de *falsificação*, ou seja, a segurança, a fiabilidade, a força probatória dos documentos ou outros instrumentos com importância na vida jurídica quotidiana.³²⁹

A manipulação de dados ou programas com valor probatório assume a mesma importância do que a *falsidade* de outros documentos. “Também aqui o que muda é o *meio* de levar a efeito a falsidade”.³³⁰

A *falsidade informática* é um tipo de crime que, aliado à *burla informática*, é cada vez mais recorrente. De tal forma que o legislador decidiu enquadrar este crime no artigo 3.º da Lei n.º109/2009 de 15 de setembro. Nos termos do n.º1 desta disposição: “Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou, por qualquer outra forma, interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou com multa de 120 a 600 dias”.

Esta previsão contém uma inovação face à anterior Lei da Criminalidade Informática, nomeadamente ao anterior artigo 4.º, já que faz referência a dados registados ou incorporados em cartões bancários³³¹ de pagamento, punindo estes factos com pena de prisão de 1 a 5 anos.

Esta norma destina-se, assim, a proteger interesses semelhantes aos que tradicionalmente são tutelados através dos delitos de *falsificação*, mas neste caso através dos meios informáticos e tecnológicos, já que a própria norma enquadra dois

³²⁹ Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2.ª ed. Refundida e Actualizada, Almedina, Coimbra, 2006, p. 683.

³³⁰ *Idem, Ibidem*.

³³¹ O cartão bancário engloba dois conceitos: cartão de débito e cartão de crédito. No entanto, os atuais diplomas legais existentes ainda não analisam este meio de pagamento como um todo, prevendo, uma norma penal que contempla o cartão de crédito (a sua contrafação e passagem) e esquecendo-se do cartão de débito. O cartão de débito corresponde à verdadeira noção de moeda, permitindo ao seu titular aceder de facto à totalidade do seu património. Silva, Vanessa Rossana Queiróz Nunes da, *A Fraude com Cartão Bancário em Portugal na Atualidade*, UAL - Universidade Autónoma de Lisboa, Relatório profissional apresentado para obtenção de grau de Mestre em Direito na Área de Ciências Jurídico-Criminais, Lisboa, março 2013, p.54.

adjetivos tecnológicos, “apagar” e “suprimir”. O primeiro significa eliminar os dados que estejam num suporte informático, por exemplo: quando um *cracker* entra num sistema e elimina todos os dados que um utilizador tenha guardado no seu computador. Já o segundo significa reter e ocultar os dados, por exemplo: quando o *cracker* em vez de apagar os referidos dados, apenas os oculta ou os torna de difícil acesso por parte do utilizador a quem pertenciam, sendo necessária a intervenção de um técnico.

O envio de mensagens “Spam” é também considerado um crime de falsidade informática, pelo artigo 3.º da Lei do Cibercrime. Nestes casos, o agente falsifica uma página da *Internet* ou uma mensagem e, posteriormente reencaminha como sendo verdadeira.

Este preceito abrange também os casos de transações bancárias, operações de contabilidade e pagamentos, em que alguém se aproveita dos dados registados numa determinada base de dados e faz uso dos mesmos.³³²

³³² Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 522.

4.2.3. - *Blackboxing e Blueboxing*

Os crimes *Blackboxing* e *Blueboxing* são formas de perturbação das telecomunicações. Nestes casos, o agente faz uma interferência nas frequências das linhas telefónicas (*blackboxing*), onde liga estes dispositivos electrónicos (*blueboxing*), cujo efeito, de entre outros, é o impedimento total ou a diminuição da taxa devida à operadora de telecomunicações³³³.

De uma forma geral, trata-se de uma forma de “enganar” as operadoras telefónicas, de modo a não pagar qualquer tarifa ou a pagar um valor mais baixo comparativamente ao valor devido.

A prática deste crime constitui crime de *burla nas telecomunicações* e encontra-se tipificado no artigo 221.º, n.º2 do Código Penal, com pena de prisão até 3 anos: “A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.”

³³³ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, pp.521 e 522.

4.2.4. – Carding

“O *Carding* consiste numa forma de dados ou de elementos de identificação quer na face quer contidos em bandas magnéticas de cartões de crédito, de débito ou de telecomunicações, bem como a implantação de dados ou de elementos de identificação noutros suportes técnicos.”³³⁴ Trata-se, como tal, de uma prática distinta da *falsidade informática*, sendo aplicável a tal prática a previsão do crime de *falsificação*, já que o que acontece é a própria falsificação do cartão de crédito.

Se os nomes impressos (*carding*) consistirem na utilização de elementos de identificação constante de *mail orders* ou de dados bancários de terceiros, tal ato constituirá a prática de um crime de burla, punível com pena de prisão até três anos ou com pena de multa, como prevê o artigo 221.º do Código Penal, sendo agravada se o montante em causa for elevado ou se tal conduta for praticada mais do que uma vez, artigo 221.º, n.º5 alínea a).

Por outro lado, o abuso da possibilidade conferida pela posse de cartão de crédito ou de garantia, mesmo que seja apenas pela forma tentada, é punível com pena de prisão até três anos, podendo ser agravado até cinco anos ou de dois anos a oito anos, caso o valor seja elevado ou consideravelmente elevado, artigo 221.º, n.º5 alínea b).³³⁵

³³⁴ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.523.

³³⁵ *Idem, Ibidem.*

4.2.5. – Transmissão de Vírus

Um dos crimes informáticos que os utilizadores mais conhecem são os *vírus informáticos*. Anualmente são criados e difundidos nas redes digitais, nomeadamente na *Internet*, milhares de programas que são ou contêm vírus. Só em 2001 foram produzidos e difundidos cerca de 11 mil novos vírus.³³⁶

De igual forma, a capacidade de expansão e a perigosidade dos vírus mais recentes tem aumentado de forma assustadora. Por exemplo, julga-se que o vírus “I LOVE YOU”, que se expandiu por todo o mundo através de correio eletrónico no fim do ano de 2000, atingiu 45 milhões de computadores. Por seu lado, o vírus “Code Red” atacou no seu primeiro dia de existência 400 mil computadores, incluindo a rede da Casa Branca, em Washington.³³⁷

A forma mais comum e mais fácil de transmissão deste tipo de ataques é através do *correio eletrónico*. Nestes casos o autor do vírus apenas tem de enviar ou introduzir o vírus na rede para depois infectar vários utilizadores. Todas as operações e interações que esses computadores façam com outros computadores, se ainda estiverem infectados, apenas servirão para espalhar o referido vírus. Estes ataques têm como objetivo paralisar os sistemas informáticos de utilizadores comuns, empresas, provedores e até governos.

Esta é considerada uma das formas mais eficaz e, por isso mesmo, mais perigosa de divulgação de vírus informáticos, já que os estragos realizados são imediatos e é difícil averiguar de onde proveio o vírus, nomeadamente, quem foi o seu criador ou o utilizador que o espalhou.

Os tipos de vírus nestes casos podem ser divididos em dois grupos: os menos graves e os mais graves. Os vírus menos graves são criados para se auto enviarem e têm como função causar transtorno ao tráfego de ligação à *Internet*; por exemplo: através do bloqueio de páginas, ligação à *Internet* lenta, falha no servidor, dificuldade em aceder a dadas páginas ou serviços, entre outras situações de carácter temporário. Os vírus mais graves têm finalidades mais nefastas e provocam vários danos quer no próprio computador, quer nas páginas e servidores; por exemplo: podem apagar todo o conteúdo

³³⁶ Verdelho, Pedro, *Cybercrime*, in *Direito da Sociedade da Informação*, vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003, pp. 352 e 353.

³³⁷ *Idem*, *Op. Cit.*, p. 353 *apud*. Diário Digital de 4 de janeiro de 2002.

de um computador, como sistemas, arquivos e ficheiros. Poderão, outrossim, servir para cometer outros crimes, como *phishing*, acesso a base de dados, dados pessoais, contas bancárias, entre outros.

Para combater este tipo de ataques e atenuar os seus efeitos, a Lei n.º109/2009 de 15 de setembro consagra no artigo 4.º o *dano relativo a programas ou outros dados informáticos*. Como dispõe o n.º1: “Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.” Da mesma forma e no n.º3 encontra-se prevista a sanção para a produção, venda, distribuição ou qualquer forma de divulgação de vírus informático: “Incorre na mesma pena do n.º1 quem ilegítimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número.”

Importa referir que para os casos previstos nos números 1, 2 e 4, o procedimento penal depende de queixa, tal como define o n.º6 do supra referido artigo, o que desde logo pressupõe dois factos:

1. Que o utilizador saiba que foi vítima deste tipo de ataque; e
2. Quem foi o seu agente, isto é, contra quem será apresentada a queixa, o que nem sempre é fácil de provar.

Por outro lado, o envio de um vírus pela *Internet* pode igualmente configurar a prática de um crime de *sabotagem informática*, tal como prevê o n.º1, do artigo 5.º da Lei 109/2009, de 15 de setembro: “Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entrar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias”.

Contrariamente ao que acontece no crime de *dano informático*, a *sabotagem informática* não tem por pressuposto subjetivo a obtenção de uma vantagem patrimonial para o sujeito ou para terceiro, bastando que o ato seja praticado “contra um sistema informático”, sendo neste caso o elemento subjetivo, “entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático”.

4.2.6. – Acesso ilegítimo

Nos tipos de crimes informáticos enquadramos ainda o chamado *acesso ilegítimo*. Nestes casos, ocorre uma utilização não consentida e abusiva de contas e palavras-passe por parte de terceiros para acederem à *Internet*: “Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias”, tal como define o artigo 6.º da Lei n.º109/2009, de 15 de setembro.

Este tipo de crime é parecido com o ataque *furto de tempo*, já que ambos consistem na utilização abusiva de contas eletrónicas e palavras-passe para acederem à *Internet*, mas nestes casos o que acontece é que o agente utiliza essas informações (endereço eletrónico e palavra-passe) não para utilizar o serviço de *Internet* gratuitamente, como acontece no crime de *furto de tempo*, mas sim para aceder a informação pessoal do utilizador, quer esta esteja contida no computador, por exemplo, nos ficheiros ou nos documentos, mas também nas próprias páginas da *Internet* que o utilizador consulta diariamente.

4.2.7. – Espionagem Informática e o sistema ECHELON

A *espionagem*, aqui no âmbito tecnológico, consiste nos atos ilícitos que têm como objetivo a obtenção de dados ou informações sigilosas por meio de sistema informático.

Como referiu Howard Rheingold: “Há uma grande controvérsia nos Estados Unidos sobre os poderes de espionagem que o governo está a usar contra os terroristas, vigiando cidadãos. Já passou demasiado tempo sem que as pessoas se tenham preocupado sobre onde isto nos vai levar. A ligação electrónica do mundo não está completa, não há câmaras em todas as esquinas. Ainda. Essas câmaras não são todas digitais e não estão todas ligadas entre si. Ainda. O *software* de reconhecimento facial, que permite escolher uma cara num vídeo entre uma multidão e identificá-la, não é completamente eficaz. Ainda. Por isso acho que temos de pensar, agora, em leis, em restrições. Os governos terão de ter mandatos, motivos para poderem espiar indivíduos. Está na altura de os cidadãos acordarem e perceberem que, se confiam nos seus governos para proteger as suas liberdades, não faz sentido que o façam retirando-lhes as suas liberdades”.³³⁸

De facto, todas as hipóteses supra mencionadas são atualmente uma realidade. A ligação eletrónica do mundo está praticamente completa, quase todos os cidadãos têm ligação à *Internet* e as câmaras de vigilância começam a ser instaladas nas principais ruas de cada cidade. Inclusive em Portugal, são vários os pontos da cidade (especialmente os de maior afluência turística e cultural) que atualmente já utilizam câmaras de vigilância.

No entanto, todas estas evoluções tecnológicas têm também um impacto negativo na privacidade e liberdade dos cidadãos.

Justifica-se que, neste contexto, se conceda uma breve atenção ao projeto ECHELON, nomeadamente às suas características fundamentais, aos seus objetivos e, bem assim, aos riscos que comporta para as liberdades e para os direitos fundamentais dos indivíduos.³³⁹

³³⁸ Professor de Tecnologia de Cooperação no curso de jornalismo digital da Universidade norte-americana de Stanford, autor do livro “Smart Mobs” (“Multidões Espertas”), entrevista na Revista “Pública”, de 15 de janeiro de 2006.

³³⁹ Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2.^a ed. Refundida e Actualizada, Almedina, Coimbra, 2006, p. 214.

O ECHELON é definido como “um sistema global de interceptação de comunicações privadas e económicas”.³⁴⁰ Este sistema foi descrito pela primeira vez pelo autor neozelandês Nicky Hager no seu livro “Secret Powers – New Zeland’s role in the international spy network”, publicado em 1996.

De acordo com o Relatório da Comissão, o sistema ECHELON apresenta duas características específicas que o distinguem dos outros sistemas de informação:

1. “a capacidade praticamente global de vigilância, uma vez que, recorrendo principalmente a estações receptoras via satélite e a satélites de espionagem, se torna possível interceptar qualquer comunicação via telefone, telefax, Internet ou *e-mail*, emitida seja por quem for, de forma a aceder ao respectivo conteúdo”;
2. “o facto de o sistema assentar na cooperação internacional entre vários países – o Reino Unido, os Estados Unidos da América, o Canadá, a Austrália e a Nova Zelândia (Estados UKUSA)³⁴¹ –, o que representa uma mais-valia relativamente a sistemas nacionais, revelando-se mesmo essencial para a vigilância das comunicações rádio via satélite, na medida em que só assim se pode assegurar que, no caso de comunicações internacionais, será possível interceptar as informações transmitidas por ambos os interlocutores”.³⁴²

A ameaça que o ECHELON encerra para a vida privada e para a economia e a livre concorrência não se traduz apenas no poderoso sistema de vigilância em que assenta, mas também no facto de operar num sistema praticamente à margem da lei.³⁴³

Mike Frost, um antigo colaborador dos serviços secretos canadianos³⁴⁴, disse, em entrevista ao canal CBS, que todos os dias em todo o mundo são controladas pelo ECHELON – que definiu como uma rede secreta de vigilância do governo – conversas telefónicas, correios eletrónicos e fax, bem como comunicações civis.³⁴⁵ Numa outra

³⁴⁰ Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2.^a ed. Refundida e Actualizada, Almedina, Coimbra, 2006, p. 214.

³⁴¹ UKUSA designa um acordo SIGINT (sistema de espionagem eletrónica), assinado em 1948 entre o Reino Unido, os Estados Unidos da América, ao qual, ulteriormente, também aderiram a Austrália, o Canadá e a Nova Zelândia. A sigla UKUSA constitui o acrónimo de “United Kingdom – USA”.

³⁴² Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2.^a ed. Refundida e Actualizada, Almedina, Coimbra, 2006, pp. 216 e 217.

³⁴³ *Idem*, *Op. Cit.*, p. 217.

³⁴⁴ Trata-se do CSE, sob tutela do Ministério da Defesa do Canadá.

³⁴⁵ Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2.^a ed. Refundida e Actualizada, Almedina, Coimbra, 2006, p. 218.

entrevista, o mesmo colaborador referiu como exemplo o facto de o CSE ter registado numa base de dados sobre possíveis terroristas o nome e o número de telefone de uma cidadã que proferia uma frase ambígua numa conversa telefónica inocente para um amigo.³⁴⁶ Nas comunicações interceptadas, o computador tinha encontrado a palavra-chave “bomba”, pelo que reproduzira a conversação. Importa referir que na conversa em questão, a cidadã referia que a interpretação do filho numa peça de teatro da escola tinha sido uma “bomba”. Este simples exemplo demonstra bem a dimensão dos riscos de perseguição injusta e de discriminação abusiva que um sistema como ECHELON pode proporcionar, especialmente, em sociedades dominadas por preocupações securitárias, como é o caso daquelas que fazem parte do mundo ocidental, mormente após o 11 de setembro.³⁴⁷

Concluimos, assim, que todo e qualquer ato que envolva a interceção de comunicações e de registo de dados pessoais pelos serviços de informação de segurança com esse objetivo representa uma grave ingerência na vida privada dos indivíduos em apreço e que apenas pode ocorrer num “Estado policial”.³⁴⁸ Desta forma, num Estado de direito, o direito à intimidade da vida privada beneficia de proteção constitucional, em que as ingerências apenas são toleradas após avaliação jurídica das circunstâncias concretas de cada situação e no respeito do princípio da proporcionalidade.³⁴⁹

³⁴⁶ Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2.^a ed. Refundida e Actualizada, Almedina, Coimbra, 2006, pp.218 e 219.

³⁴⁷ *Idem*, *Op. Cit.*, p. 219.

³⁴⁸ *Idem*, *Op. Cit.*, p. 220.

³⁴⁹ *Idem*, *Idem*.

4.2.8. – Intercepção ilegítima

A *intercepção*, tal como define a própria alínea e) do artigo 2.º da Lei n.º 109/2009, de 15 de setembro, é “o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros”. A intercepção ilegítima pode dividir-se em quatro tipos de ataques: a) *Sniffing*; b) *Varredura de portas*; c) *Ataques DoS (Denial of Service)*; d) *Ping O’Death*.

a) No primeiro caso, os *Hackers* ou *Crackers* usam um programa ou dispositivo que monitoriza o tráfego em rede, *sniffer*, para capturar os dados transmitidos. Os *Sniffers* são úteis para administração de redes, mas sendo utilizados por *Hackers* ou *Crackers*, permitem obter palavras-chave e quaisquer outras informações ou conteúdos pessoais.³⁵⁰

b) Os programas de *varreduras de portas* servem para procurar na *Internet* os computadores que tenham portas ativas, abertas e/ou componentes ou periféricos compartilhados em rede, ou seja, servem para procurar locais do computador que possam ser acedidos por terceiros. Os programas mais completos são o *LanGuard Scanner*³⁵¹ e o *Nmap*³⁵² que permitem percorrer todo o sistema em questão à procura de serviços e portas em operação, partilhas de rede com acesso a discos e quebra de palavras-chave de partilha.³⁵³

Estes programas de *varredura de portas* ou de *hosts* são ferramentas muito úteis para administradores de rede e consultores de segurança para identificação e correção de possíveis falhas de segurança. No entanto são, também, muito utilizados por *Hackers* e *Crackers* para invadir computadores e sistemas de terceiros.

³⁵⁰ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.1042.

³⁵¹ *LanGuard Scan*. Disponível em <http://www.gfi.com/languard/>, permite que o utilizador mais imprevidente possa passar situações de verdadeiro risco para a sua privacidade. Com os recursos que oferece o *LanGuard*, qualquer um que mantenha os seus recursos compartilhados mesmo com *password*, este programa pode quebra-las em minutos ou até mesmo segundos, dependendo da rapidez da sua conectividade à *Internet*. *Idem*, *Op. Cit.*, p.528.

³⁵² O *Nmap* é um varredor de *hosts*, computador ligado à *Internet* onde um *website* é alojado para poder ser acedido pelos internautas. Computador central, também designado por servidor, onde se encontra gravado, alojado o conjunto de programas e ficheiros de um ou mais sítios que usa recursos avançados para verificar o estado do “alvo”. Trata-se de um programa gratuito disponível para os seguintes sistemas operativos: *Linux* e *Windows*, *Mac OS*, *Solaris*, *FreeBSD* e *OpenBSD*, a partir do sítio oficial <http://www.insecure.org>. *Idem*, *Ibidem*.

³⁵³ *Idem*, *Ibidem*.

A única forma de defesa do utilizador comum face a estes ataques é a instalação e configuração de *firewall* com regras bem definidas, assim como de um antivírus³⁵⁴. De igual forma o utilizador deve diminuir os serviços ativos, deixando apenas os indispensáveis ao seu funcionamento, assim como programas de detenção de intrusos.

c) Os ataques *DoS*, *Denial of Service*, ou em português, ataques de negação de serviço, são efetuados contra sítios de grandes empresas ou entidades e, apesar de terem uma duração limitada (duram apenas algumas horas), têm consequências gravíssimas para as mesmas. Estes ataques causam, geralmente, a interrupção de serviços de sítios, enviando sucessivamente pacotes de protocolo de *Internet* mal construídos.³⁵⁵

Tudo começa quando um computador malicioso gera mensagens aparentemente normais. Estes pacotes dão a impressão que são criados no mesmo servidor que os está a receber. Ao tentar responder a esse fluxo constante de mensagens de dados defeituosos, o servidor, que está a ser vítima desse ataque, torna-se incapaz de aceitar outras conexões, o que faz com que qualquer envio de mensagem implique um retorno nulo.³⁵⁶

Este ataque é, de certa forma, semelhante aos ataques que enchem as fotocopiadoras com inúmeras mensagens longas e repetidas. Um dos objetivos deste tipo de ataques é sobrecarregar os servidores ou os fornecedores de serviço *Internet* com mensagens geradas automaticamente. Outros podem consistir na perturbação dos servidores que fazem funcionar o sistema de nome de domínio ou visar danificar os *routers* (encaminhadores).³⁵⁷ Os ataques destinados a perturbar os sistemas são os que têm um impacto imediato, já que os proprietários das páginas eletrónicas precisam que estas estejam sempre a funcionar e, em caso de falha, esta consiga ser reparada de forma breve, o que não acontece nestes tipos de ataque.

d) A expressão, *Ping O'Death*, define uma espécie de ataques bastante explorada na *Internet*. Este tipo de ataque consiste no envio de um pacote *IP* com um tamanho superior ao máximo permitido (65535 bytes) para o computador que se deseja atacar. O

³⁵⁴ São já algumas as marcas que disponibilizam nas suas próprias páginas eletrónicas o download gratuito do seu programa certificado, por exemplo, *Microsoft Security Essentials* [Em linha]. Disponível em www.microsoft.com.

³⁵⁵ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 529.

³⁵⁶ *Idem, Ibidem.*

³⁵⁷ *Idem, Ibidem.*

que acontece é que o pacote é enviado na forma de fragmento, pois nenhum tipo de rede permite o tráfego de pacotes com este tamanho e, quando a máquina de destino tenta montar esses fragmentos, dá origem a uma série de situações, entre elas: bloqueio de computadores (casos mais comuns), reinício automático do sistema, abortar as tarefas que estavam em curso e exibição de mensagens de erro irreversível.³⁵⁸

Este ataque recebeu o nome de *Ping O' Death* graças aos primeiros ataques com esta natureza, já que foram perpetrados a partir do programa *ping*. Atualmente, qualquer pacote *IP* com mais de 65535 bytes (pacote inválido) provoca o mesmo efeito.³⁵⁹

Estes três ataques que acabámos de mencionar (alíneas a, b e c) enquadram-se todos no crime de *interceção ilegítima*, presente no artigo 7.º da Lei 109/2009, de 15 de setembro. Como dispõe o n.º1: “Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa”.

“Incorre na mesma pena prevista no n.º1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número”, n.º 3 do supra referido artigo.

³⁵⁸ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.530.

³⁵⁹ *Idem, Ibidem*.

4.2.9. – Reprodução ilegítima de programa protegido

A *Reprodução ilegítima de programa protegido* encontra-se tipificada no artigo 8.º da Lei n.º 109/2009 de 15 de setembro. A partir do exposto nos números 1 e 2 do referido artigo, vemos como o legislador conseguiu abranger todos os tipos de crimes relacionados com a reprodução, divulgação ou comunicação ao público de um programa informático protegido por lei, bem como de um produto semicondutor ou a explorar comercialmente ou importar, para esses fins, uma topografia ou um produto semicondutor fabricado a partir da mesma.

Ao adquirir um programa e aceitar o acordo de licenciamento que acompanha a instalação de *software*, o consumidor compra apenas o direito de uso do *software* e não o direito de revenda ou de reprodução do programa, como tantos fazem, as chamadas “cópias pirata”. O custo real e o valor de cada peça de *software* recaem no trabalho intelectual utilizado para desenvolver aquele programa, ou aquele computador e não na caixa, embalagem ou no próprio disco.³⁶⁰

Não conta como *reprodução ilegítima de programa protegido* ou *pirataria informática* o uso de cópias de segurança, os chamados *backups*, que permitem guardar no disco rígido do computador toda a nossa informação, que em caso de avaria ou deterioração da primeira versão nos permite aceder à cópia desses dados.

Como refere Joel Timóteo Ramos Pereira, dentro da *reprodução ilegítima de programa protegido* podemos encontrar quatro modalidades:

1. *Cópia irregular* - esta constitui um tipo de pirataria na qual um indivíduo ou empresa replica indevidamente um *software* original. No caso de licenças em volume (grandes quantidades de cópias), isso significa informar um número de instalações de *software* inferior ao realmente em uso ou instalado.
2. *Software pré-instalado no disco rígido* - consiste na instalação de um programa ou programas no disco rígido do computador, quando este é vendido, sem que cada um desses programas contenha a devida licença de instalação e utilização, normalmente licenciadas com uma palavra de acesso. Na maioria dos casos existe uma cópia adquirida legalmente, com licença para um computador ou para

³⁶⁰ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.530.

um número limitado, a partir da qual se procede à instalação em diversos outros computadores.

3. *Falsificação* - trata-se da reprodução do *software* em grande escala, ou seja, consiste na reprodução de um programa original para vários falsos, com a garantia de serem todos originais, já que aparentam muitas semelhanças, incluindo a própria capa e selos. O preço é a única exceção, já que é sempre significativamente inferior ao original.
4. *Canais ilegais de distribuição* - são locais onde é possível adquirir produtos cuja revenda é proibida ou cuja distribuição é apenas permitida a proprietários devidamente qualificados para essa finalidade.
5. *Warez* - trata-se de um programa distribuído ilegalmente através da *Internet*. O “z” na palavra é propositado, já que é utilizado para definir algo ilegal. Existem vários sítios na *Internet* que disponibilizam *warez* (basta fazer uma pesquisa deste termo) e em muitos deles é igualmente disponibilizado o número de série do programa, que permite não só desbloquear a proteção, como fazer o próprio funcionar.³⁶¹

³⁶¹ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 531.

4.3. - Criminalidade Organizada

É recorrente, nas instâncias judiciais e políticas, nacionais e internacionais, o debate sobre as novas formas de criminalidade, em especial, sobre a criminalidade organizada. Trata-se de uma realidade grave e preocupante com dimensão planetária e incidência no quotidiano de todos.³⁶²

Podemos afirmar que a criminalidade organizada não é um fenómeno novo, já que são vários os exemplos de ataques praticados ao longo dos anos. Porém, não restam dúvidas de que o seu exponencial crescimento ocorreu durante o século XX, em grande parte, graças ao desenvolvimento da sociedade da informação, dos novos produtos, serviços e meios de atuação.

Atualmente assiste-se ao aumento do número de casos de criminalidade organizada. A organização da atividade criminal assume uma natureza nova, quer pela sua transnacionalidade, quer pelo modelo que as tecnologias disponíveis e os fluxos migratórios permitem estruturar.³⁶³ “A criminalidade de hoje não tem fronteiras.”³⁶⁴ E este é um dos vários desafios que a criminalidade coloca aos Estados: a dispersão da ação criminosa, no tempo e no lugar, o número de ataques e a gravidade dos mesmos.

A verdade é que, como refere Reginaldo Rodrigues de Almeida³⁶⁵, só conhecemos e temos acesso a 20% da *Internet*, também conhecida como *Surface Web*³⁶⁶, que representa a parte dita “comum” da rede. Toda a outra percentagem corresponde a uma parte da *Internet* que não conhecemos e à qual poucos têm acesso, onde é necessária uma senha de acesso e elevados conhecimentos tecnológicos, onde as próprias autoridades têm dificuldade em aceder. A esta parte da *Internet* é dado o nome de *Dark Web*³⁶⁷. Dentro da *Dark Web* podem ainda ser criadas outras redes paralelas, como é o caso da *Darknet*³⁶⁸.

³⁶² Davin, João, *A Criminalidade Organizada Transnacional, A Cooperação Judiciária e Policial na UE*, 2.^a edição revista e aumentada, Almedina, Novembro 2007, p. 3.

³⁶³ *Idem, Ibidem*.

³⁶⁴ Mota, José Luís Lopes da, Vice-Presidente da Eurojust, seminário da Eurojust, Lisboa, 20.04.2006.

³⁶⁵ Entrevista realizada a Reginaldo Rodrigues de Almeida no dia 19 de maio de 2014.

³⁶⁶ A *Surface Web* pode ser definida como a parte da *Internet* que é geralmente acessível através dos motores de busca, como sejam o *Google*, o *Bing* ou o *Yahoo!*. Ramalho, David Silva, “A Investigação Criminal na *Dark Web*”, in *Revista de concorrência e regulação*, Coimbra, a.4n.14-15, Abr.-Set.2013, p. 385.

³⁶⁷ É usual distinguirem-se vários níveis dentro da *Dark Web*, cujo acesso seria progressivamente mais difícil à medida que nos aproximamos do nível mais profundo, a chamada *Mariana's Web*. No entanto, a existência de uma hierarquização desta natureza é altamente contestada. Ramalho, David Silva, “A

Segundo a agência Efe³⁶⁹, este é um espaço onde os simples usuários não podem aceder pelo *Google* ou pelo *Yahoo*. Para chegar a esta *Internet* é preciso um navegador diferente, concebido de forma a evitar que se identifique o seu endereço de *IP*. Algo que o responsável pelo *Grupo de Crimes Telemáticos da Guarda Civil espanhola* reconhece tornar difícil a investigação.³⁷⁰

Alberto Silva Franco descreve assim o crime organizado: “O crime organizado possui uma textura diversa: tem carácter transnacional na medida em que não respeita as fronteiras de cada país e apresenta características assemelhadas em várias nações; detém um imenso poder com base em estratégia global e numa estrutura organizativa que lhe permite aproveitar as fraquezas estruturais do sistema penal; provoca danosidade social de alto vulto; tem grande força de expansão, compreendendo uma gama de condutas infracionais sem vítimas ou com vítimas difusas; dispõe de meios instrumentais de moderna tecnologia; apresenta um intrincado esquema de conexões com outros grupos delinquenciais e uma rede subterrânea de ligações com os quadros oficiais da vida social, económica e política da comunidade; origina acto de extrema violência; urde mil disfarces e simulações e, em resumo, é capaz de inerciar ou fragilizar os poderes do próprio Estado.”³⁷¹

As crescentes formas de globalização, baseadas em comunicações rápidas bem como o recurso a tecnologia sofisticada sustentada em meios informáticos de última geração,

Investigação Criminal na Dark Web”, in *Revista de concorrência e regulação*, Coimbra, a.4n.14-15, Abr.-Set.2013, p. 393.

³⁶⁸ Darknet é uma rede virtual estabelecida entre vários utilizadores, inacessível a terceiros e que funciona através de uma rede de telecomunicações pública, neste caso a *Internet*, que visa a partilha de informações e ficheiros em formato digital sem, contudo, permitir que, quer os endereços de IP dos seus membros, quer o teor das comunicações entre si estabelecidas, possam ser descobertos. Por exemplo: pense-se na existência de um grupo de indivíduos de várias nacionalidades que se conhecem e decidem partilhar imagens de pornografia infantil em formato *peer-to-peer* uns com os outros, sem que qualquer outra pessoa possa aceder a esses dados, estabelecendo para tal uma rede de partilha privada – neste caso estaremos perante uma *Darknet* na *Dark Web*. *Idem*, *Op. Cit.*, p.394.

³⁶⁹ Agência Efe - A agência EFE é um serviço de notícias internacional fundado em 1939 na Espanha. É a quarta maior agência de notícias do mundo. Sítio oficial, disponível em www.efes.com

³⁷⁰ Existem sítios que monitorizam atividades na *Internet* que promovem o ódio, racismo ou práticas ilícitas. Os de maior relevo são o *Hatewatch* (<http://www.hatewatch.org>) que procura identificar se crimes reais, como homicídios, tiveram origem a partir de mensagens divulgadas pela *Internet* e, o sítio da Liga Anti-Difamação (<http://adl.org>). Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 462.

³⁷¹ Franco, Alberto Silva, *O difícil processo de tipificação*, Boletim do Instituto Brasileiro de Ciências Criminais, n.º21, p.5 *apud.*, Lavorenti, Wilson e Silva, José Geraldo, in *Crime Organizado na Atualidade*, Campinas – SP, Bookseller, 2000, p.18.

trouxeram enormes benefícios para o crescimento da economia mundial, da mesma forma que acarretaram efeitos perversos.³⁷²

A nível comunicacional, a *Internet*, criou um novo paradigma para este tipo de criminalidade, já que garante a rapidez na comunicação assim como um elevado grau de secretismo graças às comunicações encriptadas.³⁷³ Por outro lado, dificultou a atuação das autoridades judiciárias ou policiais que, no decurso de uma investigação, se confrontam com mudanças sucessivas e inesperadas de equipamentos e até de operadoras.³⁷⁴

É através da *Internet* que os grupos de criminalidade organizada recrutam potenciais interessados, quer para os seus serviços quer como futuros membros da organização criminosa. Da mesma forma, a *Internet* serve também como “montra” global onde são feitas trocas, compras e vendas de todo o tipo de produtos e serviços de génese ilegal, como sucede com os medicamentos de venda condicionada.³⁷⁵

Os grupos criminosos cedo se aperceberam das possibilidades do mundo tecnológico para a prática de atos ilícitos bem como para a ocultação dos seus agentes e lucros. De igual modo, aperceberam-se que uma atuação dispersa é o ponto-chave para, no decurso do processo criminal, atuarem em mercados atraentes do ponto de vista económico e dificultar, consideravelmente, a ação das autoridades policiais e judiciárias. Se a atividade criminal tivesse lugar em diversas jurisdições poderia, assim, explorar pontos de vulnerabilidade do sistema jurídico, nomeadamente, a escassa ou, muitas vezes, deficiente cooperação policial e judiciária.³⁷⁶

³⁷² Nas reuniões preparatórias da Convenção das Nações Unidas contra o Crime Organizado Transnacional foi referenciado que: “... *efforts of the international community to develop international instruments against transnational organized crime arise from the recognition that the problem has become much more serious. New forms of transnational co-operation between organized criminal groups emerged in the closing decades of the 20th century. The globalization of economic systems and developments in transportation and communications technologies have created enormous opportunities for human communication and economic development, but they have also created significant new opportunities for organized crime* ...”. Com mais detalhes consultar o website da United Nations Office on Drugs and Crime (UNODC) em: <http://www.unodc.org>. Especificamente no endereço: <http://www.unodc.org/adhoc/palermo/convensumm.htm> sob o lema - Summary of the United Nations Convention against transnational organized crime and protocols thereto.

³⁷³ Davin, João, *A Criminalidade Organizada Transnacional, A Cooperação Judiciária e Policial na UE*, 2.^a edição revista e aumentada, Almedina, Novembro 2007, p. 42.

³⁷⁴ *Idem*, Op. Cit., p. 43.

³⁷⁵ *Idem*, Op. Cit., p.42.

³⁷⁶ *Idem*, Op. Cit., p. 60.

A acumulação e troca de informação nestes campos é um passo fundamental quer para a atividade policial quer para a judiciária.

Concluimos, uma vez mais, que o domínio da informação é o fator fundamental para o combate eficaz ao crime organizado e às novas formas de criminalidade: conhecer os agentes e o seu respetivo *modus operandi*, saber quais os interlocutores em cada Estado e os mecanismos mais rápidos de contacto, dominar o direito internacional e comunitário constituem as funções indispensáveis de polícias e magistrados comprometidos com a investigação criminal.³⁷⁷

³⁷⁷ Davin, João, *A Criminalidade Organizada Transnacional, A Cooperação Judiciária e Policial na UE*, 2.^a edição revista e aumentada, Almedina, Novembro 2007, p. 5.

4.4. - Ataques contra sistemas informáticos

As redes de comunicação eletrónicas e os sistemas de informação fazem atualmente parte integrante da vida quotidiana de todos os cidadãos, da mesma forma que desempenham um papel fundamental no sucesso de toda a economia.

Esta evolução, decorrente da interligação das redes informáticas com os sistemas de informação, traz grandes vantagens, da mesma forma que traz ameaças de ataques³⁷⁸ intencionais contra os sistemas informáticos. Estes ataques podem assumir diversas formas, de entre as quais destacamos: o acesso ilegal, a propagação de códigos maliciosos- vírus, ataques de negação de serviço, *botnets*.

Uma das razões, que tanto tem preocupado as autoridades de defesa nacional e internacional, quanto a este tema, é a possibilidade de praticar ataques contra sistemas informáticos a partir de qualquer ponto do mundo, em qualquer direção ou em várias direções ao mesmo tempo e a qualquer momento.

Os ataques de *hackers* contra empresas privadas e organismos públicos de infraestruturas básicas, como serviços de água, eletricidade ou telefone, aumentaram 28% nos primeiros seis meses de 2002.³⁷⁹ Outro exemplo, o sítio do Presidente russo, Vladimir Putin, foi atacado por 96 *hackers* nas primeiras vinte e quatro horas em que funcionou, em junho de 2002.³⁸⁰ A Rússia e, em particular, São Petersburgo e Novossibirsk, têm ficado conhecidas pelo aparecimento de um grande número de piratas informáticos.

De acordo com a Comissão Europeia, desde fevereiro de 2005, altura em que a União Europeia se dotou de normas a este respeito, registou-se um aumento significativo de ataques aos sistemas informáticos governamentais e privados, tendo-se registado em

³⁷⁸ Ataque - ato que visa o desvio do controlo de segurança de um sistema, procurando atingir a sua vulnerabilidade ou eficácia.

Ataques de *password* - tentativa para obter ou descodificar uma palavra-passe de um utilizador legítimo. Os *Hackers* podem usar dicionários de palavras-passe, programas específicos ou *Sniffers* em ataques de palavras-passe. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1030.

³⁷⁹ Verdelho, Pedro, *Cibercrime*, in *Direito da Sociedade da Informação*, vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003, p.352, *apud.*, *Riptech Inc*, sociedade americana, citada pelo *Diário Digital* de 9 de julho de 2002.

³⁸⁰ Verdelho, Pedro, *Cibercrime*, in *Direito da Sociedade da Informação*, vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003, p.352, *apud.*, *Diário de Notícias* de 25 de junho de 2002.

2009 ataques a 100 países.³⁸¹ Neste caso, o *software* criou as chamadas “*botnets*” para danificarem os computadores.

Mais recentemente, num relatório publicado no final de 2013, a empresa de segurança informática *Symantec* dá conta de que mais de 1.400 instituições financeiras foram alvo do conhecido ataque *trojan* só em 2013, sendo os mais conhecidos bancos norte americanos os principais alvos destes ataques.³⁸² “O atacante está sobretudo interessado nos dados financeiros do consumidor, mas muitas vezes as informações recolhidas também podem ter potencial interesse para a espionagem corporativa, dando vantagem competitiva aos que obtiverem aqueles dados”.³⁸³

O alerta é assim global e a ameaça constante. Como prevê a Organização Internacional dos Reguladores dos Mercados de Capitais (*IOSCO*), o próximo grande choque financeiro deverá certamente chegar do espaço virtual, como resultado de sucessivos ataques a importantes figuras do setor financeiro.³⁸⁴ “O potencial de perdas é enorme uma vez que os criminosos entram dentro do sistema de negociação financeira de um banco, onde não há limitação sobre o que se pode fazer caso se consiga passar pelos sistemas de controlo.”³⁸⁵

Quanto às motivações, podem, na realidade, ser as mais diversas, desde ações concretas de espionagem internacional, industrial ou comercial, que podem ir até ações de falsificação de envio de *emails*, ou mesmo casos de *phishing* para efeitos de fraude bancária.³⁸⁶ A motivação do ataque é um fator importante já que permite definir corretamente as estratégias de defesa adequadas.³⁸⁷

Como refere Neelie Kroes “para que todos os europeus se convertam ao digital é necessário que se sintam confiantes e seguros em linha. As ameaças informáticas não

³⁸¹ Comissão Europeia, Bruxelas, 30 de setembro de 2010, [Em linha]. Disponível em http://europa.eu/rapid/press-release_IP-10-1239_pt.htm, (consultado em 15.10.2014).

³⁸² Documento original, disponível em <http://observador.pt/2014/08/31ataques-informaticos-bancos-deixam-especialistas-em-seguranca-em-alerta-maximo/>, (consultado em 15.10.2014).

³⁸³ Orla Cox, [Em linha], gestora da *Symantec*, oferece proteção contra vírus e outros *softwares* maliciosos. Disponível em www.symantec.com.

³⁸⁴ Disponível em <http://observador.pt/2014/08/31ataques-informaticos-bancos-deixam-especialistas-em-seguranca-em-alerta-maximo/>, (consultado em 15.10.2014).

³⁸⁵ Michael Coates, diretor da *Start-Up* de segurança informática *Shape Security*. *Idem, Ibidem*.

³⁸⁶ Cordeiro, Raul, “Ataques de DDOS, Medidas Preventivas”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p. 49.

³⁸⁷ *Idem, Ibidem*.

conhecem fronteiras. (...) ”.³⁸⁸ Como tal, “as instituições e os Governos da União Europeia devem trabalhar mais do que nunca em conjunto, para nos ajudar a compreender a natureza e a escala das novas ameaças informáticas”.³⁸⁹

Como forma de combater os ataques contra sistemas informáticos, a Comissão Europeia, apresentou, em 2010, duas medidas para garantir que a Europa se conseguia defender perante este tipo de ataques.³⁹⁰ Uma proposta de diretiva sobre as novas formas de *Cibercrime*, entretanto adotada: a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho. Esta proposta de Diretiva foi complementada por uma proposta de regulamento destinado a reforçar e modernizar a Agência Europeia para a Segurança das Redes e da Informação (ENISA), criada pelo Regulamento (CE) n.º460/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004, entretanto adotada em 2011 (Regulamento (UE) n.º 580/2011 do Parlamento Europeu e do Conselho, de 8 de junho de 2011, que altera o Regulamento n.º460/2004 que cria a ENISA). Ambas pertenciam à “Agenda Digital para a Europa e do Programa de Estocolmo, no intuito de aumentar a confiança e a segurança na rede”³⁹¹.

Cecilia Malmström refere: “O crime está a explorar novos caminhos. Com a ajuda de *software* maligno, é possível assumir o controlo de grande número de computadores e obter números de cartões de crédito ou informações sensíveis e lançar ataques de grande escala. É tempo de reforçarmos os nossos esforços contra o *Cibercrime*, muitas vezes utilizado pela criminalidade organizada. (...) ”³⁹².

³⁸⁸ Neelie Kroes, Vice-presidente da Comissão responsável pela Agenda Digital. Comunicado de Imprensa, Comissão Europeia, [Em linha], Bruxelas, 30 de setembro de 2010, Disponível em http://europa.eu/rapid/press-release_IP-10-1239_pt.htm, (consultado em 15.10.2014).

³⁸⁹ *Idem, Ibidem.*

³⁹⁰ *Idem, Ibidem.*

³⁹¹ *Idem, Ibidem.*

³⁹² *Idem, Ibidem.*

4.5. - Pedofilia e Pornografia Infantil

Graças às suas funções, a *Internet* põe-nos em contacto com as mais diversas realidades e atividades sejam, elas ilícitas ou não. Sendo as crianças e os jovens quem mais utiliza a *Internet*, são também os utilizadores mais suscetíveis a tais atividades.

As tecnologias da informação e comunicação expandiram também as formas de praticar crimes contra crianças e jovens. Como noutras áreas, para além das suas grandes vantagens, a evolução tecnológica tem sido auxiliar do crime, quer através da criação de novas formas de crime quer através de novas formas de praticar antigos crimes.³⁹³

Os crimes relacionados com a pedofilia e a pornografia infantil³⁹⁴ são os crimes relativos a conteúdos que mais têm preocupado os Estados Membros. Esta preocupação resulta do aumento deste tipo de crime, bem como do insucesso das medidas adotadas ao longo dos anos.

Em 1999, foi adotada uma das primeiras medidas da União Europeia contra a pornografia infantil: a Decisão n.º 276/1999/CE do Parlamento Europeu e do Conselho que adotou “um plano de ação comunitário plurianual para fomentar uma utilização mais segura da *Internet* através do combate aos conteúdos ilegais e lesivos nas redes mundiais”, tendo como principal objetivo a proteção de menores e da dignidade da pessoa humana, relativamente contra a pornografia infantil, pedofilia, tendências xenófobas ou racistas. As linhas de ação desse plano, adotado para os anos 1999-2002, visavam o prisma da proteção da criança em relação a conteúdos que, mesmo não tendo carácter pornográfico ou pedófilo, poderiam colocar a criança em risco. As principais linhas de ação eram as seguintes:

³⁹³ Gabinete Cibercrime, Colóquio, *As crianças e a Internet, uso seguro, abuso e denúncia*, Procuradoria-Geral da República, 4 de outubro de 2013, Conclusões, ponto 2.

³⁹⁴ *Pedofilia ou pornografia infantil* é um conceito que tem aumentado exponencialmente um pouco por todo o mundo, em grande parte, graças à *Internet*. Este problema tem-se agravado com o aparecimento de novas tecnologias como a *criptografia* que serve para esconder pornografia e demais materiais ofensivos em arquivos ou durante a sua transmissão.

Criptografia - origem do grego “*kryptós*” que significa escondido, oculto, mais “*grápho*” que significa grafia, escrita. É a arte ou a ciência de escrever uma cifra ou em código. Conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário o decifre e compreenda. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1033.

- Criação de uma rede europeia de linhas diretas para as quais os utilizadores possam comunicar eventuais conteúdos ilegais de que tomem conhecimento ao utilizar a *Internet*;
- Incentivo da autorregulação e da criação de códigos de conduta por parte da indústria (a este propósito surgiu o artigo 16.º da Diretiva sobre Comércio Eletrónico: Diretiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de junho de 2000);
- Desenvolvimento de sistemas de filtragem de conteúdos ilegais que permitam ao utilizador selecionar o que quer e não quer receber;
- Desenvolvimento de classificadores de fácil compreensão e mundialmente compreensíveis, por exemplo: através de uma escala numérica crescente consoante o grau de violência para os conteúdos;
- Fomento de ações de sensibilização para todos os utilizadores, nomeadamente os pais, os professores e as próprias crianças e adolescentes.³⁹⁵

Em 29 de maio de 2000, foi adotada a Decisão do Conselho n.º 2000/375/JAI³⁹⁶ especificamente relacionada com o combate à pornografia infantil na *Internet*, que impunha aos Estados Membros tomarem medidas para:

- a) Incentivar os utilizadores da *Internet* a informarem as autoridades sobre a divulgação de pornografia infantil: dever geral de informação ativa (artigo 1.º, n.º1);
- b) Criar unidades especializadas num tratamento eficaz e célere das informações, punindo este tipo de criminalidade: dever de atuação imediata das autoridades (artigo 1.º, n.º2);
- c) Promover a cooperação entre os Estados Membros, bem como com a Europol: princípio de cooperação internacional (artigo 2.º);
- d) Manter um diálogo com os *ISP's*, com vista à criação de medidas de aplicação voluntária ou juridicamente vinculativas, de eliminação da pornografia infantil da *Internet*: colaboração com os *ISP's* (artigo 3.º);
- e) Alterar, se necessário, a legislação processual penal para rápida e eficazmente combater este tipo de crimes (artigo 4.º).

³⁹⁵ Gomes, Mário M. Vargues, *O Código da Privacidade e da Proteção de Dados Pessoais na Lei e na Jurisprudência (Nacional e Internacional)*, Centro Atlântico, Portugal, 2006, p.24.

³⁹⁶ Decisão 2000/375/JAI do Conselho, de 29 de maio de 2000, sobre o combate à pornografia infantil na Internet, (JOCE L 138, de 9.6.2000).

- f) Cooperar entre si e em contacto com o sector industrial para desenvolver filtros e outros meios destinados a impedir e detetar a divulgação de pornografia infantil (artigo 5.º).

Esta Decisão de 2000, foi complementada pela Decisão-Quadro 2004/68/JAI³⁹⁷, entretanto substituída pela Diretiva 2011/93/UE do Parlamento Europeu e do Conselho de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil³⁹⁸. Esta Diretiva harmoniza na União Europeia e define uma série de crimes relativos ao abuso sexual (artigo 3.º), à exploração sexual (artigo 4.º), à pornografia infantil (artigo 5.º), mas também criminaliza novas formas de exploração de pornografia infantil através da *Internet* e o aliciamento de crianças por via eletrónica, por exemplo, através das redes sociais, para fins sexuais (artigo 6.º). Tendo em consideração a importância para o tema desta dissertação, importa analisar em maior profundidade estes tipos de criminalidade, cometida através de sistemas de informação, nomeadamente a pornografia infantil e o aliciamento.

Assim, nos termos do número 3.º do artigo 5.º da Diretiva 2011/93/UE, a obtenção intencional de acesso a pornografia infantil por meio das tecnologias da informação e da comunicação passa a ser punível em toda a União Europeia com uma pena máxima de prisão que não pode ser inferior a 1 ano. E a distribuição, difusão ou transmissão de pornografia infantil (n.º4) ou a sua oferta, fornecimento ou disponibilização (n.º5) deve ser punível com uma pena máxima de prisão não inferior a 2 anos. A produção de pornografia infantil passa a ser punível com uma pena máxima de prisão não inferior a 3 anos (n.º6).

A pornografia infantil é definida amplamente na alínea c) do artigo 2.º, como “materiais que representem visualmente crianças envolvidas em comportamentos sexualmente explícitos, reais ou simulados (i); ou “representações dos órgãos sexuais de crianças para fins predominantemente sexuais” (ii); ou materiais que representem visualmente uma pessoa que aparente ser uma criança envolvida num comportamento sexualmente explícito, real ou simulado, ou representações dos órgãos sexuais de uma pessoa que aparente ser uma criança, para fins predominantemente sexuais” (iii), ou ainda,

³⁹⁷ Decisão-Quadro 2004/68/JAI do Conselho, de 22 de dezembro de 2003, relativa à luta contra a exploração sexual de crianças e a pornografia infantil, (JOUE L 13/44, de 20.1.2004).

³⁹⁸ Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho. (JOUE L 335/1, de 17.12.2011).

“imagens realistas de crianças envolvidas em comportamentos sexualmente explícitos ou imagens realistas dos órgãos sexuais de crianças para fins predominantemente sexuais” (iv).

Esta é de facto uma definição muito ampla, já que pode conduzir à criminalização da posse, difusão, produção, transmissão de filmes como pornografia infantil onde atuam maiores de idade, mas que aparentam ser crianças, tal como prevê a subalínea iii). No entanto, em relação aos materiais que representam visualmente uma pessoa que aparenta ser uma criança, artigo 2.º alínea c), subalínea iii), cabe aos Estados Membros decidir se aplicam estes tipos legais de crime, se a pessoa que aparenta ser uma criança tiver efetivamente 18 anos ou mais no momento da representação.

Quanto ao material pornográfico referido na subalínea iv) da alínea c) do artigo 2.º da Diretiva, referente às imagens realistas, o n.º8 também permite aos Estados Membros não criminalizar a sua posse, difusão, transmissão e outras situações previstas, se for produzido e estiver na posse do produtor apenas para uso privado, não utilizar material pornográfico na aceção das subalíneas i), ii) e iii) (representações) e não existir risco da sua difusão.

Por fim, nos termos do n.º3 do artigo 8.º cabe aos Estados Membros decidir se criminalizam a “produção, aquisição ou posse de material pornográfico que envolva crianças que atingiram a maioridade sexual, quando esse material for produzido e possuído com o consentimento dessas crianças e apenas para uso privado das pessoas envolvidas, na medida em que tais actos não comportem abuso”.

É importante salientar o artigo 6.º da presente Diretiva, já que prevê o “aliciamento de crianças para fins sexuais”. Como dispõe o n.º1, os Estados Membros devem tomar as medidas necessárias para garantir que os seguintes comportamentos intencionais sejam puníveis:

- “A proposta de um adulto, feita por intermédio das tecnologias da informação e da comunicação, para se encontrar com uma criança que ainda não tenha atingido a maioridade sexual, com o intuito de cometer um dos crimes referidos no artigo 3.º, n.º 4, e no artigo 5.º, n.º 6, se essa proposta for seguida de actos materiais conducentes ao encontro, é punível com uma pena máxima de prisão não inferior a um ano.”

Ainda quanto ao aliciamento, é imposto aos Estados Membros que tomem as medidas necessárias para garantir que seja punível a tentativa de cometer, por meio das tecnologias da informação e da comunicação, os crimes previsto no artigo 5.º números 2 e 3, por um adulto que alicie uma criança que não tenha atingido a maioridade sexual a disponibilizar pornografia infantil representando essa criança (n.º2 do artigo 6.º).

Os atos de instigação, auxílio, cumplicidade e tentativa são igualmente punidos segundo o artigo 7.º. Assim, os Estados Membros devem adotar as medidas necessárias para garantir que a instigação ou o auxílio e a cumplicidade na prática dos crimes referidos nos artigos 3.º a 6.º sejam puníveis (n.º1, artigo 7.º).

A tentativa é também punível, nos termos do n.º 2 do artigo 7.º. Os Estados Membros devem tomar as medidas necessárias para garantir que a tentativa da prática dos crimes referidos no artigo 3.º, números 4, 5 e 6, no artigo 4.º números 2, 3, 5, 6 e 7, e no artigo 5.º, números 4, 5 e 6 seja punível.

O artigo 9.º é muito importante, já que diz respeito às circunstâncias agravantes para estes casos, nomeadamente, quanto aos crimes referidos nos artigos 3.º a 7.º que envolvem as Tecnologias da Informação:

- a) O crime ser cometido contra uma criança numa situação particularmente vulnerável, nomeadamente devido a deficiência mental ou física, a uma situação de dependência ou a um estado de incapacidade física ou mental;
- b) O crime ser cometido por um membro da família da criança, por uma pessoa que coabita com a criança ou por uma pessoa que abusou de posição manifesta de confiança ou de autoridade;
- c) O crime ser cometido por várias pessoas em conjunto;
- d) O crime ser cometido no âmbito de uma organização criminosa na aceção da Decisão-Quadro 2008/841/JAI do Conselho, de 24 de outubro de 2008, relativa à luta contra a criminalidade organizada³⁹⁹;
- e) O autor do crime já ter sido condenado por crimes da mesma natureza;
- f) O autor do crime por em perigo, deliberadamente ou por imprudência, a vida da criança;

³⁹⁹ Decisão-Quadro 2008/841/JAI do Conselho, de 24 de outubro de 2008, relativa à luta contra a criminalidade organizada, (JOUE L 300/42, de 11.11.2008), p. 42.

- g) O crime ter sido cometido com especial violência ou ter causado danos particularmente graves à criança”.

Ainda quanto aos artigos 3.º a 7.º, impõe o n.º1, do artigo 12.º, que os Estados Membros tomem “as medidas legislativas e outras que se revelem necessárias para garantir que as pessoas colectivas possam ser consideradas responsáveis pelas infracções penais presentes na presente Convenção, cometidas em seu benefício por qualquer pessoa singular, agindo individualmente ou enquanto membro de um órgão da pessoa coletiva, que nela ocupe uma posição de liderança, com base”:

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

Os Estados Membros devem tomar as medidas necessárias para garantir que as pessoas coletivas possam ser responsabilizadas, caso a falta de supervisão ou de controlo por parte de uma pessoa referida no n.º1 torne possível que uma pessoa sob a sua autoridade cometa um dos crimes referidos nos artigos 3.º a 7.º, em benefício dessa pessoa coletiva (n.º2 do artigo 12.º).

Por fim, importa salientar que a responsabilidade das pessoas coletivas previstas nos números 1 e 2 deste artigo, não exclui a instauração de ações penais contra as pessoas singulares que sejam autoras, instigadoras ou cúmplices dos crimes referidos nos artigos 3.º a 7.º (n.º3 do artigo 12.º).

Quanto às medidas de natureza processual encontram-se previstas nos artigos 15.º e 17.º.

Começando pela análise do artigo 15.º, relativo à “Investigação e acção penal”, o n.º1 do referido artigo impõe aos Estados Membros que tomem as medidas necessárias para garantir que a investigação ou a acção penal relativas aos crimes referidos nos artigos 3.º a 7.º não dependam de queixa ou de acusação efetuadas pela vítima ou pelo seu representante, e que a acção penal possa prosseguir, mesmo que essa pessoa retire as suas declarações. Este artigo pode ser um bom incentivo para os inúmeros casos de desistências de denúncia dos abusos, na grande maioria, motivados por medo ou coação.

É ainda imposto aos Estados Membros que tomem as medidas necessárias para permitir a ação penal por um dos crimes referidos no artigo 3.º, no artigo 4.º, números 2, 3, 5, 6 e 7, e por um dos crimes graves referidos no artigo 5.º, n.º6, caso tenha sido utilizada pornografia infantil na aceção do artigo 2.º, alínea c), subalíneas i) e ii), durante um período suficiente após a vítima ter atingido a maioridade e proporcional à gravidade do crime em causa (n.º2 artigo 15.º).

Os Estados Membros devem ainda tomar as medidas necessárias para garantir que as pessoas, as unidades ou os serviços responsáveis pela investigação ou pela ação penal relativa aos crimes referidos nos artigos 3.º a 7.º tenham acesso a instrumentos de investigação eficazes, tais como os instrumentos utilizados no caso da criminalidade organizada e de outros crimes graves (n.º3 artigo 15.º).

Neste âmbito, os Estado Membros devem igualmente adotar as medidas necessárias para permitir que as unidades ou serviços de investigação consigam identificar as vítimas dos crimes referidos nos artigos 3.º a 7.º, especialmente através da análise de matérias de pornografia infantil, tais como fotografias ou gravações audiovisuais transmitidas ou disponibilizadas por meio das tecnologias da informação e da comunicação (n.º4 artigo 15.º).

Quanto ao artigo 17.º relativo à “competência jurisdicional e coordenação da acção penal”, determina no seu n.º 1 que os Estados Membros devem adotar as medidas necessárias para estabelecer a sua competência jurisdicional relativamente aos crimes referidos nos artigos 3.º a 7.º, caso:

- a) “O crime seja cometido, total ou parcialmente, no seu território; ou
- b) O autor do crime seja seu nacional.”

Segundo o n.º2 do mesmo artigo, os Estados Membros devem informar a Comissão, caso decidam estender a sua competência jurisdicional aos crimes referidos nos artigos 3.º a 7.º cometidos fora do seu território, nomeadamente, se:

- a) “O crime for cometido contra um dos seus nacionais ou contra uma pessoa que resida habitualmente no seu território; ou
- b) O crime for cometido em benefício de uma pessoa colectiva estabelecida no seu território; ou
- c) O autor do crime residir habitualmente no seu território.”

Os Estados Membros devem garantir que a sua competência jurisdicional abranja as situações em que um crime referido nos artigos 5.º e 6.º e, se for relevante, nos artigos 3.º e 7.º, seja cometido por meio de tecnologias de informação e da comunicação acessíveis no seu território, independentemente de estarem ou não baseadas no seu território (n.º3 artigo 17.º).

Para a instauração de ações penais relativas aos crimes referidos nos artigos 3.º a 7.º cometidos fora do território do Estado Membro em causa, em relação aos casos previstos no n.º1, alínea b), do presente artigo, ou seja, quando o autor do crime seja seu nacional, os Estados Membros devem tomar as medidas necessárias para garantir que a sua competência jurisdicional não dependa da condição de a ação penal só se poder iniciar após ser feita uma queixa pela vítima no lugar em que o crime foi cometido ou uma denúncia do Estado em cujo território o crime foi cometido (n.º5 artigo 17.º).

É importante salientar o artigo 23.º relativo à “Prevenção”, já que os crimes sexuais que envolvem crianças tendem a aumentar, em grande parte graças às novas ferramentas das Tecnologias de Informação e Comunicação. Desta forma, realça o n.º1 do referido artigo, os Estados Membros devem tomar as medidas adequadas, como a educação e a formação, para desencorajar e reduzir a procura que favoreça todas as formas de exploração sexual de crianças.

Da mesma forma, devem tomar medidas adequadas, nomeadamente através da *Internet*, tais como campanhas de informação e sensibilização, programas de investigação e educação, se necessário em cooperação com as organizações relevantes da sociedade civil e com outros interessados, para aumentar a consciencialização sobre este problema e como forma de reduzir o risco de as crianças poderem ser vítimas de abuso ou exploração sexual (n.º2 artigo 23.º).

Assim, os Estados Membros devem promover a formação regular dos seus funcionários suscetíveis de entrar em contacto com crianças vítimas de abuso ou exploração sexual, incluindo os agentes da polícia no terreno, com o intuito de lhes permitir identificar e lidar com as várias situações de crianças vítimas e potenciais vítimas de abuso ou exploração sexual (n.º3 artigo 23.º).

A maioria destes atos são filmados e colocados na *Internet*, nomeadamente em sítios eletrónicos ligados à pedofilia ou pornografia infantil. Como tal, é imperativo que os

Estados eliminem estes sítios, já que são a principal forma de transmissão e divulgação de vídeos e fotografias. O artigo 25.º, relativo às “medidas contra sítios da Internet que contenham ou divulguem pornografia infantil”, é muito importante já que impõe aos Estados Membros que eliminem os sítios eletrónicos alojados no seu território que contenham ou difundam pornografia infantil e se esforcem por eliminar os que estão alojados no estrangeiro (n.º1 artigo 25.º).

Os Estados Membros devem ainda tomar as medidas necessárias para bloquear o acesso às mesmas páginas sediadas no seu território. Estas medidas devem ser adotadas através de processos transparentes e devem incluir garantias adequadas, nomeadamente para assegurar que a restrição se limite ao que é necessário e proporcionado, e que os utilizadores sejam informados do motivo das restrições. Essas garantias devem ainda incluir a possibilidade de recurso judicial (n.º2 artigo 25.º).

Um das dificuldades da repressão criminal da pornografia infantil através da *Internet* prende-se com a sua descoberta e investigação. A forma mais fácil e mais utilizada na descoberta de práticas ilegais, nomeadamente as praticadas por pedófilos, consistem na atuação de agentes infiltrados. Nestes atos, o agente da polícia de investigação assume uma determinada identidade na *Internet*, mais concretamente, em salas de *chat* ou em *newsgroups*, onde, na maioria dos casos assumem, identidades de crianças e jovens, por serem os alvos mais procurados. Também são já conhecidos os casos de presença destes agentes nas novas redes sociais, tais como *Facebook*, *Twitter*, *Instagram*, por conterem, na maioria das vezes, vídeos e imagens pessoais de crianças e adolescentes. As autoridades alertam, ainda, para o aumento da exposição de dados e fotografias pessoais e da necessidade de se proteger ao máximo a identidade das crianças, na maioria dos casos dos próprios filhos, que os utilizadores colocam nestas redes sociais.

Os agentes entram nas salas de conversação (salas de *chat*) usando *nicknames* (nomes falsos) sugestivos, como “*like young*” ou “*pre-teen girls*”, de modo a atrair um maior número de potenciais agentes (pedófilos). Apresentam-se como adolescentes, ou como adultos interessados em pornografia envolvendo crianças, esperando ser solicitados para conversa (*chat*).⁴⁰⁰

⁴⁰⁰ Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 511.

Mas não basta criminalizar e dotar os serviços responsáveis pela perseguição criminal de meios para combater eficazmente este fenómeno. A vertente preventiva é igualmente muito importante. A este propósito é essencial o envolvimento dos ISP's dos utilizadores da *Internet*, em geral. Por exemplo, nos Estados Unidos da América, os ISP's estão a ser abrangidos por uma medida legislativa designada como “cláusula do bom samaritano”, incluída no *Tellecommunications Act de 1996*, criada de forma a incentivar os cidadãos ao auxílio ao combate à disseminação da pornografia infantil através do controle dos conteúdos da *Internet*.⁴⁰¹

Atualmente, e não obstante alguns navegadores já facultarem a possibilidade de controlo da informação a receber, como é o caso do *Internet Explorer* e *Mozilla Firefox*, a verdade é que são ainda muitos os que não dispõem dessa função e tornam possível que qualquer utilizador, incluindo crianças, aceda a sítios de pornografia, conteúdos difamatórios, obscenos ou racistas/xenófobos, sem qualquer limitação e sem que seja possível em termos legais sancionar a entidade proprietária do sítio, precisamente porque não existe a obrigatoriedade legal de classificação de conteúdos.

Em nossa opinião, a solução ideal passa, assim, por uma maior colaboração das empresas dos sítios mais influentes com os órgãos de segurança. É necessário que empresas como a *Google*, *Facebook*, *Youtube*, já que são empresas com um elevado número de utilizadores, na sua maioria jovens, cooperem e colaborem lado a lado com as entidades ligadas ao combate à pornografia infantil, para diminuir estes casos. De igual forma, é importante classificar certos sítios eletrónicos, onde sejam mostradas fotografias ou vídeos, de acordo com uma escala referente ao conteúdo que estes disponibilizam, por exemplo: aos sítios com características e comentários xenófobos/racistas era dada uma classificação; se o conteúdo fosse de cariz sexual ou pornográfico tinha outro, e assim sucessivamente. Quanto mais elevado fosse o número, maior perigo este representava para os utilizadores. Desta forma e graças a esta classificação, todos os utilizadores estavam cientes do conteúdo que iam encontrar, os perigos que corriam e as consequências das suas ações, pelo menos quanto aos tipos mais comuns e lesivos.

Neste âmbito, destacamos pela positiva, a parceria entre a *Microsoft* e a Universidade de Dartmouth em 2009, em que desenvolveram um *software* chamado *PhotoDNA*, cujo

⁴⁰¹ Raínha, Paula; Vaz, Sónia Queiróz, *Guia Jurídico da Internet em Portugal*, ed., CENTROATLANTICO.PT, Portugal, 2001, p.74.

objetivo é o de facilitar a deteção e remoção das piores imagens de pornografia infantil disponíveis *online*. O funcionamento do *PhotoDNA* assenta na descoberta de um conjunto de características únicas em cada fotografia que permite distingui-la de qualquer outra imagem e que são identificáveis mesmo que seja alterada, que perca a definição ou mesmo que seja redimensionada.⁴⁰² A extração desta informação visa permitir detetar cópias de certas imagens previamente analisadas em sistemas informáticos como computadores ou servidores. Assim, com base na recolha de uma fotografia com conteúdo pedo-pornográfico e imediata extração do seu *PhotoDNA*, torna-se possível, com 100% de fidedignidade, detetar cópias dessa imagem em servidores e, em última instância, identificar o indivíduo que as detém ou que as disponibilizou.⁴⁰³

Importa salientar que este *software* é cedido de forma gratuita às entidades policiais que o solicitem.

⁴⁰² Ramalho, David Silva, “A Investigação Criminal na Dark Web”, in *Revista de concorrência e regulação*, Coimbra, a.4n.14-15, Abr.-Set.2013, pp. 420 e 421. A este respeito veja-se a página da *Internet* disponibilizada pela *Microsoft* com a explicação do *PhotoDNA*, [Em linha]. Disponível em www.microsoft.com/en-us/news/presskits/photodna/.

⁴⁰³ Trata-se de uma tecnologia que foi inicialmente cedida ao *National Center for Missing & Exploited Children* (NCMEC), já que este centro contém mais de 65 milhões de imagens e vídeos de exploração sexual infantil, e que entretanto já foi instalada nos servidores da própria *Microsoft*, bem como, desde 2011, do *Facebook*. Está também prevista a sua gradual implementação no motor de busca *Bing*, *Skydrive* e no *Hotmail*. Ramalho, David Silva, “A Investigação Criminal na Dark Web”, in *Revista de concorrência e regulação*, Coimbra, a.4n.14-15, Abr.-Set.2013, p. 421.

5. A Cibercriminalidade no plano internacional

5.1. - Tendências

Nas últimas duas décadas a *Internet*, e mais genericamente, o *Ciberespaço* tiveram um papel fundamental na evolução de todos os setores da sociedade: a vida diária, os direitos fundamentais, as interações sociais e económicas dependem do bom funcionamento das tecnologias de informação e das comunicações.

Um *Ciberespaço* aberto e livre tem promovido a inclusão política e social em todo o mundo, da mesma forma que derrubou barreiras entre países, comunidades e cidadãos, aproximando-os cada vez mais uns dos outros, através da partilha de informações e ideias entre todos os pontos do globo, do mesmo modo que proporcionou um aumento da liberdade de expressão e o exercício dos direitos fundamentais.⁴⁰⁴

As tecnologias da informação e das comunicações tornaram-se o pilar fundamental do crescimento económico e são um recurso crítico de que todos os setores económicos dependem. Estas estão atualmente na base dos complexos sistemas que fazem funcionar as economias em setores fundamentais como as finanças, a saúde, a energia e os transportes. Do mesmo modo, encontram-se cada vez mais nos modelos de negócios construídos com base na disponibilidade ininterrupta da *Internet* e no bom funcionamento dos sistemas informáticos.⁴⁰⁵

É graças à *Internet* e às novas tecnologias que assistimos ao aumento de pequenas e médias empresas, à criação de novos negócios (*e-business*), não só nacionais mas internacionais, novas formas de ensino (*e-learning*) e de lazer (*e-book*⁴⁰⁶), novas formas de comércio (*e-commerce*), bem como novas formas de adquirir bens e serviços (*e-procurement*⁴⁰⁷).

⁴⁰⁴ (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p. 2.

⁴⁰⁵ *Idem, Ibidem*.

⁴⁰⁶ *E-Book* - Livro escrito ou disponibilizado em formato eletrónico. Os formatos mais utilizados são em *PDF* (*Adobe Reader*) e *DOC* (*Microsoft Word*). *E-Book* também pode significar um livro eletrónico; título autoral (livros, estudos, artigos) que é compilado na forma de *software* e disponibilizado, de forma gratuita ou onerosa, na *Internet*. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p.1033.

⁴⁰⁷ *E-Procurement* - a palavra “*procurement*” significa adquirir, comprar. Consiste numa aplicação ou num *website* que tem por objetivo a aquisição de mercadorias, produtos ou serviços, geralmente suprimentos para posterior fornecimento a outros interessados. *Idem, Op. Cit.*, p.1034.

Não obstante a evolução tecnológica ao longo dos últimos anos ter proporcionado enormes benefícios⁴⁰⁸, veja-se, por exemplo: os avanços realizados na área da Saúde através dos meios tecnológicos, na área da Biologia, da Física, da Química e até na área do Ensino, tem igualmente criado um mundo digital bastante vulnerável.

As quebras das redes de segurança, na maioria das vezes provenientes de ataques contra os sistemas informáticos, intencionais ou acidentais, estão a aumentar a um ritmo preocupante, já que são perpetrados em grande escala e poderão pôr em risco a prestação de serviços fundamentais para a vivência em sociedade, tais como: os cuidados de saúde, os acessos a tribunais e órgãos de polícia, bem como a garantia dos serviços de abastecimento de água, de eletricidade, gás, ou serviços móveis.

Em 2008, o Fórum Económico Mundial calculou que a probabilidade de ocorrer uma rutura importante nas *Infraestruturas Críticas da Informação* nos próximos 10 anos era de 10% a 20%, com um potencial custo económico global de cerca de 250 000 000 000 USD.⁴⁰⁹

O aumento da espionagem económica e de atividades patrocinadas no mundo tecnológico coloca os governos e as empresas dos vários Estados à mercê de uma nova categoria de ameaças. Estas ameaças podem ter diversas origens: ataques criminosos, ataques politicamente motivados, terroristas ou patrocinados por Estados extremistas⁴¹⁰, assim como catástrofes naturais e erros involuntários. De igual forma, os ataques tendem a ser cada vez mais frequentes e cada vez mais desenvolvidos, não sendo possível, na maioria dos casos, identificar o autor.

Outra das tendências que apontamos quanto ao futuro da *Cibercriminalidade* será a diminuição da vida privada. Segundo alguns autores, prevê-se uma maior exposição da vida privada de cada um, criando assim, um menor controlo do cidadão quanto aos seus dados pessoais e à sua segurança, bem como um menor controlo dos terminais de comunicação e maior dano económico resultante da combinação dos fatores

⁴⁰⁸ Uma vez concretizado o mercado único digital, a Europa poderá aumentar o seu Produto Interno Bruto (*PIB*) em quase 500.000 milhões de euros por ano, uma média de 1.000 euros por pessoa. *Idem, Ibidem.*

⁴⁰⁹ Global Risks, 2008.

⁴¹⁰ Antonio Forzieri (EMEA Cyber Security conduit for confidence organization Symantec) refere que Israel tem vindo a aumentar o seu número de *hackers* e que estes são “assustadoramente talentosos” [Em linha]. Disponível em www.worldnewspaperonline.com

anteriormente referidos.⁴¹¹ Mesmo com as transferências para a chamada “*cloud*”, mais segura do ponto de vista técnico, a vulnerabilidade estará sempre do lado do utilizador.

À medida que aumenta a frequência destes ataques, aumenta, simultaneamente, a gravidade dos seus resultados.

De uma forma geral, a tendência será: o aumento da *Cibercriminalidade*, a diminuição da privacidade e da segurança dos cidadãos, das empresas, órgãos do Estado e consequentemente, o aumento da desconfiança dos cidadãos quanto à *Internet*.

Todos estes fatores evidenciam os novos desafios tecnológicos e por que razões os governos de todo o mundo consideram o *Cibercrime* uma questão internacional cada vez mais importante.

⁴¹¹ Entrevista a Rogério Bravo, Inspetor-Chefe, Polícia Judiciária de Lisboa, no dia 18 de fevereiro de 2014.

5.2. - Dificuldades da experiência prática e tentativas de resolução

Como vimos no ponto anterior, é fundamental que sejam tomadas medidas de prevenção não só por parte da União Europeia, mas por parte de todos os Estados, no combate à *Cibercriminalidade*. No entanto, colocam-se vários entraves a esta atuação.

Nos pontos seguintes destacamos as principais dificuldades no combate à *Cibercriminalidade*:

- A transnacionalidade, com a ausência de fronteiras no mundo digital torna-se quase impossível identificar os agentes, os seus ataques e os locais de onde provêm esses ataques.⁴¹²
- Os diferentes tipos de criminalização que aliados à transnacionalidade dificultam a aplicação de uma única jurisdição e, consequentemente, a atuação e cooperação internacional.⁴¹³
- A ausência de legislação especificamente tecnológica, ou seja, as leis criminais são tradicionalmente criadas para a proteção de objetos materiais e não de objetos imateriais ligados ao *Cibercrime*, como dados e informações digitais.⁴¹⁴
- O aumento de ataques informáticos. Graças à proliferação de novos sistemas informáticos e consequentemente, de novas formas de crimes tecnológicos,

⁴¹² O *Cibercrime* não pode ser considerado um “novo” tipo de crime que é capaz de transpor várias jurisdições e leis, já que existem outros exemplos como: o tráfico de pessoas, drogas ou armas, que frequentemente “circulam” entre várias fronteiras e Estados. No entanto, o perigo dos ataques de *cibercrime* é que podem abranger várias jurisdições, em segundos. UNODC, United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, February 2013, United Nation, New York, 2013, p. 56.

⁴¹³ Um exemplo: Um cidadão da Oceânia fez um “upload” de um documento legal que continha expressões de ódio, num servidor do seu próprio país. Foi feito *download* desse documento num país europeu. Posteriormente, quando o cidadão viajou para esse país europeu, foi detido e sentenciado por tais atos, que não constituíam crime no seu país de origem. O caso foi discutido. No entanto, o Supremo Tribunal Federal do país europeu susteve a mesma sentença. Argumentou, que, embora o agente não tivesse atuado nem no país europeu, nem tenha enviado o referido ficheiro para o país europeu, no entanto, ameaçou a paz pública no território, tal como exigido pelo estatuto relevante. O Tribunal salientou, porém, que a interpretação não poderia ser generalizada para outros estatutos sobre conteúdo ilegal. (Tradução livre). UNODC, United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, February 2013, United Nation, New York, 2013, p. 56, *apud.*, Judgement of the German Bundesgerichtshof of 1 December 2000 (1 StR 184/00, BGH MMR 2001, pp.228 et seqq.)

⁴¹⁴ Por exemplo: o conceito de “roubo” tem o mesmo significado em várias leis nacionais de vários países. Mas o “roubo” de dados ou informações digitais, por exemplo, pode não fazer parte do enquadramento do tipo legal de “roubo”. Este exemplo demonstra a necessidade de, em algumas áreas, ser feita uma adaptação doutrinária às novas informações tecnológicas. (Tradução livre). UNODC, United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, February 2013, United Nation, New York, 2013, p. 51 *apud.*, Sieber, U., *Straftaten und Strafverfolgung im Internet*, in *Gutachten des Deutschen Juristentags*, Munich: C.H. Beck, 2012, pp. C14-15.

assistimos ao aumento destes ataques, bem como ao aumento da gravidade dos mesmos.

- O aumento do número de agentes criminosos que atuam isoladamente ou em grupo.
- A fraca capacidade de alerta e de resposta, face a este tipo de crimes informáticos. Na maioria dos casos, os ataques informáticos acontecem muito tempo antes de ser dado o alerta para o perigo, não sendo desde logo perceptíveis. E, quando o são, é necessário desencadear uma série de mecanismos que dependem da atuação de várias entidades, o que gera uma lentidão dos meios de defesa. Como acontece, por exemplo, no caso das bases de dados, das operadoras telefónicas, dos registos de *IP*.⁴¹⁵
- A maior fluidez dos elementos de prova, que aliada à facilidade com que estes dados podem ser apagados ou alterados, torna difícil o combate a este tipo de ataques.⁴¹⁶
- O mau uso dos meios tecnológicos por parte dos cidadãos. O aumento da exposição pública, o descuido e o desinteresse em salvaguardar informações e dados pessoais são outro dos pontos que mais têm preocupado as autoridades. Casos como a pedofilia e a pornografia infantil são exemplos de crimes que aumentaram de forma exponencial nos últimos tempos.⁴¹⁷

Perante estas dificuldades, a Europa permanecerá vulnerável se não for feito um esforço substancial para melhorar as capacidades, os recursos e os processos públicos e privados para prevenir, detetar e dar resposta aos incidentes resultantes da *Cibercriminalidade*.

⁴¹⁵ São claros exemplos de cooperação entre os próprios organismos e os órgãos de defesa no combate ao *Cibercrime*, que, no entanto, não conseguem dar uma resposta rápida, já que esta cooperação padece ainda de muitos formalismos.

⁴¹⁶ Os mecanismos de governação só serão verdadeiramente eficazes se todos os participantes puderem trabalhar com informações fiáveis, condição esta que é de extrema importância para os governos, já que são os principais responsáveis por garantir a segurança e o bem-estar dos cidadãos. (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p.6.

⁴¹⁷ Paralelamente surgiram novas ferramentas capazes de ocultar este tipo de crimes, como é o caso da *criptografia*. Serve para esconder pornografia e demais materiais ofensivos em arquivos ou durante a sua transmissão. Conjunto de técnicas que permite tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário a decifre e compreenda. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1033.

Como tentativas de resolução, destacamos:

- O desenvolvimento da cooperação entre as várias entidades, quer a nível internacional quer a nível nacional, com responsabilidades na área criminal de modo a permitir uma eficaz investigação dos crimes, a conservação do material probatório (como preveem os artigos 12.º e seguintes da Convenção sobre o Cibercrime), a captura dos criminosos e o seu efetivo sancionamento.
- Os direitos individuais não podem ser assegurados sem redes e sistemas seguros. Assim, é necessário que toda a partilha de informações, quando estejam em causa dados pessoais, respeite a legislação da União Europeia sobre proteção de dados e tenha plenamente em conta os direitos individuais neste domínio. Desta forma, todos os intervenientes relevantes sejam autoridades públicas, o setor privado ou os cidadãos individualmente, têm de adotar medidas para se protegerem⁴¹⁸.
- A adoção de legislação sobre *Cibercrime* que permita:
 1. Definir padrões claros de comportamentos a adotar no uso de aparelhos tecnológicos;
 2. Dissuadir os infratores e proteger os cidadãos;
 3. Facilitar as investigações criminais, mas protegendo a privacidade dos utilizadores;
 4. Garantir procedimentos criminais justos e efetivos;
 5. Requerer padrões mínimos de proteção em áreas como manipulação de dados e retenção;
 6. Facilitar a cooperação entre países sobre matérias criminais, como o *Cibercrime* e provas eletrónicas.⁴¹⁹

Em face do exposto, concluímos que a adoção de novas medidas legislativas terá um papel fundamental na prevenção e combate à *Cibercriminalidade*, abrangendo várias áreas: criminalização, poderes processuais, jurisdição, cooperação internacional e responsabilidade dos prestadores de serviço (*Internet Service Providers*).

⁴¹⁸ (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p.2.

⁴¹⁹(Tradução livre). UNODC, United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, February 2013, United Nation, New York, 2013, p. 52.

Capítulo III - A resposta do Direito à Cibercriminalidade

1. - O Direito Internacional Público

A era da *Internet* coloca enormes desafios à escala global, que os Estados isoladamente considerados não têm capacidade para debelar. Devido à sua escala global, à sua crescente acessibilidade e ao anonimato que proporciona, a *Internet* facilita o crime transnacional, ao mesmo tempo que dificulta a atuação das autoridades responsáveis pela perseguição criminal, tradicionalmente limitadas pelo princípio da territorialidade da jurisdição criminal.⁴²⁰

O carácter global da *Internet* exige, pois, uma ação da comunidade internacional para regular e criar um espaço novo e global de ação policial e perseguição criminal. No entanto, o desenvolvimento da cooperação internacional tem envolvido algum esforço por parte dos governos, já que uma atuação conjunta implica uma certa perda de soberania. Como refere Manuel Castells, “de facto, ao fazer isto, perderam soberania, já que se viram obrigados a partilhar o poder e a pôr-se de acordo em relação a normas comuns de regulamentação, de maneira que eles mesmos se converteram numa rede, uma rede de agências de regulamentação e controlo policial. Mas a soberania partilhada foi o preço que teve de pagar-se para reter, de modo colectivo, algum grau de controlo político”⁴²¹.

Tornara-se claro que a infraestrutura de comunicações informáticas da qual dependiam a riqueza, a informação e o poder de todo o mundo era bastante vulnerável à intrusão e interferência de agentes mal-intencionados.⁴²² A verdade é que a segurança global da rede era muito fraca e facilmente penetrável, em grande parte, graças à ausência de fronteiras e jurisdições capazes de regular a mesma. Como refere Manuel Castells “se se consegue entrar numa rede por qualquer um dos seus pontos, resulta que se pode circular pelos seus diversos nós com relativa facilidade”.⁴²³

O uso de novas tecnologias não traz apenas benefícios para as sociedades, constitui também a oportunidade de cometer novos tipos de crimes, tais como: criação e

⁴²⁰ Cfr., Clough, Jonathan, *Principles of Cybercrime*, Cambridge University Press, Cambridge, 2010, pp.5 e ss.

⁴²¹ Castells, Manuel, *A Galáxia Internet, Reflexões sobre Internet*, Negócios e Sociedade, pp. 211 e 212.

⁴²² *Idem*, *Op. Cit.*, p.210.

⁴²³ *Idem*, *Op. Cit.*, p.211.

divulgação de vírus informáticos, *phishing*⁴²⁴, criação de *botnets*, ou crimes mais tradicionais com recurso às novas tecnologias, como, por exemplo, os crimes de pedofilia e pornografia infantil, ou tráfico e exploração de seres humanos.⁴²⁵

Paralelamente, surgem novos tipos de agentes, como os chamados *Hackers* ou *Crackers* que atravessam as barreiras dos computadores (a chamada *firewall*⁴²⁶) com o intuito de prejudicar terceiros, através do furto de números de cartões de crédito, envio de vírus informáticos, desativar ou alterar o conteúdo de sítios eletrónicos de cariz político ou de entidades governamentais, entre outros exemplos.

Dada a natureza global das redes de informação, nenhuma política de combate à *Cibercriminalidade* pode ser eficaz se os esforços de cooperação se limitarem apenas à União Europeia. Os criminosos podem atacar sistemas de informação ou cometer crimes de um Estado Membro para outro, mas também a partir de territórios exteriores à União Europeia.⁴²⁷

As instâncias governamentais, bem como as internacionais, têm consciência de que este é um tema cada vez mais global e que o aumento do número de casos deste crime se traduz, cada vez mais, numa preocupação. Ao longo dos últimos anos, este tema tem sido debatido na União Europeia⁴²⁸, no Grupo dos 8 (G8)⁴²⁹, na OCDE⁴³⁰, nas Nações Unidas⁴³¹ e no Conselho da Europa⁴³².

⁴²⁴ *Phishing* (ou em Português “*Ciber-iscagem*”) - por *phishing* entende-se as tentativas fraudulentas de obtenção de informações sensíveis, como senhas e dados do cartão de crédito, através de uma comunicação eletrónica, utilizando uma identidade falsa que se faz passar por verdadeira. (COM (2007) 267 final), *Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões*, “Rumo a uma Política geral de luta contra o Cibercrime”, [Em linha], Bruxelas, 22.5.2007,p.3.

⁴²⁵ *Parecer 4/2001*, relativo ao “Projeto de Convenção do Conselho da Europa sobre Cibercriminalidade”, Adotado em 22 de março de 2001, p.2. Disponível em http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm, (consultado em 12.11.2014).

⁴²⁶ *Firewall*- sistema de proteção contra a saída de dados ou a entrada de interferências provenientes de um sistema exterior. Ponto de conexão da rede com o mundo externo, tudo o que chega passa pelo *firewall*, que decide o que pode ou não entrar, dependendo do nível de segurança criado pela entidade. O *firewall* analisa o tráfego entre a rede interna e a rede externa em tempo real, permitindo ou bloqueando o tráfego de acordo com as regras definidas previamente. Todavia, o *firewall* não protege de infeção com vírus, *trojans*, sejam decorrentes de *downloads*, anexos a mensagens de correio eletrónico. Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 1034.

⁴²⁷ Esta possibilidade de os cibercriminosos cometerem os ataques informáticos a partir de qualquer parte, deve-se à sua transnacionalidade. Como iremos abordar mais à frente, a *transnacionalidade* é uma das características que mais dificulta o combate à *Cibercriminalidade*.

⁴²⁸ Temos como exemplo a *Comunicação da Comissão ao Conselho e ao Parlamento Europeu* “Criar uma Sociedade da Informação mais segura reforçando a segurança das infraestruturas de informação e

Atualmente as *Tecnologias da Informação e das Comunicações* são uma realidade cada vez mais presente na nossa sociedade. Estes sistemas, serviços, redes e infraestruturas tecnológicas são uma parte vital da nossa economia e da nossa sociedade, já que dependemos do uso destas no dia-a-dia. Como tal, são, em geral, consideradas *Infraestruturas Críticas da Informação (ICI)*, já que a sua perturbação ou a sua destruição teria um forte impacto nas funções vitais da sociedade. Como exemplo desse impacto, destacamos os *ciberataques* ocorridos em grande escala contra a Estónia em 2007, contra a Lituânia e contra a Geórgia, bem como os cortes de cabos transcontinentais em 2008.⁴³³

O papel económico e social do sector das *Tecnologias da Informação e das Comunicações e das Infraestruturas* é sublinhado em relatórios recentes sobre a inovação e o crescimento económico, como a comunicação sobre a avaliação intercalar

lutando contra a cibercriminalidade”, [Em linha], 26.1.2001. Disponível em <http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html>, (consultado em 12.11.2014).

⁴²⁹ Temos como exemplo a Recomendação 3/99 relativa à conservação dos dados referentes ao tráfego, por parte dos fornecedores de serviços *Internet*, para efeitos de aplicação da lei, [Em linha], 7.9.1999. Disponível em http://europa.eu/comm/internal_market/en/media/dataprot/wpdocs/index.htm, (consultado em 12.11.2014).

⁴³⁰ OCDE - A Organização para a Cooperação e Desenvolvimento Económico adotou 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).

⁴³¹ Nações Unidas - A Assembleia Geral das Nações Unidas adotou a 15 de novembro de 2000, a *Convenção das Nações Unidas contra o Crime Organizado Transnacional* que no seu artigo 27.º n.º3 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).

⁴³² Grupo de Trabalho de Proteção de Dados, *Parecer 4/2001, relativo ao Projeto de Convenção do Conselho da Europa sobre Cibercriminalidade*, [Em linha], 22.3.2001, Bruxelas, p.2. Disponível em http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm, (consultado em 12.11.2014).

⁴³³ (COM (2009) 149 final), *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, relativa à “proteção das infraestruturas críticas da informação – Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência”, Bruxelas, 30.3.2009, p.2.

da iniciativa i2010⁴³⁴, o relatório do grupo Aho⁴³⁵ e os relatórios económicos anuais da União Europeia⁴³⁶.

Também a OCDE tem sublinhado a importância das *Tecnologias da Informação e das Comunicações* e da *Internet* para estimular o desempenho económico e o bem-estar social e reforçar a capacidade das sociedades para melhorarem a qualidade de vida dos cidadãos no mundo inteiro.

Assim, hoje mais do que nunca, deparamo-nos com uma urgência de aprender a governar a globalização e os perigos que esta acarreta. A defender as tecnologias da informação e das comunicações e as infraestruturas críticas da informação, já que o desenvolvimento e sustentabilidade dos Estados, enquanto pequenas sociedades do mundo, dependem de uma infraestrutura coesa e segura. Como tal, é necessário tomar medidas internacionais contra estes ataques e prevenir que o bom funcionamento das infraestruturas não seja posta em causa.

No mundo globalizado a interação entre as diferentes ordens jurídicas e jurisdições é essencial para um combate eficaz à *Cibercriminalidade*, um fenómeno transnacional por natureza. No entanto, a existência de diferentes legislações nacionais pode conduzir à criação de “portos seguros” para os autores dos crimes, pelo que uma harmonização das legislações dos Estados constitui uma medida importante para um combate eficaz a esta forma de criminalidade.⁴³⁷ Por outro lado, a cooperação judiciária internacional é igualmente relevante. Daí que uma regulação através de instrumentos de Direito Internacional Público seja, hoje, essencial para a prevenção e combate à criminalidade.

⁴³⁴ (COM (2008) 199 final), *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões*: “Preparar o futuro digital da Europa; revisão intermédia da iniciativa i2010”, [Em linha], Bruxelas, 17.4.2008. Disponível em <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0199:FIN:ES:PDF>, (consultado em 12.11.2014).

⁴³⁵ Disponível em http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm, (consultado em 12.11.2014).

⁴³⁶ *The EU Economy: 2007 Review*, [Em linha]. Disponível em http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf, (consultado em 12.11.2014).

⁴³⁷ UNODC, United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, February 2013, United Nations, New York, 2013, pp. 58 e ss.

1.1. – Principais instrumentos de Direito Internacional

Tendo em consideração que a *Cibercriminalidade* é um fenómeno global, a Organização Internacional mais bem colocada para adotar uma resposta mundial eficaz é a Organização das Nações Unidas. Criada pela Carta das Nações Unidas, assinada por cinquenta e um países a 26 de junho de 1945, a sua missão principal é a de “manter a paz e a segurança internacionais” e “desenvolver relações de amizade entre as nações baseadas no respeito do princípio da igualdade de direitos e da autodeterminação dos povos.”⁴³⁸ Mas, nos últimos sessenta anos, a ONU acumulou numerosas funções, muito para além de apenas garantir a paz e evitar conflitos, passando a intervir em áreas tão diversas como: a educação, a saúde, a cultura, mas também a justiça, o combate ao crime, de que é exemplo a UNODC ou os seus Congressos Mundiais de Prevenção do Crime e Justiça Criminal, que têm desempenhado um papel importante no esforço conjunto de combate à *Cibercriminalidade*.

Não obstante, até ao momento não foi possível adotar um Tratado das Nações Unidas de combate à *Cibercriminalidade*, à semelhança do que aconteceu em outros fenómenos de criminalidade transnacional, como a criminalidade organizada transnacional (Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional, adotada em 15 de novembro de 2000) ou o tráfico de drogas (Convenção das Nações Unidas contra o Tráfico Ilícito de Estupefacientes e Substâncias Psicotrópicas, adota em 20 de dezembro de 1988).

No entanto, o *Cibercrime* tem sido uma preocupação da ONU desde os anos 90. O 8.º Congresso das Nações Unidas sobre Prevenção do Crime e Justiça Criminal, realizado em Havana, de 27 de agosto a 7 de setembro de 1990, reconhecendo a dimensão internacional dos crimes relacionados com os computadores, apelou a uma resposta internacional dinâmica para a sua prevenção e controlo e exortou a uma ação concertada dos Estados Membros da ONU, de forma a modernizarem as suas leis penais e processuais penais e melhorarem medidas de segurança e prevenção.⁴³⁹ As conclusões deste Congresso foram corroboradas pela Assembleia Geral das Nações Unidas, na sua

⁴³⁸ Pinto, Maria do Céu, *O Papel da ONU na Criação de uma Nova Ordem Mundial*, prefácio, 2010, p.22.

⁴³⁹ Cfr. Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders, [Em linha], Nova Iorque, 1991, Disponível em https://www.unodc.org/documents/congress//Previous_Congresses/8th_Congress_1990/028_ACONF.144_28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf (consultado em 12.11.2014).

Resolução n.º45/121, de 14 de dezembro de 1990⁴⁴⁰. Destaque merece, ainda, a Resolução da Assembleia Geral das Nações Unidas n.º 64/221, de 21 de dezembro de 2009, sobre cibersegurança⁴⁴¹, mas sobretudo as suas Resoluções n.º 55/63, de 4 de dezembro de 2001⁴⁴², n.º 56/121, de 23 de janeiro de 2002⁴⁴³ sobre o combate ao uso criminoso das tecnologias de informação. Nestas Resoluções, a Assembleia Geral das Nações Unidas recomendou aos Estados Membros a adoção de uma série de medidas para combaterem o *Cibercrime*, como por exemplo: harmonização de legislação e práticas para evitar “portos seguros”; reforço da cooperação internacional; promoção da formação e reforço do equipamento das autoridades para combaterem este tipo de criminalidade; ou a proteção da confidencialidade, integridade e acesso aos dados e criminalização de acesso ilegal.

Um marco importante na ação das Nações Unidas no domínio do combate à *Cibercriminalidade* foi o seu 12.º Congresso de Prevenção do Crime e Justiça Criminal, que se realizou em Salvador (Brasil), nos dias 12 a 19 de abril de 2010, onde o combate ao *Cibercrime* ocupou um lugar de destaque nas sessões plenárias, onde se discutiu a possibilidade de celebração de uma convenção das Nações Unidas sobre o *Cibercrime*⁴⁴⁴, como forma de ultrapassar o alcance limitado dos instrumentos de Direito Internacional existentes, que têm um carácter regional. A proposta de celebração de um novo instrumento internacional para harmonizar as legislações nacionais e promover a cooperação internacional (como convenção autónoma ou um Protocolo Adicional à Convenção das Nações Unidas contra a Criminalidade Organizada Transnacional), mereceu, no entanto, a oposição de várias delegações nacionais, que consideraram a Convenção do Conselho da Europa contra o *Cibercrime* como o instrumento adequado, utilizado não só pelos seus Estados parte, mas também por outros Estados, como modelo adequado para as legislações nacionais. Outros consideraram a iniciativa prematura, havendo previamente questões fundamentais, como as relativas à jurisdição extraterritorial (e soberania nacional), à proteção de

⁴⁴⁰ Publicada in <http://www.un.org/documents/ga/res/45/a45r121.htm> (consultado em 17.2.2015).

⁴⁴¹ Disponível em http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211(consultado em 17.2.2015).

⁴⁴² Disponível em http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf (consultado em 17.2.2015).

⁴⁴³ Disponível em http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf (consultado em 17.2.2015).

⁴⁴⁴ Ver Relatório elaborado pelo Secretariado, [Em linha], p. 62. Disponível em http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf (consultado em 17.2.2015).

direitos humanos, privacidade e ao envolvimento do sector privado nas negociações. A Declaração de Salvador ficou, assim, aquém das expectativas e, em vez de um instrumento internacional de alcance mundial, limitou-se a recomendar ao UNODC que preste assistência técnica aos Estados Membros e promova a sua capacitação para melhorar a sua legislação nacional e reforçar a capacidade das suas autoridades para combater o *Cibercrime* e aumentar a segurança das suas redes informáticas.⁴⁴⁵ Na sua Resolução n.º 65/230, de 21 de dezembro de 2010⁴⁴⁶, a Assembleia das Nações Unidas corroborou a Declaração de Salvador e requereu ao UNODC que estabelecesse um grupo de peritos para elaborar um estudo abrangente sobre o problema do *Cibercrime* e as respostas dadas a ele pelos Estados Membros, pela comunidade internacional e pelo sector privado, com vista a analisar as opções para reforçar ou propor novas medidas de combate ao *Cibercrime*, de natureza legislativa ou outra, a nível nacional ou internacional. Em fevereiro de 2013, o UNODC publicou um estudo abrangente sobre o *Cibercrime*, fazendo um diagnóstico da situação e avançando conclusões importantes, como a necessidade de uma maior harmonização das legislações nacionais, a fragmentação dos instrumentos internacionais e a existência de divergências entre eles, diferentes abordagens quanto à criminalização de alguns atos ou a insuficiência dos quadros legais para a investigação do *Cibercrime*.⁴⁴⁷

Outra Organização Internacional que se tem ocupado das questões da *Cibercriminalidade* é a Organização para a Cooperação e Desenvolvimento (OECD), que foi a primeira organização que adotou recomendações neste âmbito, embora, atualmente, a sua atividade esteja centrada nas questões da *cibersegurança*.⁴⁴⁸

Mas ao nível internacional têm sido muitos os esforços levados a cabo por diversos Estados no combate à *Cibercriminalidade*, que exige mais do que a adoção de resoluções ou recomendações (*soft law*), antes reclama a adoção de instrumentos vinculativos de Direito Internacional referentes ao *Cibercrime*, quer convenções

⁴⁴⁵ Ponto 41 da Declaração de Salvador, [Em linha], adotada no 12.º Congresso das NU de Prevenção do Crime e Justiça Criminal. Disponível em http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf

⁴⁴⁶ Disponível em <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N10/526/34/PDF/N1052634.pdf?OpenElement>

⁴⁴⁷ UNODC, *Comprehensive Study on Cybercrime*, fevereiro de 2013, disponível in: http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

⁴⁴⁸ Informação da OCDE [Em linha]. Disponível em <http://www.cybercrimelaw.net/OECD.html> (última consulta em 17.02.2015).

bilaterais, quer convenções regionais. De entre instrumentos internacionais de combate ao *Cibercrime*, destacamos os seguintes:

- A Convenção sobre Cibercrime, do Conselho da Europa;
- A Convenção da Liga dos Estados Árabes (*the League of Arab States Convention on Combating Information Technology Offences*);
- O Acordo da Comunidade dos Estados Independentes (*the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information*);
- O Acordo da Organização para a Cooperação de Shangai (*the Shanghai Cooperation Organization Agreement in the Field of International Information Security*).

A *Convenção do Conselho da Europa sobre Cibercrime*, o primeiro tratado internacional de direito penal e processual penal nesta matéria, é objeto de tratamento autónomo no ponto seguinte, não só pela importância que tem na ordem jurídica internacional, mas também pela influência que exerceu na União Europeia (inspirando a sua legislação) e pelo facto de estar em vigor na ordem jurídica portuguesa.

A *Convenção da Liga dos Estados Árabes*, tal como dispõe o seu artigo 1.º, o objetivo desta Convenção é melhorar e reforçar a cooperação entre países árabes no combate aos crimes contra as tecnologias da informação, a fim de proteger a segurança e os interesses dos Estados Árabes, assim como a segurança da sociedade.⁴⁴⁹

O acordo da Comunidade dos Estados Independentes, de 1 de junho de 2011, foi celebrado entre os seguintes Estados: Azerbaijão (sujeito à legislação nacional); Arménia; Bielorrússia; Geórgia; Cazaquistão; Quirguistão (com reservas); Moldávia; Rússia; Tajiquistão; Turquemenistão; Uzbequistão e Ucrânia. O seu objetivo é combater as infrações relacionadas com os sistemas informáticos. Como dispõe o próprio preâmbulo “este acordo pretende estabelecer um quadro jurídico para a cooperação entre a aplicação da lei e dos órgãos judiciais dos Estados Membros do presente acordo, no combate às infrações relacionadas com os sistemas informáticos”⁴⁵⁰.

⁴⁴⁹ (Tradução livre), texto original [Em linha]. Disponível em <http://www.era-comm.eu/Cybercrime/library.html> (última consulta em 17.02.2015).

⁴⁵⁰ (Tradução livre). *Idem, Ibidem*.

Segundo Peter Ferdinand, a Organização para a Cooperação de Shangai⁴⁵¹ assume uma importância específica, já que “resulta de uma iniciativa diplomática chinesa” e é “a primeira organização do género a ser estabelecida pela China, na qual Pequim desempenha um papel primordial”.⁴⁵² Os membros desta organização asseguraram, desde logo, que não tinham intenção de desafiar os Estados Unidos da América, nem qualquer outro Estado, e que a sua cooperação visava unicamente contribuir para a segurança da região. Como entendem alguns autores, esta organização deve ser vista não como um polo “anti-ocidental”, mas sim como um polo “não-ocidental”.⁴⁵³ No entanto, como constata Peter Ferdinand “a colaboração diplomática dos membros da Organização é, em parte, uma reação contra a expansão da NATO para leste e as ameaças, a longo prazo, que isso pode provocar”.⁴⁵⁴

⁴⁵¹ O grupo de Xangai emergiu como resultado de uma nova ordem mundial, originada pelo colapso da União Soviética e pelo clima de incertezas que se seguiu. É um organismo internacional fundado em 14 de junho de 1996, por cinco Estados: a China, Rússia, Cazaquistão, Quirguistão, Tadjiquistão e Uzbequistão. Com exceção deste último, todos os outros Estados faziam já parte do conhecido “Shanghai 5”. Foi com a entrada do Uzbequistão em 2001, que esta organização passou a ter o nome pela qual é conhecida atualmente, Organização para a Cooperação de Xangai (OCX). A sua principal função é a cooperação para a segurança, em especial, quanto ao terrorismo, ao separatismo e ao extremismo, embora também aborde temas relacionados com a cooperação económica e social.

⁴⁵² Disponível em <http://mundorama.net/2013/12/04/a-organizacao-de-cooperacao-de-xangai-origens-e-missao-por-paulo-duarte/>, *apud.*, Ferdinand, Peter, *Sunset, sunrise: China and Russia construct a new relationship*, International Affairs, 2007.(consultado em 5.8.2015)

⁴⁵³ Disponível em <http://mundorama.net/2013/12/04/a-organizacao-de-cooperacao-de-xangai-origens-e-missao-por-paulo-duarte/>, *apud.*, Facon, I., *Les relations stratégiques Chine-Russie en 2005 : la réactivation d'une amitié pragmatique*, Fondation pour la Recherche Stratégique, 2006 (consultado em 5.8.2015)

⁴⁵⁴ Disponível em <http://mundorama.net/2013/12/04/a-organizacao-de-cooperacao-de-xangai-origens-e-missao-por-paulo-duarte/>, *apud.*, Ferdinand, Peter, *Sunset, sunrise: China and Russia construct a new relationship*, International Affairs, 2007.(consultado em 5.8.2015)

1.2.- Convenção do Conselho da Europa sobre o Cibercrime

O Conselho da Europa que tem já uma vasta experiência e tradição de cooperação internacional em assuntos penais e em direitos humanos trabalhou desde 1997 num projeto de Convenção sobre *Cibercriminalidade*.⁴⁵⁵ De igual forma, adotou várias e importantes Recomendações no que diz respeito à *Cibercriminalidade*: a Recomendação R(81) 12, a Recomendação R(85) 5, a Recomendação R(89) 9⁴⁵⁶ e a Recomendação R(95) 13⁴⁵⁷.

Não obstante todas as tentativas de combate à *Cibercriminalidade*, foi na reunião do G8 em Paris, em junho de 2000, que se deu início a uma ação conjunta, onde o Conselho da Europa manifestou a sua preocupação quanto a este tema, organizando uma *Convenção contra o Cibercrime*. Esta foi a tentativa mais completa e de maior alcance do controlo das comunicações em rede criada até àquele momento. Face a essa *Convenção*, foram muitos os países do mundo, como a Rússia, a China, a Malásia, Singapura, entre outros, que aplaudiram esta nova e determinada atitude, por parte de vários governos importantes para tentar controlar a *Internet*. Atitude que interpretaram como um sinal positivo, comparativamente à sua anterior desconfiança nos mesmos.⁴⁵⁸

A Convenção sobre o *Cibercrime*⁴⁵⁹ foi adotada pelo Comité de Ministros do Conselho da Europa, em 8 de novembro de 2001, e aberta à assinatura por ocasião da Conferência Internacional sobre Criminalidade, em Budapeste, no dia 23 de novembro de 2001. Esta convenção, que entrou em vigor no dia 1 de julho de 2004, foi assinada por 53 Estados e ratificada por 44⁴⁶⁰. De todos os Estados Membros do Conselho da Europa, apenas a Rússia e S. Marino não a assinaram. Todos os Estados Membros da União Europeia são signatários, embora a Grécia e a Irlanda ainda não a tenham ratificado. Portugal ratificou esta Convenção em 2009, tendo entrado em vigor na nossa ordem jurídica no

⁴⁵⁵ *Parecer 4/2001*, relativo ao “Projeto de Convenção do Conselho da Europa sobre Cibercriminalidade”, [Em linha], 22.3.2001, Bruxelas, p.2. Disponível em http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

⁴⁵⁶ *Recomendação R(89) 9*, sobre a “criminalidade informática que estabelece diretrizes para os legisladores nacionais, respeitantes à definição de certos crimes informáticos”.

⁴⁵⁷ *Recomendação R(95) 13*, relativa a “problemas da lei processual penal ligados às tecnologias da informação”.

⁴⁵⁸ Castells, Manuel, *A Galáxia Internet, Reflexões sobre Internet, Negócios e Sociedade*, p.212.

⁴⁵⁹ Esta convenção está publicada em Anexo à *Resolução da Assembleia da República n.º 88/2009*, que a aprovou, Diário da República, 1.ª Série, n.º 179, de 15 de setembro de 2009, pp. 6354 e ss. Também se encontra disponível em <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>

⁴⁶⁰ cfr. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG> [Em linha] (consultado em 17.02.2015).

dia 1 de julho de 2010⁴⁶¹. Embora originada no seio do Conselho da Europa, esta é uma convenção com um alcance mundial, já que nos termos do seu artigo 37.º foi aberta à adesão de Estados não membros do Conselho da Europa. Já foi ratificada pela Austrália, República Dominicana, Japão, Maurícia, Panamá e Estados Unidos da América, tendo ainda sido assinada pelo Canadá e África do Sul.

Esta Convenção é, assim, o primeiro instrumento de direito internacional de alcance global sobre *Cibercrime* com o objetivo de harmonizar os tipos legais de crime, cometidos através da *Internet* e redes de computadores e estabelecer um regime eficaz de cooperação internacional. Tendo em consideração a desadequação das normas de direito processual tradicionais para a perseguição dos crimes cometidos no *Ciberespaço*, a Convenção também procura dotar os Estados de normas processuais inovadoras que permitam investigar e perseguir criminalmente este tipo de crimes, reconhecendo valor legal e força probatória aos dados digitais. Por fim, a Convenção tem uma série de disposições para fomentar a cooperação judiciária internacional no combate ao *Cibercrime*.

As disposições de Direito Penal substantivo da Convenção sobre o *Cibercrime* foram completadas pelo “Protocolo Adicional relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos”, concluído em Estrasburgo, no dia 28 de janeiro de 2003, tendo entrado em vigor no dia 1 de março de 2006⁴⁶², tendo até ao momento sido ratificado por 23 Estados. Vários Estados Membros da União Europeia não o assinaram, nem ratificaram, tais como: Bulgária, Hungria, Irlanda, Eslováquia e Reino Unido e, em relação a Estados terceiros, apenas o Canadá e a África do Sul o assinaram, embora nenhum o tenha ratificado. Portugal ratificou este Protocolo em 2009, que entrou conjuntamente com a Convenção em vigor na nossa ordem jurídica, em 1 de julho de 2007.

⁴⁶¹ Resolução da Assembleia da República n.º 88/2009, DR 1.ª série, n.º 179, de 15 de setembro de 2009.

⁴⁶² Este Protocolo foi aprovado pela Resolução da Assembleia da República n.º 91/2009 e ratificado pelo Decreto do Presidente da República n.º 94/2009, Diário da República, 1.ª série, n.º 179, de 15 de setembro de 2009.

1.2.1. – Disposições de Direito Penal Material

A parte da Convenção relativa à lei penal material encontra-se prevista no Capítulo II, Secção 1.

O artigo 2.º relativo ao “acesso ilícito” prevê que cada Estado deverá adotar as medidas legislativas e outras que se revelem necessárias para clarificar como infração penal nos termos do seu direito interno, quando praticado intencionalmente, o acesso ilícito a um sistema informático seja no seu todo ou em parte dele.

O crime de “intercepção ilícita” encontra-se previsto no artigo 3.º da Convenção. Segundo este preceito cada Estado signatário deverá adotar todas as medidas necessárias para estabelecer como infração penal, no seu direito interno, quando praticada intencionalmente, a intercepção não autorizada através de meios técnicos, de transmissões não públicas de dados informáticos, para, de ou dentro de um sistema informático, incluindo as radiações eletromagnéticas emitidas por um sistema informático que transporte esses dados.

No artigo 4.º encontra-se previsto o “dano provocado nos dados”. Este artigo impõe que cada Estado adote todas as medidas necessárias para classificar como infrações penais no âmbito do seu direito interno, os atos praticados intencionalmente: a danificação, o apagamento, a deterioração, a alteração ou supressão não autorizados de dados informáticos (n.º1).

Os Estados podem ainda, nos termos do n.º2, reservar-se ao direito de exigir que o comportamento descrito no n.º1 do presente artigo tenha provocado danos graves.

A “sabotagem informática” está prevista no artigo 5.º. Como prevê este artigo, cada Estado deve adotar todas as medidas necessárias para classificar como infração penal nos termos do seu direito interno, quando praticada intencionalmente, a perturbação grave, não autorizada, do funcionamento de um sistema informático mediante inserção, transmissão, danificação, eliminação, deterioração, alteração ou supressão de dados informáticos.

O crime previsto no artigo 6.º “utilização indevida de dispositivos” (na versão original *misuse of devices*) é inovador, já que prevê no seu n.º 3 a possibilidade de formular parcial reserva à sua aplicação, o que foi consagrado por influência do Japão. Assim,

nos termos do n.º3, cada Estado pode reservar-se ao direito de não aplicar o n.º1 do presente artigo, desde que essa reserva não diga respeito à venda, distribuição ou qualquer outra forma de disponibilização dos elementos referidos no n.º1 alínea a), ii), do presente artigo.

Os artigos 7.º e 8.º são relativos às infrações relacionadas com computadores. Tal como nos outros casos, os Estados devem adotar todas as medidas necessárias para enquadrar no seu direito interno estas duas infrações penais. A “falsificação informática”, prevista no artigo 7.º, ocorre quando praticadas intencional e ilicitamente, a introdução, a alteração, o apagamento ou a supressão de dados informáticos dos quais resultem dados não autênticos, com o intuito de que esses dados sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não diretamente legíveis ou inteligíveis. Segundo o mesmo artigo, cada Estado pode, ainda, exigir que para que haja responsabilidade criminal tenha de haver intenção fraudulenta ou outra intenção criminal semelhante. Quanto à “burla informática”, prevista no artigo 8.º, ocorre quando praticado intencional e ilicitamente, o prejuízo patrimonial causado a outra pessoa por meio de:

- a) Qualquer introdução, alteração, apagamento ou supressão de dados informáticos;
- b) Qualquer interferência no funcionamento de um sistema informático, com intenção de obter para si ou para terceiros um benefício económico ilegítimo.

O artigo 9.º da Convenção diz respeito às infrações relativas à pornografia infantil. Por um lado, este instrumento de direito internacional consagra os 18 anos como a idade de referência quando se fala de um menor, embora qualquer um dos Estados possa impor um limite de idade inferior, não podendo, contudo, ser fixado abaixo dos 16 anos, tal como prevê o n.º 3 do artigo 9.º.

O n.º 1 do referido artigo sanciona as seguintes condutas:

- a) Produção de pornografia infantil com o propósito de a divulgar através de um sistema informático;
- b) Oferta ou disponibilização de pornografia infantil através de um sistema informático;
- c) Difusão ou transmissão de pornografia infantil através de um sistema informático;

- d) Obtenção para si ou para outra pessoa de pornografia infantil através de um sistema informático;
- e) Posse de pornografia infantil num sistema informático ou num dispositivo de armazenamento de dados informáticos.

Como podemos constatar, a Convenção prevê como crime a mera posse de material pornográfico infantil num sistema de computadores (alínea e) don.º1 artigo 9.º).

A tendência mais recente das instâncias internacionais vai precisamente no sentido da criminalização da mera posse de material pedófilo. A presente Convenção vai mais longe, atingindo não só as situações em que as imagens em causa representem efetivamente crianças como também as representações fictícias de crianças. Por exemplo: as imagens de crianças completamente criadas em computador ou as imagens de adultos a representar crianças. A criminalização da mera posse de material pedófilo visa, por um lado, satisfazer interesses práticos, de prova de factos em investigação. Ou seja, visa permitir punir quem tenha material pedófilo, suspeitando-se, sem prova suficiente, que o destina à difusão.⁴⁶³ Desta forma, permite às autoridades policiais e judiciais prosseguir e acionar criminalmente pessoas de quem se suspeita ser difusoras de material pornográfico pedófilo, pela via da mera posse. Por outro lado, a punição da mera posse pretende ser uma forma de dissuadir o eventual interesse pela difusão deste tipo de material. Importa salientar que, se no caso da punição da mera posse de imagens de crianças pode ainda ver-se uma forma, embora não direta, de proteção dos interesses dessas crianças, no caso da mera posse de imagens virtuais ou de falsas crianças essa razão não existe.⁴⁶⁴

Contudo, a previsão do n.º 4 do artigo 9.º permite a formulação de reserva à aplicação, entre outras, da punição de todas as situações de mera posse e da punição do *procuring* de material pornográfico.⁴⁶⁵

As “infracções respeitantes a violações do direito de autor e dos direitos conexos” encontram-se tipificadas no artigo 10.º da Convenção. Neste artigo a Convenção apenas obriga os Estados signatários a incriminar violações de direito de autor e conexos, quando cometidos por via de um sistema de computadores, de forma idêntica à já

⁴⁶³ Verdelho, Pedro; Bravo, Rogério (et. al.), *Leis do Cibercrime*, Vol. I, Centro Atlântico, p. 13.

⁴⁶⁴ *Idem, Ibidem.*

⁴⁶⁵ *Idem, Ibidem.*

prevista na lei nacional de cada Estado, em respeito por tratados internacionais, nomeadamente: a *Convenção de Berna para a Protecção das Obras Literárias e Artísticas*, revista pelo *Acto de Paris de 24 de Julho de 1971*, do *Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio e do Tratado da OMPI sobre o Direito de Autor*, com exceção de quaisquer direitos morais reconhecidos por essas Convenções, quando tais atos são praticados de forma intencional, para fins comerciais e por meio de um sistema informático (n.º1 do artigo 10.º). E ainda ao abrigo da *Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão* (Convenção de Roma), do *Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual relacionados com o Comércio* e do *Tratado da OMPI sobre Interpretações sobre Interpretações ou Execuções e Fonogramas*, com exceção de quaisquer direitos morais reconhecidos por essas Convenções, quando tais atos são praticados de forma intencional, para fins comerciais e por meio de um sistema informático (n.º2 do artigo 10.º)

Todavia, consagrou-se no n.º 3 do presente artigo, uma restrição à aplicabilidade destes tratados no ambiente digital. “De facto, optou-se por limitar a aplicabilidade de sanções criminais a situações em que a violação do direito de autor fosse grave, o que foi traduzido pela expressão *on a commercial scale*. Optou-se também por excluir a punição da violação de direitos morais e a punição de violações não intencionais de direito de autor”.⁴⁶⁶

O artigo 11.º da Convenção relativo à “tentativa, auxílio ou instigação”, prevê a obrigação de os Estados incriminarem atos de cumplicidade à prática de todos os crimes previstos (n.º1) e a obrigação de incriminarem a tentativa no que respeita a alguns dos crimes (n.º2), ficando de fora os crimes de acesso ilegal, *misuse of devices* e os crimes relacionados com o direito de autor e conexos.

Por fim, quanto à responsabilização criminal das pessoas coletivas, a mesma encontra-se prevista no artigo 12.º da Convenção. Esta responsabilidade ocorre se forem praticados atos cometidos em seu benefício por qualquer pessoa singular, agindo individualmente ou enquanto membro de um órgão da pessoa coletiva, que nelas ocupem uma posição de liderança, com base (n.º1):

⁴⁶⁶ Verdelho, Pedro; Bravo, Rogério (et. al.), *Leis do Cibercrime*, Vol. I, Centro Atlântico, p. 14.

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

Mas ocorre também se, por omissão de supervisão ou controlo da parte de um legal representante da pessoa coletiva, alguém sob a sua autoridade pratica um ato ilícito em seu benefício (n.º2).⁴⁶⁷

Em seguida iremos analisar as disposições de direito processual penal.

⁴⁶⁷ Verdelho, Pedro; Bravo, Rogério (et. al.), *Leis do Cibercrime*, Vol. I, Centro Atlântico, p. 15.

1.2.2. – Disposições de Direito Processual Penal

Uma das previsões mais importante presente na Convenção, será certamente o artigo 14.º, que consagra o “âmbito de aplicação das disposições processuais”. Neste artigo prevê-se a aplicação da Convenção aos crimes que ela define (alínea a) do n.º2) e ainda estão previstas duas extensões extremamente significativas:

- Por um lado, prevê-se que sejam aplicadas a qualquer outro tipo de crime cometido por via de um sistema informático (alínea b) do n.º2); e
- Por outro, prevê-se que sejam aplicáveis à obtenção de prova eletrónica de qualquer infração penal (alínea c) do n.º2).

Contudo, quanto a estas duas extensões, o projeto prevê que os Estados possam formular reservas, tal como prevê o n.º3 do artigo 14.º.

Nos artigos 16.º e 17.º da Convenção estão previstas a “conservação expedita de dados informáticos armazenados” e a “conservação expedita e divulgação parcial de dados de tráfego”, respetivamente. A previsão destas duas medidas processuais encontra-se separada, graças ao diferente enfoque de ambas. No entanto, ambas são medidas expeditas, impostas pela rapidez com que a informação circula no *Ciberespaço*. O seu carácter célere faz diminuir as garantias dos visados pela investigação em causa.⁴⁶⁸ Desta forma, se quanto aos meros dados de tráfego está também prevista a sua revelação expedita, o mesmo não acontece quanto aos outros dados. Por exemplo: o conteúdo da comunicação ou dados já armazenados. Ambas as medidas são inovadoras e essenciais para o sucesso de combate a eventuais investigações criminais no âmbito digital, já que os dados digitais, pelas suas propriedades, podem ser alterados ou apagados em segundos.⁴⁶⁹

O mesmo já não se verifica quanto aos dados de tráfego, já que estes permitem reconstruir o percurso de determinada comunicação. Nessa comunicação pode ter sido utilizado mais do que um servidor *Internet* e, como tal, é importante que o servidor preserve e revele, de forma rápida, qual ou quais os operadores utilizados no percurso

⁴⁶⁸ Verdelho, Pedro; Bravo, Rogério (et. al.), *Leis do Cibercrime*, Vol. I, Centro Atlântico, p.16.

⁴⁶⁹ *Idem, Ibidem*.

da comunicação em causa, permitindo assim, que de forma rápida a preservação e revelação de informação cheguem a outros operadores em tempo útil.⁴⁷⁰

É igualmente inovador o preceito do artigo 18.º da Convenção, segundo o qual cada Estado signatário deverá adotar as medidas legislativas e outras que se revelem necessárias à criação de um mecanismo de injunção destinada a cidadãos e a servidores de *Internet*, pela qual as competentes autoridades ordenam que aquelas pessoas singulares e coletivas forneçam dados armazenados num computador sob a sua responsabilidade ou forneçam dados de subscritores do serviço *Internet* (alíneas a) e b) do n.º1).⁴⁷¹

Importa salientar que o texto da Convenção prevê que a injunção de submeter dados seja referente a dados específicos. Esta limitação tem como função impedir situações de abuso policial, já que, ao permitir-se, sem reservas, dar ordens de submissão de dados informáticos (que, por certo, não podem aperceber-se antes de serem processados), estaria a permitir-se o acesso indiscriminado a toda e qualquer informação.⁴⁷²

A matéria sobre “busca e apreensão de dados informáticos armazenados” encontra-se prevista no artigo 19.º da Convenção. Segundo o n.º1 deste artigo, cada Parte deverá adotar as medidas legislativas e outras que se revelem necessárias para habilitar as suas autoridades competentes e efetuar buscas ou, de outro modo, aceder:

- a) A um sistema informático, ou a parte do mesmo, bem como aos dados informáticos nele armazenado;
- b) A um suporte informático de dados que permita armazenar dados informáticos, no seu território.

No n.º2 do artigo 19.º da Convenção, prevê-se que quando no decurso de busca ou de outro modo acessem a um sistema informático ou a parte dele, e se note que os dados que se procuram estarão guardados noutro sistema de computadores, as entidades competentes, de forma expedita, devem estender a busca, ou o acesso similar a que se proceda, ao outro sistema.⁴⁷³

⁴⁷⁰ Verdelho, Pedro; Bravo, Rogério (et. al.), *Leis do Cibercrime*, Vol. I, Centro Atlântico, p.16.

⁴⁷¹ *Idem*, *Op. Cit.*, pp. 16 e 17.

⁴⁷² *Idem*, *Op. Cit.*, p. 17.

⁴⁷³ *Idem*, *Ibidem*.

Quanto às apreensões, prevê o n.º3 do referido artigo, que os Estados devem legislar no sentido de:

- a) Apreender ou de outro modo reter um sistema informático ou parte do mesmo, ou um suporte informático de dados;
- b) Efetuar e reter uma cópia desses dados informáticos;
- c) Preservar a integridade dos dados informáticos pertinentes armazenados;
- d) Tornar esses dados informáticos inacessíveis ou retirá-los do sistema informático acedido.

Por fim, quanto à jurisdição, prevista no artigo 22.º da Convenção, prevê-se a obrigação de os Estados signatários se declararem competentes para prosseguirem criminalmente, independentemente do local da prática dos fatos, os seus cidadãos nacionais se a infração for punível no local onde foi cometida ou se não for da competência de nenhum Estado, como por exemplo, na Antártida.

1.2.3. – Cooperação Internacional

As regras referentes à cooperação internacional encontram-se previstas no Capítulo III da Convenção.

O artigo 23.º prevê os “princípios gerais relativos à cooperação internacional”, salientando o âmbito material de aplicação da convenção e a remissão para outros instrumentos internacionais.⁴⁷⁴

No artigo 24.º está prevista a extradição. No n.º 1, alínea a) do presente artigo, é fixado o limite mínimo de um ano de prisão, para que seja admissível a extradição, sendo paralelamente exigida a dupla incriminação. Contudo, o texto prevê ainda a possibilidade de haver extradição para crimes de pena inferior, em caso de existir um tratado bilateral entre os dois Estados envolvidos e nesse tratado se prever um limite inferior (n.º1, alínea b)⁴⁷⁵. Ainda a este propósito, a Convenção prevê a possibilidade de recusa de extradição nos casos em que o crime em causa seja considerado um crime político ou relacionado com um crime político e ainda quando estejam em causa interesses fundamentais do Estado requerido, tais como a soberania, a segurança, a ordem pública, entre outros.⁴⁷⁶ No n.º2 do referido artigo, está expressamente consagrado que a extradição será submetida às condições previstas na lei do país requerido e nos tratados internacionais eventualmente aplicáveis.

O artigo 27.º da Convenção contém um texto pormenorizado sobre as disposições gerais referentes à assistência mútua. Contudo, estas disposições dizem apenas respeito a situações em que os Estados não estejam vinculados por acordos internacionais. Sendo, desta forma, aplicáveis a uma pequena parte dos potenciais signatários.⁴⁷⁷

Ainda quanto aos princípios gerais em matéria de assistência mútua, o artigo 26.º prevê a possibilidade de um Estado, no decurso de investigações internas, concluir que deverá reencaminhar certas informações a um outro Estado, presente nesta Convenção.⁴⁷⁸ O n.º2 deste artigo prevê que esse envio de informação deve respeitar o cumprimento de certas condições, nomeadamente de confidencialidade.

⁴⁷⁴ Verdelho, Pedro; Bravo, Rogério (et. al.), *Leis do Cibercrime*, Vol. I, Centro Atlântico, p.18.

⁴⁷⁵ Inclui-se nestes casos, a Convenção Europeia de Extradição (STE n.º24), ou um acordo baseado em legislações uniformes ou recíprocas. *Idem, Ibidem*.

⁴⁷⁶ *Idem, Op. Cit.*, pp.18 e 19.

⁴⁷⁷ *Idem, Op. Cit.*, p. 19.

⁴⁷⁸ *Idem, Ibidem*.

No artigo 29.º da Convenção estão previstas as regras respeitantes à preservação expedita de dados armazenados num computador. Prevê-se que um Estado solicite a outro a preservação expedita de dados, desde que manifeste a intenção de vir a fazer-lhe um pedido formal de assistência para realização de uma busca, apreensão ou diligência similar. Nesse caso, o Estado requerido deverá adotar todas as medidas necessárias à preservação daqueles dados, com respeito pela sua própria lei nacional. Importa salientar o n.º 3 deste artigo, que prevê que não será necessário observar o requisito de dupla incriminação, como condição da preservação de dados. Esta dispensa do requisito de dupla incriminação apenas se refere a crimes não previstos na Convenção, ou seja, aos crimes cometidos por meio de um computador ou a crimes cuja prova esteja registada num computador. Quanto aos crimes previstos na Convenção, prevê-se em princípio, dupla incriminação.⁴⁷⁹ Trata-se de uma medida de cooperação internacional nova que resulta da especificidade do ambiente digital. Importa referir que a medida em causa é apenas sobre a preservação de dados, sem implicar a sua revelação. Quanto à revelação, tem outras regras, mais restritas, sobretudo se não respeitar dados de tráfego. Como tal, segundo este preceito, poderá haver casos de preservação de dados sem que depois haja condições para a sua divulgação ao Estado requerente.⁴⁸⁰

O artigo 30.º da presente Convenção prevê a “divulgação expedita dos dados de tráfego conservados”. São dados em relação aos quais, no âmbito da Convenção, facilitam a cooperação internacional. É importante salientar o n.º 2 deste artigo já que prevê as duas únicas situações em que, nos termos do disposto no n.º1, pode ser recusada a divulgação de dados de tráfego:

- a) Se o pedido respeitar a uma infração considerada pela Parte requerida como infração de natureza política ou com ela conexa;
- b) Se a Parte requerida considerar que o cumprimento do pedido pode atentar contra a sua soberania, segurança, ordem pública ou qualquer outro interesse essencial.

O artigo 31.º prevê o “auxílio mútuo relativamente ao acesso a dados informáticos armazenados”. Este artigo define regras gerais sobre pedidos de assistência internacional para a obtenção de dados armazenados num computador.

⁴⁷⁹ Verdelho, Pedro; Bravo, Rogério (et. al.), *Leis do Cibercrime*, Vol. I, Centro Atlântico, p.19.

⁴⁸⁰ *Idem*, *Op. Cit.*, p. 20

Quanto ao artigo 32.º, prevê o “acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público”. Este artigo prevê que “uma Parte pode, sem autorização da outra Parte”:

- a) “Aceder a dados informáticos acessíveis ao público (fonte aberta), independentemente da sua localização geográfica;
- b) Através de um sistema informático situado no seu território, aceder a dados informáticos no território de uma outra Parte, ou recebê-los, se obtiver o consentimento legal e voluntário da pessoa com legitimidade para lhe divulgar os dados através deste sistema informático”.

De uma forma geral, trata-se de, no decurso de uma investigação, obter de um computador localizado no estrangeiro, dados de livre acesso ou cujo acesso tenha sido autorizado por uma pessoa com legitimidade para autorizar tal acesso. Concretamente, trata-se da recolha de prova em locais de acesso público ou de acesso autorizado pelo legítimo titular.⁴⁸¹

Por fim, importa salientar o artigo 35.º da Convenção, que diz respeito à “Rede 24/7”. Resulta do texto deste artigo a obrigação específica de, no âmbito da cooperação internacional, ser criado um ponto de contacto permanente disponível 24 horas por dia, 7 dias por semana, a fim de assegurar a prestação de assistência imediata a investigações ou procedimentos respeitantes a infrações penais relacionadas com dados e sistemas informáticos, ou com o objetivo de recolher provas, sob a forma eletrónica, de uma infração penal (n.º1 do artigo 35.º). Este auxílio incluirá a facilitação ou, se o direito e práticas internas o permitirem, a aplicação direta das seguintes medidas:

- a) “A prestação de aconselhamento técnico;
- b) A conservação de dados em conformidade com os artigos 29.º e 30.º;
- c) A recolha de provas, informações de carácter jurídico e localização de suspeitos.”

Os pontos de contactos das Partes devem ter capacidade técnica para corresponder aos pedidos de forma rápida (n.º2 alínea a). Por outro lado, se o ponto de contacto designado por uma Parte não depender da autoridade ou autoridades dessa Parte responsáveis pela cooperação internacional ou extradição dessa Parte, o ponto de

⁴⁸¹ Verdelho, Pedro; Bravo, Rogério (et. al.), *Leis do Cibercrime*, Vol. I, Centro Atlântico, p.20.

contacto deve assegurar que pode agir em coordenação com essa ou essas autoridades de forma rápida (n.º2 alínea b).

2. O Direito da União Europeia

2.1. - A Estratégia da União Europeia de combate à Cibercriminalidade

O espaço de liberdade, segurança e justiça é, atualmente, um dos maiores desafios que a União Europeia já enfrentou⁴⁸². E falamos neste tema porque aliada à livre circulação de pessoas tem-se verificado um aumento do número de crimes transnacionais, como é o caso do aumento da *Cibercriminalidade*.

Neste tipo de crimes destacamos três principais características:

- *Imprevisibilidade*, são crimes imprevisíveis, que podem ser cometidos a qualquer momento;
- *Generalidade*, isto é, são ataques que podem ser dirigidos a vários utilizadores, desde particulares a empresas, entidades ou órgãos do Estado;
- *Transnacionalidade*, crimes que podem ser praticados por agentes situados em qualquer parte do mundo, em segundos. E é precisamente este último ponto que mais tem preocupado a União Europeia. As ações repressivas contra estes crimes são extremamente difíceis, já que os seus autores se encontram, na grande maioria, em países diferentes do país alvo do ataque e muitas das vezes fora da União Europeia⁴⁸³.

A verdade é que a *Internet* é um meio de comunicação e transmissão que se tem expandindo (e que continua a expandir) a um ritmo estonteante, com funções que podem ser usadas não só para fins proveitosos e pacíficos, mas também para fins criminosos, que são a grande percentagem. Estes fins criminosos podem pôr em risco os interesses fundamentais de um país. Por exemplo, através da preparação de atentados aos seus governantes e instituições, passando pelas infrações à moral pública ou à boa

⁴⁸² Como dispõe o artigo 3.º do Tratado que institui a União Europeia (Tratado de Lisboa), é objetivo da União Europeia proporcionar “aos seus cidadãos um espaço de liberdade, segurança e justiça sem fronteiras internas, em que seja assegurada a livre circulação de pessoas, em conjugação com medidas adequadas em matéria de controlos na fronteira externa, de asilo e imigração, bem como de prevenção da criminalidade e combate a este fenómeno”. Sousa, Constança Urbano de (Coordenadora), *O Espaço de Liberdade, Segurança e Justiça da União Europeia: desenvolvimentos recentes*, Departamento de Direito, Universidade Autónoma de Lisboa, p. 5.

⁴⁸³ (COM (2007) 267 final), *Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões*, “Rumo a uma Política geral de luta contra o Cibercrime”, Bruxelas, 22.5.2007, p.3.

reputação das pessoas ou como meio para a prática de criminalidade internacional organizada, até às fraudes informáticas e violação da propriedade intelectual.⁴⁸⁴

Do mesmo modo, a evolução das técnicas de *Cibercriminalidade* tem sido rápida, surgindo cada vez mais novos tipos e formas de crimes⁴⁸⁵, que dificultam a atuação dos sistemas de segurança. É graças ao aparecimento deste tipo de crimes, que é cada vez mais importante dotar a União Europeia de uma política de defesa contra estes ataques. Por exemplo, através da harmonização do direito penal relativo a diversos crimes de natureza transnacional, como é o caso da *Cibercriminalidade*⁴⁸⁶.

A Europa dispõe de excelentes capacidades de investigação e é pioneira em alguns dos mais avançados desenvolvimentos tecnológicos e de segurança. No entanto, muitos dos líderes mundiais, com competência em matéria de produtos e serviços *TIC* inovadores estão sediados fora da União Europeia. Tal facto aumenta o risco de a Europa se tornar excessivamente dependente, não só de *Tecnologias de Informação e das Comunicações* produzidas noutros países, mas também de soluções de segurança desenvolvidas fora das suas fronteiras.⁴⁸⁷

Para solucionar este problema, é fundamental garantir que os componentes de *hardware* e *software* produzidos na União Europeia e em países terceiros, que são utilizados em serviços e infraestruturas críticos e cada vez mais em dispositivos móveis, sejam de confiança, seguros, e garantam a proteção dos dados pessoais.⁴⁸⁸ Apenas é possível assegurar um elevado nível de segurança se todos os elementos da cadeia de valor, tais como fabricantes de equipamentos, criadores de *software*, fornecedores de serviços da

⁴⁸⁴ Com receio destes ataques, em França, onde se começa a investigar com eficácia a prática de crimes através da *Internet*, já com alguma frequência os tribunais têm ordenado medidas no sentido da eliminação pura de certos sítios eletrónicos, uma vez demonstrada a prática criminal, sem preocupação sobre o modo como tecnicamente as medidas vão ser executadas, mas preocupados com o seu resultado final. Isto acontece não apenas com a proteção da propriedade intelectual mas também com o combate à pedofilia e ao tráfico sexual. Ao que se anuncia, esta prática também começa a ser utilizada nos Estados Unidos da América. Marques, Garcia; Martins, Lourenço, *Lições de Direito da Comunicação, Direito da Informática*, Almedina, Novembro 2000, p.505.

⁴⁸⁵ Temos como exemplo o número cada vez maior de sítios com conteúdos ilícitos acessíveis na Europa, incluindo os casos de pornografia infantil; incitamentos a atos terroristas, os cada vez mais recentes, casos de ataques de larga escala contra sistemas de informação ou organizações e particulares; glorificação ilícita da violência, do terrorismo, do racismo e da xenofobia.

⁴⁸⁶ Ramos, Armando R. Dias, *A novíssima Diretiva relativa ao cibercrime*, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014, p.6.

⁴⁸⁷ (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p.13.

⁴⁸⁸ *Idem, Ibidem*.

sociedade da informação, adotarem a segurança tecnológica como uma prioridade e trabalharem em conjunto.⁴⁸⁹

As leis e normas que se aplicam noutros domínios das nossas vidas quotidianas devem aplicar-se igualmente no domínio do *Ciberespaço*, sem exceção. Desta forma, a União Europeia deve preservar um ambiente digital que garanta o maior grau de liberdade e de segurança possível, em benefício de todos⁴⁹⁰.

Embora reconheça que cabe em grande parte aos Estados Membros responder aos desafios da segurança no *Ciberespaço*, a União Europeia tem adotado estratégias e ações específicas que podem melhorar o desempenho geral da União Europeia. Estas ações incluem uma variedade de ferramentas políticas⁴⁹¹ e envolvem diferentes tipos de atores, desde as instituições da União Europeia aos Estados Membros ou à indústria.⁴⁹²

Igualmente a nível da União Europeia e como reforço da cooperação europeia, foi criado o *Fórum Europeu dos Estados Membros (EFMS)*⁴⁹³, que tem mantido discussões

⁴⁸⁹ Tudo indica (tal como revela a avaliação de impacto constante do documento de trabalho dos serviços da Comissão, que acompanha a proposta de diretiva relativa à segurança das redes e da informação, Ponto 4.1.5.2), que muitos dos intervenientes ainda veem na segurança pouco mais do que um encargo adicional, o que faz com que seja escassa a procura de soluções nesse domínio. É, tal como revela a (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, “É necessário que sejam implementados ao longo de toda a cadeia de valor dos produtos TIC utilizados na Europa requisitos de desempenho em matéria de cibersegurança. O setor privado precisa de incentivos para garantir um elevado nível de cibersegurança; por exemplo, rótulos que indiquem um desempenho adequado a nível de cibersegurança permitirão às empresas com um bom desempenho e um bom historial a esse nível transformá-lo num trunfo e obter vantagem competitiva”. *Idem, Op. Cit.*, pp. 13 e 14.

⁴⁹⁰ Como referiu Neelie Kroes (Vice Presidente da Comissão responsável pela Agenda Digital), “para que todos os europeus se convertam ao digital é necessário que se sintam confiantes e seguros em linha. As ameaças informáticas não conhecem fronteiras. Uma Agência Europeia para a Segurança das Redes e da Informação modernizada trará mais conhecimentos especializados e reforçará os intercâmbios de boas práticas na Europa. As instituições e os Governos da União Europeia devem trabalhar mais do que nunca em conjunto, para nos ajudar a compreender a natureza e a escala das novas ameaças informáticas. Precisamos dos conselhos e do apoio da ENISA para conceber mecanismos de resposta eficazes para proteger os nossos cidadãos e empresas em linha”, [Em linha], Comissão Europeia, Bruxelas, 30.9.2010. Disponível em http://europa.eu/rapid/press-release_IP-10-1239_pt.htm (consultado em 15.10.2014).

⁴⁹¹ Como é o caso das ações relacionadas com a partilha de informações, quando estejam em causa dados pessoais, devem ser conformes com a legislação da União Europeia relativa à proteção de dados. (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p. 5.

⁴⁹² *Idem, Ibidem*.

⁴⁹³ O Fórum Europeu dos Estados Membros, lançado por via da Comunicação (COM (2009) 149), é uma plataforma utilizada para promover o debate entre as autoridades públicas dos Estados Membros sobre as boas práticas políticas em matéria de segurança e resiliência das infraestruturas críticas da informação. (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p. 6

e pontos de vista produtivos sobre a política pública para a *Segurança das Redes e da Informação*, podendo ainda ser integrado no mecanismo de cooperação, uma vez instaurado.⁴⁹⁴

Neste contexto de mudança, é urgente tomar medidas, quer a nível nacional quer a nível europeu, contra todas as formas de *Cibercrime*, que ameaçam cada vez mais as infra-estruturas da nossa sociedade, das empresas e dos cidadãos. Para tal e como forma de travar o aumento da *Cibercriminalidade*, a Comissão propõe um conjunto de medidas que visam:

- Assegurar a transposição e a implementação mais rápidas das diretivas relativas à *Cibercriminalidade*;
- Instar junto dos Estados Membros que ainda não ratificaram a *Convenção sobre Cibercrime*, para que o façam quanto antes, aplicando também as suas disposições o mais rapidamente possível;
- Apoiar os Estados Membros, através dos seus programas de financiamento⁴⁹⁵, na identificação das lacunas e no reforço da sua capacidade para investigar e combater a *Cibercriminalidade*⁴⁹⁶;
- Coordenar, em colaboração com os Estados Membros, os esforços para identificar as melhores práticas e técnicas disponíveis para combater a *Cibercriminalidade*, por exemplo, no que diz respeito ao desenvolvimento e à utilização de ferramentas forenses ou à análise das ameaças;
- Trabalhar em estreita cooperação com o novo EC3, no quadro da Europol e com a Eurojust para harmonizar tais abordagens políticas com as melhores práticas na esfera operacional.⁴⁹⁷

⁴⁹⁴ (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p. 6.

⁴⁹⁵ Em 2013, no âmbito do programa “Prevenir e combater a criminalidade” (ISEC). Após 2013, no âmbito do Fundo para a Segurança Interna (novo instrumento do QFP). *Idem, Op. Cit.*, p. 10.

⁴⁹⁶ Além disso, a Comissão irá apoiar os organismos que fazem a ligação entre a investigação, as universidades, os agentes policiais/judiciais e o setor privado, cujo trabalho tem afinidades com o que é atualmente realizado pelos centros de excelência para a *cibercriminalidade* já criados em alguns Estados Membros e que são financiados pela Comissão. *Idem, Ibidem*.

⁴⁹⁷ (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, pp. 10 e 11.

Desenvolver a política e as capacidades de *ciberdefesa* no quadro da *Política Comum de Segurança e Defesa* (PCSD) é outra das estratégias de combate à *Cibercriminalidade* adotadas pela União Europeia.

Para aumentar a resiliência dos sistemas de comunicação e informação que apoiam a política de defesa dos Estados Membros e os interesses da segurança nacional, o desenvolvimento de capacidades de *ciberdefesa* deve dar especial atenção à detenção de ameaças informáticas sofisticadas, na resposta a dar a estes casos e na posterior recuperação em caso de ataques.

Perante o aumento do número de ameaças multifacetadas, é fundamental melhorar as sinergias entre as abordagens civis e militares na proteção dos ativos informáticos críticos. Estes esforços devem ser apoiados pela investigação e desenvolvimento e por uma cooperação mais estreita entre os governos, o setor privado e as universidades da União Europeia.⁴⁹⁸

Outra das estratégias europeias a adotar passa por definir uma política internacional coerente em matéria de *Ciberespaço* e promover os valores fundamentais da União Europeia. A preservação de um *Ciberespaço* aberto, livre e seguro, é um desafio de dimensão mundial a que a União Europeia deve responder conjuntamente com os parceiros e organizações internacionais relevantes, com o setor privado e com a sociedade civil. Embora seja difícil definir barreiras no *Ciberespaço*, a verdade é que é impossível assegurar que este se mantenha um espaço seguro, sem um mínimo de controlo. Para tal, na sua política internacional relativa ao *Ciberespaço*, a União Europeia deverá promover a abertura e a liberdade da *Internet*, encorajar os esforços tendentes a estabelecer normas de comportamento e aplicar as leis internacionais em vigor no *Ciberespaço*.⁴⁹⁹

Ainda neste âmbito a Comissão, a Alta Representante e os Estados Membros devem, em conjunto, definir para a União Europeia uma política internacional coerente em matéria de *Ciberespaço* que vise um maior empenho e reforço das relações com os principais

⁴⁹⁸ (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p.12.

⁴⁹⁹ A cooperação internacional da União Europeia nas questões que dizem respeito ao *ciberespaço* pautar-se-á pelos valores fundamentais da União Europeia, ou seja, a dignidade humana, a liberdade, a democracia, a igualdade, o Estado de direito e o respeito pelos direitos fundamentais. *Idem, Op. Cit.*, p.16.

parceiros e organizações internacionais, bem como com a sociedade e o setor privado⁵⁰⁰. Esta cooperação deverá ser efetuada com o intuito de acrescentar valor aos atuais diálogos bilaterais entre os Estados Membros da União Europeia e os países terceiros⁵⁰¹.

Para responder aos desafios que o espaço digital enfrenta à escala global, a União Europeia deverá estabelecer uma cooperação mais próxima com as organizações ativas neste domínio, como é o caso do Conselho da Europa, a OCDE, a ONU, a OSCE, a NATO, a UA, a ASEAN e OEA. No campo bilateral, isto é, na cooperação com os Estados Unidos, será de extrema importância o desenvolvimento da colaboração do Grupo de Trabalho UE-EUA para a *Cibersegurança* e a *Cibercriminalidade*.⁵⁰²

Como já referimos, para que o *Ciberespaço* permaneça aberto e livre, devem aplicar-se no mundo digital as mesmas normas, princípios e valores que a União Europeia defende para o mundo físico⁵⁰³. Deste modo, os direitos fundamentais, a democracia e o Estado de direito devem ser protegidos no mundo digital. A nossa liberdade e prosperidade dependem cada vez mais de uma *Internet* segura, robusta e inovadora.⁵⁰⁴ Mas a liberdade no mundo digital exige também segurança e proteção, e dessa forma o *Ciberespaço* deve ser protegido contra incidentes, atividades maliciosas e utilizações abusivas. E nesta matéria, os governos desempenham um papel fundamental, já que devem garantir a existência de um *Ciberespaço* livre e seguro.

São várias as funções que competem aos governos de cada Estado, das quais destacamos as seguintes: salvaguardar o acesso e a abertura, respeitar e proteger os direitos fundamentais no espaço digital e manter a fiabilidade e a interoperabilidade da *Internet*.⁵⁰⁵

⁵⁰⁰ A União Europeia pretende promover a responsabilidade social das empresas (responsabilidade social das empresas: uma nova estratégia da União Europeia para o período de 2011-2014; (COM (2011) 681 final) e lançar iniciativas internacionais para melhorar a coordenação a nível mundial neste domínio. (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p. 17.

⁵⁰¹ No âmbito destes diálogos bilaterais a União Europeia atribuirá uma especial importância ao diálogo com os países terceiros (em especial aos países com as mesmas ideias e que partilhem os valores defendidos pela União Europeia). Procurará, de igual forma, assegurar um nível elevado de proteção dos dados, nomeadamente, em caso de transferência de dados pessoais para um país terceiro). *Idem, Ibidem*.

⁵⁰² *Idem, Ibidem*.

⁵⁰³ Também as obrigações legais consagradas no Pacto Internacional sobre os Direitos Cíveis e Políticos, na Convenção Europeia dos Direitos do Homem e na Carta dos Direitos Fundamentais da União Europeia devem ser igualmente respeitados no mundo digital. *Idem, Ibidem*.

⁵⁰⁴ *Idem, Op. Cit.*, p. 2.

⁵⁰⁵ *Idem, Ibidem*.

A União Europeia pode complementar o trabalho dos Estados Membros, facilitando a adoção de uma abordagem coordenada e colaborativa, que reúna as autoridades policiais e judiciais e as partes interessadas dos setores público e privado da União Europeia e internacionais. Nas questões de segurança internacional, a União Europeia incentiva a elaboração de medidas que promovam a confiança na *cibersegurança*, de modo a aumentar a transparência e reduzir o risco de mal entendidos quanto ao comportamento dos Estados.⁵⁰⁶

Concluindo: para promover a resiliência do *Ciberespaço* na União Europeia, tanto as autoridades públicas como o sector privado devem desenvolver capacidades e cooperar de forma eficaz. Tal como comprovam os resultados positivos alcançados através das várias atividades realizadas⁵⁰⁷, a prossecução da ação da União Europeia pode ajudar a combater os riscos e ameaças de dimensão transfronteiriça de que é alvo o *Ciberespaço* e contribuir para uma resposta coordenada em situações de emergência.⁵⁰⁸ Estas medidas darão, assim, um forte contributo para o bom funcionamento do mercado interno e servirão para promover a segurança interna da União Europeia.

⁵⁰⁶ No entanto, a União Europeia não apela à criação de novos instrumentos jurídicos internacionais quanto às questões do *ciberespaço*. (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p.17.

⁵⁰⁷ Destacamos as referências feitas na (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, bem como a avaliação de impacto que integra o documento de trabalho dos serviços da Comissão (anexo à proposta de diretiva relativa à segurança das redes e da informação, em particular as secções 4.1.4 e 5.2., os anexos 2, 6 e 8). *Idem, Op. Cit.*, p.5.

⁵⁰⁸ *Idem, Ibidem.*

2.2. A Diretiva 2013/40/UE sobre Cibercrime

2.2.1. – Antecedentes

Como temos vindo a observar, o combate à *Cibercriminalidade*, depende de uma uniformização da legislação internacional, especialmente, a nível europeu. Neste sentido, foram adotados vários diplomas sobre os quais vamos explanar em seguida.

Anteriormente à adoção daquele que é considerado o principal instrumento internacional sobre crime no *Ciberespaço*, a Convenção sobre o Cibercrime do Conselho da Europa, adotada em Budapeste a 23 de novembro de 2001 (o qual analisámos supra), foram adotadas as Recomendações do Conselho de Ministros do Conselho da Europa que estabeleciam as diretrizes aos legisladores nacionais, no que diz respeito à definição de certos crimes informáticos e respetivas punições. Nomeadamente, as Recomendações R (89) 9 e R (95) 13.

Inspirando-se na Recomendação R (89) 9, Portugal foi pioneiro no seio da comunidade europeia, em legislar sobre a criminalidade informática, através da Lei n.º 109/91, de 17 de agosto, revogada pela Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime).⁵⁰⁹

A 16 de março de 2005 foi publicado no Jornal Oficial⁵¹⁰ a Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro de 2005, relativa a ataques contra os sistemas de informação.⁵¹¹ Como dispõe o próprio preâmbulo, o objetivo desta Decisão-Quadro era reforçar a cooperação entre as autoridades judiciais e outras autoridades competentes, nomeadamente as autoridades policiais e outros serviços especializados responsáveis pela aplicação da lei nos Estados Membros, mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação.

⁵⁰⁹ Ramos, Armando R. Dias, *A novíssima Diretiva relativa ao cibercrime*, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014, p.179.

⁵¹⁰ Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho. (JOUE L 218/12, de 14.8.2013).

⁵¹¹ Ramos, Armando R. Dias, *A novíssima Diretiva relativa ao cibercrime*, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014, p.179.

Perante a multiplicidade de diplomas, eram evidentes as consideráveis lacunas e as diferenças entre as legislações dos Estados Membros neste e em outros domínios, o que dificultava a atuação e cooperação policial e judiciária.

A natureza transnacional e sem fronteiras dos modernos sistemas de informação facilitam a propagação de ataques de dimensão transfronteiriça, o que evidencia a necessidade urgente de adotar medidas suplementares para aproximar o direito penal neste domínio.⁵¹² A coordenação da ação penal contra casos de ataques a sistemas de informação deverá ser facilitada pela transposição e aplicação adequadas da Decisão-Quadro 2009/948/JAI do Conselho, de 30 de novembro de 2009, relativa à prevenção e resolução de conflitos de exercício de competência em processo penal.⁵¹³

Neste sentido, importa ainda salientar as seguintes medidas adotadas:

- A Decisão-Quadro 2004/413/JAI, relativa à exploração sexual de crianças;
- A Decisão-Quadro 2001/413/JAI⁵¹⁴, do Conselho de 28 de maio de 2001, “relativa ao combate à fraude e à contrafacção de meios de pagamento que não em numerário”;
- A Diretiva 2002/58/CE⁵¹⁵, do Parlamento Europeu e do Conselho de 12 de julho de 2002, “relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações eletrónicas”; e
- A Comunicação da Comissão Europeia, de 22 de maio de 2007, “Rumo a uma política geral de luta contra o cibercrime”.⁵¹⁶

No ponto seguinte iremos analisar as disposições da Diretiva sobre o Cibercrime.

⁵¹² Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, (JOUE L 218/8, de 14.8.2013), p. 11.

⁵¹³ Decisão-Quadro 2009/848/JAI do Conselho, de 30 de novembro de 2009, relativa à prevenção e resolução de conflitos de exercício de competência em processo penal, (JOUE L 328/42, de 15.12.2009), p. 42.

⁵¹⁴ Decisão-Quadro 2001/413/JAI do Conselho de 28 de maio de 2001, relativa ao combate à fraude e à contrafacção de meios de pagamento que não em numerário, (JOCE L 149/1, de 2.6.2001).

⁵¹⁵ Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas), (JOCE L 201/37, de 31.7.2002).

⁵¹⁶ (COM(2009) 149 final), 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”. Disponível em http://europa.eu/legislation_summaries/information_society/si0010_en.htm.

2.2.2. – Análise das disposições da Diretiva sobre o Cibercrime

A Diretiva que ora analisamos tem como finalidade aproximar as infrações penais no domínio de ataques contra sistemas de informação dos Estados Membros e estabelecer regras mínimas relativas às sanções aplicáveis e respetivas infrações. Visa igualmente, facilitar a prevenção da prática desse tipo de infrações e melhorar a cooperação entre as autoridades judiciais e outras autoridades competentes, tais como: a Eurojust, a Europol e o seu Centro Europeu de Cibercriminalidade, e a Agência Europeia para a Segurança das Redes e da Informação (artigo 1.º).

O artigo 2.º, sob a epígrafe “definições”, apenas enuncia as mesmas definições já plasmadas na Decisão-Quadro 2005/222/JAI, relativamente ao que se deve entender por: “Sistemas de informação”, “Dados informáticos”, “Pessoa colectiva” e acesso ou interferência “Não autorizado”.⁵¹⁷

O mesmo sucede com os artigos 3.º a 5.º, referentes ao “acesso ilegal a sistemas de informação”, à “interferência ilegal no sistema” e à “interferência ilegal nos dados”, respetivamente, mantêm a mesma redação e epígrafes dos artigos 2.º a 4.º, respetivamente, da Decisão-Quadro 2005/222/JAI.

O artigo 6.º é inovador no que à interceção ilegal diz respeito. Esta norma prevê a adoção pelos Estados Membros de medidas necessárias para assegurar que a interceção intencional e não autorizada, através de meios técnicos, de transmissões não públicas de dados informáticos, a partir de ou num sistema de informação, incluindo emissões eletromagnéticas de um sistema de informação que comporte esses dados, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade.⁵¹⁸

Desta forma, pretende-se criminalizar a ingerência nas comunicações recorrendo a quaisquer tipo de dispositivos que possam intercetar a comunicação de dados, em, plena analogia com a interceção das comunicações telefónicas, punível em todos os ordenamentos jurídicos internacionais⁵¹⁹.

⁵¹⁷ Ramos, Armando R. Dias, *A novíssima Diretiva relativa ao cibercrime*, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014, p.181.

⁵¹⁸ *Idem Ibidem*.

⁵¹⁹ *Idem, Op. Cit.*, p. 182, *apud.*, Conceição, Ana Raquel, *Escutas Telefónicas, Regime Processual Penal*, Quid Juris, 2009, pp.60 a 66.

O artigo 7.º, sob a epígrafe “Instrumentos utilizados para cometer infrações” proíbe a produção, venda, aquisição para utilização, importação, detenção, distribuição ou qualquer outra forma de disponibilização de instrumentos utilizados para cometer infrações, tais como:

- a) Um programa informático, concebido ou adaptado essencialmente para cometer uma das infrações previstas nos artigos 3.º a 6.º;
- b) Uma senha, um código de acesso ou dados similares que permitam aceder à totalidade ou a parte de um sistema de informação.

Importa referir, que nestes casos se exige o elemento volitivo do dolo, já que como se prevê nesta norma “o intuito da sua utilização para a prática de uma das infrações previstas”, sempre que se revistam de alguma gravidade.⁵²⁰ Desta forma, afasta-se a punibilidade por factos praticados por mera negligência.

O artigo 8.º, relativo à “Instigação, cumplicidade e tentativa”, prevê que os Estados Membros assegurem que a instigação, o auxílio e a cumplicidade sejam puníveis como infrações penais (n.º1), bem como a tentativa da prática de tais ilícitos (n.º2). Esta norma já se encontrava prevista no artigo 5.º da Decisão-Quadro 2005/222/JAI, caindo agora a possibilidade de cada Estado Membro decidir se a tentativa seria ou não punível, relativamente ao acesso ilegal de sistemas de informação.⁵²¹

Quanto às “Sanções”, previstas no artigo 9.º da presente Diretiva, apresentam algumas diferenças face à anterior Decisão-Quadro 2005/222/JAI. Anteriormente, os limites máximos situavam-se entre um a três anos de pena de prisão.

Nos termos do artigo 9.º, sempre que esteja em causa um crime de interferência ilegal a sistema de informação (artigo 3.º) ou interferência ilegal no sistema (artigo 4.º), e sejam estes cometidos de forma intencional afetando um número significativo de sistemas de informação, com recurso aos instrumentos mencionados no artigo 7.º, a punição máxima deverá ser a de pena de prisão não inferior a três anos.⁵²²

⁵²⁰ Ramos, Armando R. Dias, *A novíssima Diretiva relativa ao cibercrime*, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014, p. 182.

⁵²¹ *Idem, Ibidem.*

⁵²² *Idem, Op. Cit.*, p. 183.

Estendeu-se a pena máxima não inferior a cinco anos para os casos em que as ações são cometidas por organizações criminosas, na aceção da Decisão-Quadro 2008/841/JAI (relativa à luta contra a criminalidade organizada), do Conselho, ou quando causem danos graves ou, ainda, quando sejam cometidas contra um sistema de informação que constitua uma infraestrutura crítica.⁵²³

O artigo 10.º é outro dos artigos que manteve os mesmos termos da anterior Decisão-Quadro 2005/222/JAI, a responsabilidade das pessoas coletivas pelas infrações previstas nos artigos 3.º a 8.º. Porém, o n.º3 do referido artigo comporta uma ressalva: não se exclui a possibilidade de ação penal contra as pessoas singulares que sejam autoras, instigadoras ou cúmplices das infrações previstas nos artigos 3.º a 8.º.

O artigo 11.º consagra as sanções aplicáveis às pessoas coletivas, tendo sido acrescentada a sanção de encerramento temporário ou definitivo dos estabelecimentos utilizados para a prática da infração (n.º1, alínea e). Esta sanção não se encontrava prevista na anterior Decisão-Quadro.

As restantes sanções aplicadas às pessoas coletivas são:

- a) A exclusão do direito a benefícios ou auxílios públicos;
- b) A proibição temporária ou permanente de exercer atividades comerciais;
- c) A colocação sob vigilância judicial;
- d) A liquidação judicial.

Quanto à competência para instaurar o procedimento criminal, prevê o artigo 12.º, a regra segue o Princípio da Territorialidade, sempre que a infração tenha sido cometida total ou parcialmente no seu território (n.º1 alínea a); ou por um dos seus nacionais, pelo menos nos casos em que o ato constitua infração no local em que seja praticado (n.º1 alínea b).

Segundo o número 2 do mesmo artigo, podem ainda ser competentes, em matéria penal, nos casos em que:

⁵²³ Ramos, Armando R. Dias, *A novíssima Diretiva relativa ao cibercrime*, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014, p. 183.

- a) O autor tenha cometido a infração quando se encontrava fisicamente presente no seu território, independentemente de a infração ter ou não sido cometida contra um sistema de informação situado nesse território; ou
- b) A infração tenha sido cometida contra um sistema de informação situado no seu território, independentemente de o seu autor se encontrar ou não fisicamente presente nesse território.

Quanto à competência relativamente às pessoas coletivas (n.º3), o Estado Membro poderá alargar a sua competência para instaurar o procedimento criminal, quanto às infrações previstas nos artigos 3.º a 8.º, cometidas fora do seu território, desde que informe a Comissão. Nomeadamente caso:

- a) “O autor tenha a sua residência habitual no seu território; ou
- b) A infração tenha sido cometida em benefício de uma pessoa coletiva estabelecida no seu território.”

Segundo o artigo 13.º, prevê-se um alargamento da troca de informações entre os Estados Membros. Como tal, os Estados Membros devem assegurar a existência de um ponto de contacto operacional nacional e recorrer à rede existente de pontos de contacto operacionais disponível 24 horas por dia e sete dias por semana. Nos casos urgentes, os Estados Membros devem igualmente assegurar procedimentos que lhes permitam indicar, no prazo máximo de oito horas a contar da receção do pedido, se o pedido será deferido, e a forma e o prazo estimado (n.º1). Este limite temporal não existia na anterior Decisão-Quadro.

O artigo 14.º, relativo ao “acompanhamento e estatísticas”, prevê cada Estado Membro deverá assegurar a criação de um sistema de registo, produção e disponibilização de dados estatísticos sobre as infrações previstas nos artigos 3.º a 7.º (n.1). Os dados recolhidos deverão ser transmitidos à Comissão Europeia, e posteriormente publicados de forma consolidada (n.º3).

Por fim, importa referir que a Proposta de Diretiva previa a revogação integral da Decisão-Quadro 2005/222/JAI.⁵²⁴ Contudo no Parlamento entendeu-se que apenas se devia substituir a Decisão-Quadro pela presente Diretiva relativamente aos Estados

⁵²⁴ Ramos, Armando R. Dias, *A novíssima Diretiva relativa ao cibercrime*, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014, p.185.

Membros que participaram na adoção desta Diretiva. Quanto aos Estados Membros que não participam na adoção da presente diretiva as remissões para a Decisão-Quadro 2005/222/JAI devem entender-se como sendo feitas para a presente diretiva (artigo 15.º).

2.2.3. – Avaliação crítica

Após a análise das disposições da presente Diretiva, importa refletir sobre os seus aspetos mais importantes, dos quais destacamos cinco:

- Aproximar o direito penal dos Estados Membros no âmbito dos ataques contra os sistemas de informação, estabelecendo um conjunto de regras mínimas relativamente às infrações penais e às suas sanções;⁵²⁵
- Reforçar a instigação, auxílio, cumplicidade e tentativa, como forma de infração penal dos ilícitos previstos, no artigo 8.º, deixando os Estados Membros de ter plena decisão de aplicação ou não das mesmas;⁵²⁶
- Combater a utilização de *botnets* para fins criminosos, que coloca em causa os sistemas de informação de infraestruturas críticas da União Europeia, compromete a existência de uma sociedade de informação mais segura e, também de um espaço de liberdade, segurança e justiça;⁵²⁷
- Aumentar a eficácia dos pontos de contacto 24/7, responsáveis pela aplicação da lei nos Estados Membros;⁵²⁸ e,
- Solucionar a falta de dados estatísticos sobre os ciberataques.⁵²⁹

No entanto, esta Diretiva padece de algumas lacunas. No domínio das infrações penais, a presente Diretiva não é muito inovadora, pelo menos quando comparada com a legislação portuguesa, uma vez que alguns dos artigos já se encontravam plasmados na Decisão-Quadro que se pretendia substituir e em outros diplomas, como a Lei do Cibercrime ou no próprio Código Penal.

Com efeito, a não revogação imediata da anterior Decisão-Quadro será geradora de confusão e divergências, já que no plano formal existem dois diplomas em vigor, adotados por Estados diferentes: por um lado para os que participaram na presente Diretiva aplicar-se-á esta; por outro lado, para os que não contribuíram para a

⁵²⁵ Ramos, Armando R. Dias, *A novíssima Diretiva relativa ao cibercrime*, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014, p.185.

⁵²⁶ *Idem*, *Op. Cit.*, p. 187.

⁵²⁷ *Idem*, *Op. Cit.*, p.186.

⁵²⁸ *Idem*, *Ibidem*.

⁵²⁹ *Idem*, *Ibidem*.

elaboração da presente Diretiva, continuará a vigorar a Decisão-Quadro 2005/222/JAI.⁵³⁰

Quanto às definições, esta Diretiva não enquadra conceitos atuais tais como os conteúdos alojados na *cloud*, nomeadamente, falta definir onde efetivamente estes conteúdos se encontram alojados e quem tem competência para o impulso processual.⁵³¹ Ainda no domínio das competências, é dada a possibilidade de cada Estado Membro definir as suas próprias competências, tal como dispõe o n.º1, do artigo 12.º da presente Diretiva. Da análise deste artigo, pode originar, em *ultima ratio*, uma dupla perseguição penal por dois ou mais Estados Membros, colocando em evidência o Princípio do *ne bis in idem*.⁵³²

Da mesma forma, o legislador europeu, não definiu na Diretiva, o que se deve entender por “alguma gravidade”. Esta expressão está presente em alguns artigos, e poderá originar várias interpretações e discrepâncias de Estado para Estado.

Em face do exposto, concluímos que a presente Diretiva 2013/40/UE, do Parlamento Europeu e do Conselho, ficou aquém do quadro atual da *Cibercriminalidade*. As novas tecnologias avançam a um ritmo estonteante, incapaz de ser acompanhado pelo Direito, e a presente Diretiva é mais um exemplo dessa dificuldade de atuação já que se centra, essencialmente, na uniformização do Direito Penal e ignora a parte processual no que à recolha de prova diz respeito. Não obstante, a presente Diretiva reforce a cooperação e a troca de informação (em alguns casos, de forma rápida) entre os Estados Membros, é fundamental definir concretamente métodos de recolha e de armazenamento de provas, já que a prova digital é o único meio de conseguir uma efetiva condenação dos seus prevaricadores.⁵³³

⁵³⁰ Ramos, Armando R. Dias, *A novíssima Diretiva relativa ao cibercrime*, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014, pp.189 e 190.

⁵³¹ *Idem*, *Op. Cit.*, p.190.

⁵³² *Idem*, *Ibidem*.

⁵³³ *Idem*, *Op. Cit.*, p.191.

2.3. – Resposta Institucional

A *Internet* sem fronteiras e global tornou-se num dos mais poderosos instrumentos de progresso a nível mundial sem supervisão ou regulação governamental. Apesar de o setor privado continuar a desempenhar um papel primordial na construção e na gestão quotidiana da *Internet*, torna-se cada vez mais importante criar requisitos de transparência, responsabilização e segurança. Da mesma forma, torna-se fundamental a cooperação entre todos os Estados e as Instituições criadas para o combate à *Cibercriminalidade*.

Existem a nível da União Europeia instituições que combatem diariamente as ameaças colocadas por este fenómeno criminal, entre as quais destacamos: Europol, EC3 e a Agência Europeia de Defesa (AED). Estas são três agências ativas, respetivamente, no campo da repressão e da defesa, com conselhos de administração em que estão representados os Estados Membros e constituem plataformas de coordenação a nível da União Europeia.⁵³⁴

Existe uma vasta coordenação e colaboração entre estas agências numa série de domínios em que estão envolvidas conjuntamente, nomeadamente no que diz respeito à análise das tendências, à avaliação dos riscos, à formação e à partilha das melhores práticas. Estas agências, conjuntamente com a equipa CERT-EU (*Computer Emergency Response Team*), a Comissão e os Estados Membros, têm como principal função apoiar o desenvolvimento de uma comunidade de confiança de peritos técnicos e políticos neste domínio.⁵³⁵

Neste contexto, destacamos também pela positiva o desempenho e participação da Europol, da Eurojust e das autoridades nacionais de proteção de dados.

Os *ciberataques* são uma das formas de atuação mais comum, causando mais de um milhão de vítimas por dia em todo o mundo. Os agentes e as redes de *Cibercriminalidade* estão a tornar-se cada vez mais sofisticados, pelo que é fundamental dispor de ferramentas operacionais corretas e de capacidades para os combater.⁵³⁶

⁵³⁴ (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013. p.20.

⁵³⁵ *Idem*, *Op. Cit.*, p.20 e 21.

⁵³⁶ *Idem*, *Op. Cit.*, p. 9 e 10.

Esta é uma atividade altamente lucrativa e de baixo risco, já que os cibercriminosos se aproveitam do anonimato dos domínios dos sítios, da rapidez com que os dados podem ser mudados ou apagados e ainda do formato transnacional que a *Internet* proporciona aos seus utilizadores, sendo possível praticar um ataque informático em qualquer ponto do mundo, a partir de qualquer lado, em segundos.

Em seguida, vamos analisar duas das Instituições que diariamente combatem este tipo de criminalidade: a *Europol* e o *Centro Europeu de Cibercriminalidade*.

2.3.1. - Europol

Como analisámos anteriormente, a *Cibercriminalidade* é um tipo de crime que não conhece jurisdições nem fronteiras e que tem um impacto na economia mundial de mais de 400 mil milhões de dólares em cada ano.

Para combater eficazmente este tipo de criminalidade é fundamental que todas as entidades cooperem no combate a esta nova ameaça. Uma dessas entidades é a Europol⁵³⁷. A Europol desempenha um papel fundamental na União Europeia, reconhecido pelos Estados Membros e por outras entidades, como é o caso da Interpol, e as autoridades internacionais responsáveis pela aplicação da lei, dispondo também de competências em matéria de criminalidade informática.

A principal função da Europol é contribuir para uma Europa mais segura em benefício de todos os cidadãos, apoiando as autoridades responsáveis pela aplicação da lei na União Europeia através do intercâmbio e análise de informações de natureza criminal.⁵³⁸

Ao longo dos anos a Europol tem-se destacado das outras entidades ao contribuir de forma significativa para o combate à *Cibercriminalidade*, tendo mesmo multiplicado as suas atividades. Um desses exemplos foi o desempenho numa grande operação levada a cabo em 2012, denominada “Rescue”, em que foram detidas 184 pessoas suspeitas de crimes sexuais contra crianças e onde foram identificadas mais de 200 crianças vítimas de abusos.⁵³⁹

A Europol é também, uma das entidades que mais tem cooperado com os Estados Membros no combate à *Cibercriminalidade*. Desta forma, adotou um acordo de cooperação com EC3 e a ENISA, como forma de “reforçar o apoio aos Estados Membros e às instituições da União Europeia na prevenção e na luta contra a

⁵³⁷ *Europol* – De acordo com a Decisão 2009/371/JAI do Conselho, de 6 de abril de 2009, a Europol é um organismo da União Europeia, com sede em Haia, responsável pela cooperação em matéria de aplicação da lei a nível europeu, reforçando as ações empreendidas pelos Estados Membros em matéria de prevenção e combate à criminalidade organizada, ao terrorismo e a outras formas graves de criminalidade que afetem dois ou mais Estados Membros. Decisão 2009/371/JAI do Conselho, de 6 de abril de 2009, que cria o *Serviço Europeu de Polícia, Europol*, artigo 4.º, n.º1, em conjugação com o anexo.

⁵³⁸ (COM (2012) 140 final), *Comunicação da Comissão ao Conselho e ao Parlamento Europeu*, “Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade”, Bruxelas, 28.3.2012, p.7.

⁵³⁹ Tal só foi possível graças a uma das maiores investigações policiais deste tipo levadas a cabo em todo o mundo. Foi graças ao trabalho dos analistas da Europol que conseguiram neutralizar os mecanismos de segurança de um servidor informático no centro da rede, que permitiu descobrir a identidade e as atividades dos alegados autores dos crimes. *Idem, Op. Cit.*, p.3.

Cibercriminalidade”⁵⁴⁰. Tal como revelam Udo Helmbrecht e Rob Wainwright⁵⁴¹, “o presente acordo representa um passo importante na luta contra cibercriminosos ainda mais experientes que investem cada vez mais tempo, dinheiro e gente em ataques direcionados. O nosso acordo é a prova de como estamos fortemente empenhados em contribuir conjuntamente nas nossas respetivas áreas de competência, e em apoiar o trabalho de cada um com o objetivo de tornar a Europa um espaço mais seguro em linha. Sabendo-se que a *Cibercriminalidade* custa à economia mundial mais de 400 mil milhões de dólares em cada ano, com uma cooperação mais estreita e a partilha de conhecimentos estamos a reforçar a capacidade da Europa para combater os cibercriminosos”.⁵⁴²

Do presente acordo destacamos, pela sua importância, as seguintes “áreas de cooperação”:

- “O intercâmbio de conhecimentos e experiências práticas;
- A elaboração de relatórios de análises da situação;
- Informação decorrente de análises estratégicas e boas práticas;
- Reforço da capacidade institucional mediante formação e sensibilização para garantir a segurança das redes e informações a nível da União Europeia. Fora desta cooperação ficou a partilha de dados pessoais”.⁵⁴³

A *Cibercriminalidade* reveste-se de um conjunto de características que a tornam numa atividade aliciante e esse é um dos aspetos que mais tem contribuído para o aumento do número de agentes criminosos e consequentemente, um aumento do número de vítimas.⁵⁴⁴

É a pensar neste aumento de crimes que a Europol continua a adotar estratégias e cooperações entre entidades para travar estas previsões. Uma das mais recentes estratégias adotadas pela Europol foi a criação de um grupo de combate ao *Cibercrime* na

⁵⁴⁰ “ENISA e Europol cooperam contra a cibercriminalidade”, [Em linha]. Disponível em <http://inteligenciaeconomica.com.pt/?p=22282>, (consultado em 15.12.2014).

⁵⁴¹ Udo Helmbrecht, Diretor Executivo da ENISA e o Diretor da Europol, Rob Wainwright, “em declaração conjunta, após assinatura da parceria estabelecida entre as duas entidades”, [Em linha]. Disponível em <http://inteligenciaeconomica.com.pt/?p=22282>, (consultado em 15.12.2014).

⁵⁴² “ENISA e Europol cooperam contra a cibercriminalidade”, [Em linha]. Disponível em <http://inteligenciaeconomica.com.pt/?p=22282>, (consultado em 15.12.2014).

⁵⁴³ *Idem, Ibidem.*

⁵⁴⁴ Uma vez que os lucros ilícitos obtidos através da *cibercriminalidade* são, em regra, muito avultados, alguns grupos de criminosos estão a adotar práticas empresariais do mundo das tecnologias de informação para desenvolverem mais e melhores ferramentas para as atividades de *cibercriminalidade*. *Idem, Ibidem.*

União Europeia e em outros países. A *Joint Cybercrime Action Taskforce* (J-CAT) irá coordenar investigações internacionais para tomar medidas contra as principais ameaças *online* e os principais alvos, tais como fóruns ocultos e os principais ataques de *malwares*, incluindo os vírus *trojans* bancários, *botnets* e fraudes online.⁵⁴⁵ Como revela Troels Ørting⁵⁴⁶ “ o objetivo é prevenir o Cibercrime, levá-lo à disrupção, apanhar bandidos e apreender os seus lucros ilegais. Este é um primeiro passo de uma longa caminhada em direção a uma *Internet* aberta, transparente, livre, mas também segura”.

Deste grupo fazem parte o *Centro Europeu da Cibercriminalidade*, a *EU Cybercrime Taskforce*, o *FBI* e a *National Crime Agency* (NCA) do Reino Unido. A equipa da J-CAT é composta por agentes de ligação dos Estados Membros da União Europeia e ainda por autoridades não pertencentes à União Europeia.⁵⁴⁷

É graças à atuação de entidades como a Europol que, em cooperação com a União Europeia, tem sido possível acompanhar os desenvolvimentos no mundo do *Cibercrime*. No entanto, à medida que a *Internet* evolui, evoluem também as técnicas de *Cibercriminalidade*, o número de agentes e o número de ameaças à sociedade de informação. Como tal e face a estas novas ameaças, será fundamental uma atuação cada vez mais direta e coerciva por parte destas entidades, assim como uma maior cooperação entre elas.

⁵⁴⁵ Disponível em <http://www.computerworld.com.pt/2014/09/01/europol-lanca-grupo-internacional-contracibercrime/>, (consultado em 15.12.2014).

⁵⁴⁶ Troels Ørting, Chefe do Centro Europeu de Cibercriminalidade (EC3).

⁵⁴⁷ À data do comunicado faziam parte da equipa da J-CAT Estados como o Canadá, Áustria, Alemanha, França, Holanda, Itália, Espanha, Reino Unido e os Estados Unidos da América. E segundo a Europol, a Austrália e a Colômbia também se comprometeram com esta iniciativa.

2.3.2. – Centro Europeu de Cibercriminalidade (EC3)

Face ao aumento da *Cibercriminalidade*, em março de 2012, a Comissão “propôs a criação de um Centro (...)”⁵⁴⁸ específico para o combate a este tipo de criminalidade.

De acordo com a Comissão Europeia, este Centro teria como missão o combate aos “grupos de criminalidade organizada”, dando especial atenção aos “ataques dirigidos contra os serviços bancários e outras operações financeiras em linha”⁵⁴⁹.

Em janeiro de 2013, tal como se tinha previsto, foi então criado o *Centro Europeu de Cibercriminalidade*, também conhecido como EC3 (*European Cybercrime Center*)⁵⁵⁰.

A principal função deste Centro é dificultar as operações das redes de criminalidade organizada que cometem a chamada “cibercriminalidade grave e organizada”⁵⁵¹. Mais concretamente apoia e coordena as operações e as investigações conduzidas pelas autoridades dos Estados Membros em diversos domínios, como por exemplo, os crimes de alta tecnologia, ciberataques, programas malignos, *botnets*, exploração sexual de menores em linha e fraude em matéria de pagamentos.

Quanto aos *crimes de alta tecnologia*, tais como ciberataques e programas malignos, o EC3 desempenha um papel importante nas operações contra estes ataques. Neste sentido, foram também concluídas duas grandes investigações internacionais (*Ransom* e *Ransom II*), que estavam relacionadas com a denominada *Police Ransomware*⁵⁵².

De acordo com as informações da Comissão, o EC3 tem também apoiado várias iniciativas internacionais no âmbito da “eliminação de *botnet* (rede de computadores

⁵⁴⁸ Sobre este tema consultar (COM (2012) 140 final) Comunicação da Comissão ao Conselho e ao Parlamento Europeu, *Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade*, Bruxelas, 28 de março de 2012, p.4.

⁵⁴⁹ Comissão Europeia, Comunicado de Imprensa, *Cibercriminalidade: cidadãos da União Europeia preocupados com a segurança dos dados pessoais e dos pagamentos em linha*, Bruxelas, 9 de julho de 2012, p. 2.

⁵⁵⁰ O EC3 faz parte da Europol e encontra-se sediado nas suas instalações. Esta partilha de instalações é essencial para garantir a participação de outros intervenientes importantes na sua direção estratégica. (COM (2012) 140 final), Comunicação da Comissão ao Conselho e ao Parlamento Europeu, *Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade*, Bruxelas, 28 de março de 2012, p.7.

⁵⁵¹ Para mais informações sobre esta matéria é importante consultar o European Commission Memo, *Frequently ask questions: The European Cybercrime Center EC3*, [Em linha], Brussels, 9 January 2012. Disponível em http://europa.eu/rapid/press-release-MEMO-13-6_en.htm, (consultado em 17.12.2014).

⁵⁵² Trata-se de “um tipo de programa maligno que bloqueia o computador da vítima, acusando-a de ter visitado sítios ilegais que contêm material de maus tratos a menores ou outras atividades ilegais”. Comissão Europeia, Comunicado de Imprensa, “Centro Europeu de Cibercriminalidade – um ano depois”, Bruxelas, 10.2.2014, p. 2.

infetados), desmantelamento e investigação de fóruns criminosos e ataques de programas malignos contra instituições financeiras”⁵⁵³, como aconteceu no “processo de desmantelamento do *botnet ZeroAccess*, em conjunto com a Microsoft e as unidades contra a criminalidade de alta tecnologia da BKA alemã, dos Países Baixos, da Letónia, do Luxemburgo e da Suíça”.⁵⁵⁴

O EC3 tem, igualmente, desempenhado um papel fundamental nos casos de exploração sexual de menores, maus tratos, comercialização de imagens e vídeos na *Internet*, apoiando várias operações e investigações neste âmbito.

Durante o primeiro ano de atuação do EC3, foram efetuados esforços significativos, em cooperação com muitos Estados Membros e parceiros de cooperação de países terceiros, na luta contra as atividades ilegais de pedófilos envolvidos na exploração sexual de crianças na *Internet* através da utilização de serviços ocultos.⁵⁵⁵ Neste sentido, os agentes investigam constantemente a chamada “*DarkNet*”, “onde os pedófilos comercializam material ilegal de maus tratos a menores em fóruns ocultos, bem como às investigações à *sextortion*”⁵⁵⁶.

Outro dos pontos de atuação do EC3 diz respeito à *fraude em matéria de pagamentos*. Em 2013 colaborou e apoiou investigações que deram origem ao desmantelamento e apreensão de três redes internacionais diferentes, responsáveis por fraudes a cartões de crédito⁵⁵⁷.

Neste sentido, a Federação de Bancos Europeus (*The European Banking Federation – EBF*) e o EC3 assinaram um memorando de entendimento (*MoU*) que realça formas de intensificar a cooperação entre o Direito e o setor financeiro da União Europeia.

⁵⁵³ Comissão Europeia, *Comunicado de Imprensa*, “Centro Europeu de Cibercriminalidade – um ano depois”, Bruxelas, 10.2.2014, p. 2.

⁵⁵⁴ *Idem, Ibidem.*

⁵⁵⁵ *Idem, Ibidem.*

⁵⁵⁶ *Sextortion* – Segundo a Comissão Europeia, *Sextortion* “é a designação dada ao fenómeno em que os abusadores do menor têm acesso a imagens inapropriadas de menores, que utilizam para coagir as suas vítimas a realizar novos atos; caso contrário, o abusador envia as imagens à família e aos amigos da vítima”. *Idem, Ibidem.*

⁵⁵⁷ Para mais informação sobre esta matéria é importante consultar *Comissão Europeia, Comunicado de Imprensa*, “Centro Europeu de Cibercriminalidade – um ano depois”, Bruxelas, 10.2.2014, pp. 2 e 3.

Dado o aumento dos crimes tecnológicos que têm afetado o setor financeiro⁵⁵⁸, espera-se que esta cooperação entre o EBF e o EC3 traga resultados positivos na prevenção e combate aos novos tipos de crimes tecnológicos, como é o caso do aumento de técnicas de crimes como “*phishing*” e *malwares informáticos*.⁵⁵⁹

A *Internet* continua a evoluir, assim como as técnicas e os meios utilizados pelos cibercriminosos. Num futuro próximo, é necessário que entidades como o EC3 adotem mecanismos e estratégias de defesa contra a *Cibercriminalidade* em tempo real, que cooperem com outras entidades para dismantelar estas redes, mediante uma detenção mais eficaz das novas formas de *Cibercrime* e da rápida detenção dos criminosos informáticos. Só desta forma será possível o Direito estar a par da evolução tecnológica.

Como revela Cecilia Malmström “o comportamento criminoso está a mudar a um ritmo acelerado, explorando os desenvolvimentos tecnológicos e as lacunas jurídicas. Os infratores continuarão a ser criativos, a desenvolver ataques sofisticados para fazer mais dinheiro e temos de ser capazes de os acompanhar. Os conhecimentos especializados desenvolvidos pelo EC3 estão a ajudar-nos a combater nesta batalha e a estimular a cooperação europeia. Através de várias operações bem sucedidas e de grande envergadura no ano passado, o *Centro Europeu de Cibercriminalidade* já obteve uma merecida popularidade entre as autoridades com funções coercivas”⁵⁶⁰.

Também a este respeito acrescenta Troels Ørting⁵⁶¹ referindo que, “nos doze meses decorridos desde o início da atividade do EC3, temos estado extremamente ocupados a ajudar as autoridades com funções coercivas da UE a prevenir e a investigar a cibercriminalidade transnacional. Estou orgulhoso e satisfeito com os resultados obtidos até agora, mas não podemos descansar sobre os louros conquistados. Estou especialmente preocupado com as formas cada vez mais complexas de programas malignos que estão a emergir juntamente com os embustes informáticos tecnologicamente mais avançados e a denominada “*sextortion*” de menores. Ainda só vimos a ponta do iceberg, mas o EC3, auxiliado pelos nossos reputados parceiros e

⁵⁵⁸ Como concluiu um “inquérito do Eurobarómetro, (...) 7% foram vítimas de fraude com o cartão de crédito ou com os serviços bancários em linha”. *Comissão Europeia, Comunicado de Imprensa*, “Centro Europeu de Cibercriminalidade – um ano depois”, Bruxelas, 10.2.2014, p. 1.

⁵⁵⁹ Gabinete Nacional de Segurança, *Cyber Newsletter*, n.º 35/2014, [Em linha], p. 13. Disponível em <http://www.gns.gov.pt/new-ciberseguranca/newsletter.aspx> (consultado em 17.12.2014).

⁵⁶⁰ *Comissão Europeia, Comunicado de Imprensa*, “Centro Europeu de Cibercriminalidade – um ano depois”, Bruxelas, 10.2.2014, p. 1.

⁵⁶¹ Troels Ørting, Chefe do Centro Europeu de Cibercriminalidade.

partes interessadas, está apostado em apoiar as futuras operações de cibercriminalidade de primeira linha dos Estados Membros”⁵⁶².

Um dos objetivos comuns das autoridades responsáveis pela aplicação da lei, assim como do setor privado, é adotar ideias e estratégias claras e precisas no combate à *Cibercriminalidade*. E, neste aspeto, o EC3, em cooperação com a Europol e os Estados Membros têm desenvolvido um papel fundamental.

⁵⁶² Comissão Europeia, *Comunicado de Imprensa*, “Centro Europeu de Cibercriminalidade – um ano depois”, Bruxelas, 10.2.2014, p. 1.

3. A Luta contra a Cibercriminalidade na Ordem Jurídica Portuguesa

3.1. – Enquadramento

Desde cedo as leis portuguesas tiveram um papel ativo na luta contra a Criminalidade Informática e o legislador nacional inspirou-se, em grande parte, nos princípios diretores constantes do Relatório do Comité Europeu para os Problemas Criminais, do Conselho da Europa, seguindo inclusive a Recomendação N.º R (89) 9 do Comité de Ministros aos Estados Membros, sobre Criminalidade relativa ao Computador, de 13 de setembro de 1989, para editar a Lei n.º109/91, de 17 de agosto.⁵⁶³

Embora os casos de *Cibercriminalidade* e o impacto por estes causados na sociedade não fosse tão grave como é atualmente, esta matéria sempre fez parte do ordenamento jurídico português.

Começando pelo Código Penal de 1982, era visível, quanto a esta matéria, o domínio da proteção dos dados pessoais, aparecendo o preceito claramente inspirado na *Convenção Europeia para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal*.

A Lei n.º 10/91, de 29 de abril, a denominada *Lei da Proteção de Dados Pessoais face à Informática (LPDPI)*, alterada pela Lei n.º28/94, de 29 de agosto, possuía um esquema geral de infrações previstas no capítulo VIII, nos artigos 34.º a 43.º, muito mais amplo do que o artigo 181.º do Código Penal de 1982 (devassa por meio da informática)⁵⁶⁴.

Em 1991, graças à Recomendação 89/9 do Conselho Europeu, foi publicada, através da Lei n.º 109/91, de 17 de agosto, a *Lei da Criminalidade Informática (LCI)*. Nesta Lei já era possível identificar as definições de novos tipos de crimes que o Conselho da Europa havia aconselhado aos legisladores nacionais regularem. Esta Lei adotou alguns

⁵⁶³ Marques, Garcia; Martins, Lourenço, *Lições de Direito da Comunicação, Direito da Informática*, Almedina, Novembro 2000, p.510.

⁵⁶⁴ O que tinha de interessante à data da sua publicação era saber se toda a previsão deste último preceito (artigo 181.º do Código Penal de 1982) estava ou não absorvida pelas disposições da nova Lei 10/91 de 29 de abril. Segundo Garcia Marques e Lourenço Martins a resposta parece ser afirmativa quanto ao n.º 1 desse artigo 181.º da versão anterior do Código Penal. Como referem “bastava confrontar o conteúdo das alíneas a) a d) do n.º 1 desse artigo 181.º com os artigos 34.º, números 1 e 3, artigo 37.º e 39.º da *Lei da Proteção de Dados Pessoais face à Informática (LPDPI)*, para constatar que esta lei posterior regulava tudo o que estava previsto naquele preceito do Código Penal”.

Acresce ainda que outras normas específicas estendiam as sanções ainda à obstrução ao acesso (tal como previa o artigo 35.º), à interconexão ilegal (artigo 36.º) e ao acesso indevido (artigo 38.º). *Idem, Op. Cit.*, p.513.

dos tipos de crimes constantes da “lista facultativa dos tipos criminais” daquela Recomendação, tais como:

- *Falsidade informática;*
- *Dano relativo a dados ou programas informáticos;*
- *Sabotagem informática;*
- *Acesso ilegítimo;*
- *Interceção ilegítima;*
- *Reprodução ilegítima de programa protegido.*

A Lei n.º109/91 previa ainda a responsabilidade criminal das pessoas coletivas que pratiquem estes crimes, bem como diversas penas acessórias. Esta Lei punia não só os administradores das empresas, como as próprias empresas.

A primeira previsão que aparecia dessa lista facultativa adotada pelo legislador português era a *fraude informática*. Esta era definida como o “tipo legal destinado a proteger a integridade da propriedade e a confiança na fiabilidade das transferências eletrónicas de fundos, com relevo especial para o abuso das máquinas de levantamentos automáticos”⁵⁶⁵.

Seguidamente no artigo 4.º aparecia o crime de *falsidade informática* e com esta previsão pretendia-se “proteger interesses semelhantes aos que tradicionalmente são tutelados através dos delitos de falsificação, isto é, a segurança, a fiabilidade, a força probatória dos documentos ou outros instrumentos com importância na vida jurídica quotidiana”⁵⁶⁶.

Os interesses protegidos pelo artigo 5.º da Lei n.º109/91 são os da integridade dos dados e do bom funcionamento e integridade dos programas, já que este artigo diz respeito ao *Dano relativo a dados ou programas informáticos*⁵⁶⁷.

O artigo 6.º dizia respeito à *sabotagem informática*, sendo este um crime de maior gravidade objetiva do que o anterior, já que neste caso o crime tem a ver com *entravar* ou *perturbar* o funcionamento do próprio sistema informático ou de comunicação de dados à distância (telemática).

⁵⁶⁵ Marques, Garcia; Martins, Lourenço, *Lições de Direito da Comunicação, Direito da Informática*, Almedina, Novembro 2000, p.518.

⁵⁶⁶ *Idem, Op. Cit.*, p. 520.

⁵⁶⁷ *Idem, Op. Cit.*, p. 525 e 526.

No artigo 7.º estava previsto o *acesso ilegítimo*, onde o Relatório do Conselho da Europa preconizava que fosse protegido o domicílio informático, uma espécie de “introdução em casa alheia”⁵⁶⁸.

O artigo 8.º refere-se à *interceção ilegítima de sistemas ou redes informáticas*, também designada de *espionagem*⁵⁶⁹.

Por fim, o artigo 9.º previa a *reprodução ilegítima de programa protegido*. Com este artigo tentava-se combater a reprodução de programas originais autênticos em grandes quantidades de programas “piratas”. Os elevados custos a que são comercializados os programas originais de computador contrapostos à facilidade com que são copiados e depois usados ou vendidos, tornaram premente a extensão da proteção penal a esta realidade⁵⁷⁰.

Paralelamente, o Direito nacional tem dado especial relevância à proteção dos dados pessoais, nomeadamente, quanto às questões da privacidade, da partilha e da segurança de dados pessoais. No período tecnológico em que nos encontramos, não podemos descurar as possibilidades e os riscos inerentes à transferência nacional e, mais concretamente, à transferência transnacional de dados via *Internet*, uma vez que se trata de dados pessoais, facultados por cada cidadão e que, por algum descuido, podem consubstanciar crimes. Face a este tipo de ameaças existem especiais medidas de segurança, como as consagradas no artigo 15.º da Lei 67/98, de 26 de outubro, referente aos Dados Pessoais, sendo estas aplicáveis quando esteja em causa o tratamento dos dados referidos nos artigos 7.º, n.º2 e 8.º, n.º1 da referida Lei.

Igualmente o artigo 4.º da Lei n.º 109/91, de 17 de agosto, é aplicado neste âmbito já que prevê o crime de falsidade informática. Esta previsão visa proteger a segurança e a força probatória dos documentos. A manipulação de dados ou programas com valor probatório é comparável à falsidade de outros documentos.

⁵⁶⁸ O artigo oficial dispunha o seguinte: “L'accès sans droit à un système ou un réseau informatique par violation des règles de sécurité”. Marques, Garcia; Martins, Lourenço, *Lições de Direito da Comunicação, Direito da Informática*, Almedina, Novembro 2000, p. 529.

⁵⁶⁹ Como aparece na definição da alínea f) do artigo 2.º do diploma “o ato destinado a captar informações contidas num sistema automatizado de dados, através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros”. *Idem, Op. Cit.*, p. 532.

⁵⁷⁰ O artigo 9.º reproduzia a sugestão do Conselho da Europa que era no sentido da tipificação penal ao referir: “La reproduction, la diffusion ou la communication au public, sans droit, d'un programme informatique protégé par la loi”. De igual forma o Direito Português seguiu também a definição elaborada pela *Organização Mundial da Propriedade Intelectual* (1978). *Idem, Op. Cit.*, p. 536.

No Código Penal esta questão também se encontra legislada no artigo 193.º, punindo com pena de prisão até dois anos ou com pena de multa até 240 dias aquele que criar, manter ou utilizar ficheiro automatizado de dados individualizáveis e referentes a convicções políticas, religiosas ou filosóficas, a filiação partidária ou sindical, à vida privada, ou à origem étnica, sendo também a tentativa punível pelo n.º 2 do mesmo artigo.

3.2. – Dificuldades e limitações práticas do quadro jurídico interno no combate à Cibercriminalidade

Uma das dificuldades de combate à *Cibercriminalidade* resulta, desde logo, das suas próprias características. Como analisámos, este é um tipo de crime:

- Transnacional - que não conhece barreiras nem jurisdições;
- Anónimo - graças às ferramentas da *Internet* é possível bloquear ou ocultar a identidade dos seus utilizadores, os chamados *IP*'s;
- Variável - ou seja, é um tipo de crime que está em constante evolução e que apresenta novas formas de atuação mais elaboradas e perigosas;
- Rentável e altamente lesivo - comparativamente ao pouco investimento que é feito nos ataques de *Cibercrime*, o lucro que é obtido é muito elevado e apresenta pequenos riscos para os infratores.

Como resultado destas características apresenta-se uma série de dificuldades de combate à *Cibercriminalidade*: *prevenção, investigação, perseguição, comprovação e punição*.

Começando pela *prevenção*, torna-se difícil antever quais serão os atos praticados já que as técnicas utilizadas estão em constante evolução, assim como a própria *Internet*. O que acontece nestes casos é uma adaptação do Direito e das formas de defesa às técnicas empregues, o que faz com que os órgãos de segurança estejam sempre um passo atrás dos infratores.

A *investigação* é uma das maiores dificuldades apresentadas no combate à *Cibercriminalidade*, já que se depara com muitos entraves, desde logo, pela “análise dos dados de tráfego”⁵⁷¹. Este é o primeiro passo para se “localizar a origem da comunicação”⁵⁷², ou seja, o endereço de *IP*. Em alguns casos, o nome do usuário desse *IP* pode não corresponder ao verdadeiro utilizador que cometeu o crime e aqui surge logo uma das dificuldades de investigação: saber quem é realmente o utilizador daquele *IP*. Para contornar este entrave, é necessário o acesso ao registo dos ficheiros armazenados no histórico pelos prestadores de serviços (*ISPs*), sendo imprescindível a colaboração destas entidades. Uma vez “identificado o ponto emissor, identifica-se o

⁵⁷¹ Dias, Vera, *A Problemática da Investigação do Cibercrime*, Faculdade de Direito, IDPCC, Lisboa, novembro 2010, p.19.

⁵⁷² *Idem, Ibidem*.

IP”⁵⁷³, que por sua vez poderá identificar um domicílio privado, uma habitação, por exemplo, um local de trabalho ou um local público, tais como cibercafés ou um centro comercial.

O passo seguinte, quanto à “investigação” é “a análise do localizado sistema informático” ⁵⁷⁴ do infrator, tentando recolher provas. E, mais uma vez, os meios de investigação são confrontados com uma série de dificuldades, principalmente, com os programas especificamente modificados para dificultar a atuação dos agentes. Sem mencionar os entraves que colocam as próprias redes *wireless*, em que todos os dias navegam, um vasto número de utilizadores sem controlo, em espaços públicos com ligação grátis à *internet*.

Como mencionámos supra, as provas são outra das dificuldades de *investigação*. Contrariamente ao que acontece com os crimes do “mundo real”, as provas nos crimes informáticos são mais fáceis de se perder, já que os infratores conseguem bloquear os dados, modificá-los ou apagá-los em segundos, deixando os órgãos de segurança sem qualquer prova.

A *comprovação* encontra-se ligada à *investigação*, já que não havendo provas dos atos criminosos cometidos, é impossível provar que estes ocorreram⁵⁷⁵. Atualmente existem crimes praticados através de transmissão ao vivo pela *Internet*, a chamada “live streaming”, o que vem dificultar ainda mais esta comprovação, já que a única prova depende da interceção dessa transmissão no momento exato em que está a ser exibida. Um exemplo destes crimes é a pornografia infantil⁵⁷⁶.

⁵⁷³ Dias, Vera, *A Problemática da Investigação do Cibercrime*, Faculdade de Direito, IDPCC, Lisboa, novembro 2010, p.20.

⁵⁷⁴ É importante salientar que mesmo encontrando os “dados de tráfego, estes são insuficientes como prova, 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”. Dias, Vera, *A Problemática da Investigação do Cibercrime*, Faculdade de Direito, IDPCC, Lisboa, novembro 2010, p.20.

⁵⁷⁵ Para evitar que tal aconteça, “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 com a lei”. *Idem, Ibidem, apud.*, Casey, Eoghan, *Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet*, Academic Press, 2000, pp.226 e 227.

⁵⁷⁶ São cada vez os meios informáticos criados para realizar/transmitir este tipo de crime. De igual forma, são criadas novas técnicas para ocultar este tipo de crimes, como o chamado “*grooming*”. Trata-se de uma “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”. Dias, Vera, *A Problemática da Investigação do Cibercrime*, Faculdade de Direito, IDPCC, Lisboa, novembro 2010, p.19, *apud.* Salom, Juan Clotet, “Delito Informático y su Investigación”, *Delitos Contra y A Través de las Nuevas*

O carácter *transnacional* da *Cibercriminalidade* é outra das maiores dificuldades de atuação, já que nestes casos a cena do crime estende-se por todo o globo, tornando extremamente difícil descodificar onde ocorreu verdadeiramente o ataque e quem foi o seu infrator⁵⁷⁷. Em regra, os ataques informáticos são propositadamente praticados em diversos pontos e por vários agentes, o que envolve vários países e, consequentemente, diferentes jurisdições. Pelos mesmos motivos, este carácter transnacional dificulta também a *perseguição* destes agentes.

Por fim, temos a *punição*. Embora a União Europeia disponha de diplomas que regulem esta matéria, é ainda difícil coordenar os padrões legais de cada ordenamento jurídico. As normas criadas a nível europeu só podem ser eficazes se os Estados Membros possuírem meios capazes de as implementar. Para combater eficazmente a *Cibercriminalidade* é necessário que, tanto a nível europeu como a nível nacional sejam, adotados meios eficazes de cooperação.

Em Portugal, a competência quanto ao *Cibercrime* está dividida entre a Polícia Judiciária e o Ministério Público, sendo este último quem tem competência para decidir. No entanto, também temos casos em que o Órgão de Polícia Criminal (OPC) e o Juiz de Instrução Criminal (JIC) podem intervir nos casos mais graves, como por exemplo, escutas telefónicas. Esta repartição de poderes e de funções torna difícil a rápida atuação dos órgãos de segurança, já que estão dependentes de uma série de trâmites⁵⁷⁸. De igual

Tecnologías Cómo Reducir su Impunidad?, *Cuadernos de Derecho Judicial*, III, *Consejo General Del Poder Judicial*, Centro de Documentación Judicial, 2006 p.128.

⁵⁷⁷ Um dos recentes métodos usados para evitar a deteção dos “utilizadores é a “splitting technique”, que consiste na divisão de tarefas entre *cibercriminosos* de várias partes do globo, que são especialistas em determinada área”. Dias, Vera, *A Problemática da Investigação do Cibercrime*, Faculdade de Direito, IDPCC, Lisboa, novembro 2010, p.19.

⁵⁷⁸ Temos como exemplo, o caso das redes de contacto 24/7 (definidas pela Diretiva 2013/40/UE). Estas redes ou pontos de contacto encontram-se na Polícia Judiciária (por força da Lei do Cibercrime, artigo 21.º), mas quem é o titular da ação penal é o Ministério Público (como dispõe o artigo 263.º do Código de Processo Penal). Como pode a Polícia Judiciária efetivar as comunicações exigidas (por exemplo nos casos urgentes, em que o prazo máximo é de oito horas), com o horário de funcionamento dos tribunais? Em outros países, como por exemplo na Alemanha, a rede de contacto 24/7 funciona no seio do Ministério Público.

Apesar de na Europa as autoridades judiciais e policiais, a nível nacional, cooperarem estreitamente através da Europol, da Eurojust e de outras entidades europeias, bem como das redes de contacto 24/7 (redes de contato ativas 24 horas por dia e sete dias da semana), é ainda fundamental reforçar e clarificar as responsabilidades de cada um. As consultas efetuadas pela Comissão indicam que estas redes de contacto ainda não são utilizadas de forma otimizada (a nível nacional tem levantado alguns problemas não só nas relações Polícia Judiciária-Ministério Público, mas também entre estes e os prestadores de serviços, ISP). Nestes casos, as respostas a pedidos de identificação de um cliente de determinado IP, não dependem da Polícia Judiciária, nem do Ministério Público, mas sim dos prestadores de serviço (ISP). Contudo os prestadores de serviço têm-se negado a fornecer a identificação do cliente quando não estejam em causa crimes graves (artigo 2.º, n.º1, alínea g). Ramos, Armando R. Dias, *A novíssima Diretiva*

forma, existe uma dificuldade de coordenação entre autoridades administrativas, como, por exemplo, a ANACOM, quanto aos dados informáticos, o que dificulta ainda mais a obtenção de provas⁵⁷⁹. Todas estas dificuldades de coordenação tornam difícil a implementação de certas medidas de prevenção e investigação criminal, que podiam ajudar no combate à *Cibercriminalidade*, como, por exemplo, a monitorização de tráfego, interceção de comunicações eletrónicas e a atuação de agentes infiltrados.

Assim, “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”⁵⁸⁰, são ainda problemas recorrentes na investigação da *Cibercriminalidade*.

relativa ao cibercrime, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014, p.188 e 189.

⁵⁷⁹ “A prova digital não é igual à prova tradicional”, como tal, é fundamental “a sua rápida e precisa recolha, (...), devido ao seu carácter temporário e volátil, de modo a evitar a sua destruição”. Dias, Vera, *A Problemática da Investigação do Cibercrime*, Faculdade de Direito, IDPCC, Lisboa, novembro 2010, p.21.

⁵⁸⁰ *Idem*, *Op. Cit.*, p.18, *apud.*, EUROPOL, *High Tech Crimes Within The EU : Old Crimes New Tools, New Crimes New Tools*, [Em linha], Threat Assessment 2007, p. 24. <http://www.europol.europa.eu/publications/Serious Crime Overviews/HTCThreatAssessement2007.pdf> (consultado em 20.11.2014).

3.3. – Soluções/ Mecanismos de Defesa

Neste último ponto mencionamos algumas tentativas de resolução que poderão ajudar no combate à *Cibercriminalidade*.

Para além da própria evolução legislativa que é necessária, a investigação deste tipo de criminalidade por parte das autoridades nacionais terá de se adaptar à nova realidade, passando, assim, de uma atuação reativa para uma atuação baseada na *colaboração*, isto é, uma colaboração mais direta com entidades cujas funções possam consubstanciar um crime informático; *preventiva*, antecipando os possíveis ataques e as novas formas de os cometer; e *transnacional*, colaborando e analisando o que acontece nos restantes países.⁵⁸¹

No âmbito nacional interno, defendemos que a integração e colaboração dos órgãos de polícia especializados neste tipo de crimes com técnicos informáticos, tal como acontece em Inglaterra, será uma solução bastante favorável.⁵⁸²

Paralelamente, é necessário garantir um quadro legal estável e claro, isto é, que defina as competências de cada entidade, bem como uma maior cooperação interna/externa. Para combater esta limitação prática a solução passa por existir um reforço quanto à cooperação – facilidade de contacto e rapidez de resposta.

Para que haja um desenvolvimento de instrumentos específicos de luta contra o *Cibercrime*, é necessário que haja um reforço da cooperação operacional dos serviços de polícia, bem como um aumento de formação profissional neste âmbito a nível internacional.

Neste sentido, é importante realizar exercícios de simulação de incidentes informáticos a nível nacional e internacional, para treinar a cooperação entre os Estados Membros e o setor privado de forma mais abrangente e sistemática.⁵⁸³ Estes exercícios de simulação

⁵⁸¹ Silva, Vanessa Rossana Queiróz Nunes da, *A Fraude com Cartão Bancário em Portugal na Atualidade*, UAL - Universidade Autónoma de Lisboa, Relatório profissional apresentado para obtenção de grau de Mestre em Direito na Área de Ciências Jurídico-Criminais, Lisboa, março 2013, p. 55.

⁵⁸² *Idem, Ibidem*.

⁵⁸³ O primeiro exercício que envolveu os Estados Membros realizou-se em 2010 (*Cyber Europe 2010*) e um segundo exercício, que envolveu também o setor privado, teve lugar em outubro de 2012 (*Cyber Europe 2012*). E em novembro de 2011efetou-se um exercício de simulação União Europeia-Estados Unidos da América (*Cyber Atlantic 2011*). Para os próximos anos estão previstos novos exercícios, nomeadamente com parceiros internacionais.

devem ser transmitidos aos cidadãos através de colóquios, conferências de esclarecimento e sensibilização para as novas tecnologias e para os riscos atuais.

Por fim, devem ser criados sítios eletrónicos disponíveis nos vários idiomas de cada Estado, contendo todo o material necessário que informe e ajude os cidadãos na luta contra a *Cibercriminalidade*: “Assegurar a cibersegurança é uma responsabilidade comum. Os utilizadores finais desempenham um papel crucial na garantia da segurança das redes e dos sistemas informáticos: é preciso que conheçam os riscos que enfrentam em linha e que tenham capacidade para tomarem medidas simples para os prevenir”.⁵⁸⁴

⁵⁸⁴ (JOIN (2013) 1 final), *Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013, p.8.

Conclusão

Em 1969, quando o governo norte-americano criou a *Internet* para fins militares, nada fazia prever a dimensão à escala mundial e as características que esta viria a alcançar.

Foi, sem dúvida, a invenção da ferramenta *World Wide Web* que veio sedimentar a grandeza da *Internet*: a capacidade de armazenar e partilhar ficheiros com computadores e pessoas de todo o mundo, bem como a possibilidade de obter informação em formato digital, de forma rápida, simples e acessível a todos, em qualquer parte. E foram essas mesmas competências que contribuíram para a massificação da *Internet* que hoje conhecemos.

Mais de 40 anos depois da criação da *Internet*, vivemos na chamada “Era Digital”, caracterizada pelo aumento e rapidez dos pontos de ligação à *Internet*; pelo aumento de dispositivos tecnológicos capazes de se ligarem à *Internet*; e pelas inúmeras evoluções tecnológicas nas mais variadas áreas: Medicina, Educação, Biologia, Direito, entre outras.

Paralelamente a estas evoluções positivas, a *Internet* trouxe também graves problemas à sociedade atual. E é no âmbito do Direito que essas dificuldades são mais perceptíveis.

À medida que a *Internet* foi evoluindo, certos utilizadores aperceberam-se das inúmeras oportunidades criminosas que a rede digital possibilitava cometer, nomeadamente, novas formas de obter lucro com o mínimo de risco. Face aos crimes realizados com recurso aos computadores e à *Internet*, foi adotado o conceito de *Cibercrime*. Como vimos, são: os crimes praticados com recurso ou por intermédio de tecnologias da informação, processamento e comunicação.

Dado o aumento deste tipo de crime, foi adotado o conceito de *Cibercriminalidade*: um conceito mais amplo, que pode ter várias interpretações doutrinárias, mas que fundamentalmente é utilizado para definir dois grandes grupos de crimes:

- Primeiro, os crimes ditos do mundo “real”, por exemplo: fraude, falsificação e roubo de identidade, pedofilia e distribuição de material pedo-pornográfico, mas que são praticados através do computador e da *Internet*.
- Segundo, graças ao aparecimento das novas tecnologias surgiram os crimes que têm como objeto o próprio computador e os seus inúmeros componentes

técnicos, tais como: os crimes relacionados com *software* e as redes *Intranet* ou *Internet*.

A *Cibercriminalidade* é atualmente uma das formas mais lucrativas e de menor risco praticadas pelos agentes, já que graças às suas características tornam difícil a atuação por parte das forças de segurança, nomeadamente, quanto à prevenção, investigação, perseguição, comprovação e punição.

Como vimos ao longo deste estudo, são várias as dificuldades apontadas para o combate à *Cibercriminalidade*. Algumas destas dificuldades estão diretamente ligadas com as suas próprias características, isto é, a *transnacionalidade*, *generalidade* e *imprevisibilidade*. São, portanto, crimes inesperados que podem ser cometidos a qualquer momento; que podem ser dirigidos a vários utilizadores, desde utilizadores particulares a empresas, ou entidades e órgãos do Estado; e podem ser praticados por agentes situados em qualquer parte do mundo. E é exatamente este último ponto que mais tem preocupado os Estados em geral. As ações repressivas contra estes crimes são extremamente difíceis, já que os seus autores se encontram, na grande maioria, em países diferentes do país alvo do ataque e, como tal, fora das suas jurisdições.

Este é um tipo de crime que diariamente vitima milhões de pessoas por todo o mundo. Como revelam dados estatísticos, todos os dias mais de um milhão de pessoas são vítimas de *Cibercriminalidade*.

Em face do nosso estudo, concluímos que este será um tipo de crime que tenderá a aumentar. Com o aumento da população e consequente aumento dos dispositivos ligados à *Internet* estima-se que, futuramente, estes ataques tecnológicos afetem ainda mais utilizadores, sejam mais perigosos e mais avançados, dificultando consideravelmente a atuação das entidades no combate a este fenómeno.

Com este estudo, concluímos, também, que as características dos *cibercriminosos* mudaram. Se no início dos anos 70 e 80 o criminoso informático podia ser definido como alguém especialista em computadores e sistemas informáticos, atualmente, graças às facilidades de acesso aos meios tecnológicos e à fácil compreensão dos mesmos, qualquer pessoa pode ser considerada “um cibercriminoso”, não havendo uma característica que defina especificamente estes agentes. A este propósito contribui o carácter anónimo que a *Internet* possibilita.

A verdade é que os *cibercriminosos* utilizam métodos cada vez mais sofisticados para se introduzirem nos sistemas informáticos, desviarem dados críticos ou exigirem resgates às empresas. O aumento da espionagem política e económica, e de atividades patrocinadas pelos Estados no mundo digital, coloca os governos e as empresas à mercê de uma nova categoria de ameaças.

A grande problemática da *Cibercriminalidade* e dos crimes que esta comporta baseia-se, essencialmente, no seguinte ponto: quando praticados em grande escala podem provocar prejuízos económicos substanciais, quer através da interrupção de sistemas de informação e comunicação, quer através da perda ou alteração de informações comerciais, confidenciais e importantes ou de outros dados presentes nas várias bases de dados existentes.

De igual forma, surgem programas malignos com características cada vez mais complexas (tais como as *botnets*) que, juntamente com os embustes informáticos tecnologicamente mais avançados e a denominada “*sextortion*” de menores, dificultam cada vez mais o papel dos órgãos de defesa internacional e nacional. Importa salientar que só em 2011 foram identificados 273 casos de suspeitos de abuso sexual infantil *online*, onde apenas 113 desses suspeitos, espalhados por vários países, foram presos. E estes são números que tenderão a crescer, se não forem adotadas as medidas necessárias.

Existe uma grande preocupação por parte dos utilizadores e das empresas em relação aos ataques informáticos. O perigo de ter contas bancárias invadidas, ser vítima de um furto de identidade ou de um vírus informático, é cada vez maior e pode originar graves prejuízos. Num mundo interligado, será difícil não receber mensagens de correio eletrónico que estejam infetados, por exemplo. No caso das grandes empresas, esta preocupação diz respeito à segurança das informações secretas e das bases de dados de que dispõem.

À medida que o mundo digital avança para uma sociedade ligada e interconectada pela *Internet*, é difícil imaginar um crime que não esteja ligado à *Internet*, ou cujas provas não dependam diretamente desta. Tais acontecimentos requerem um olhar atento por parte de todos os Estados e uma mudança fundamental na atuação do Direito, desde a recolha e análise de provas, até aos mecanismos de cooperação internacionais ligados ao crime.

Obviamente que a segurança virtual também cresce e se desenvolve a cada dia, tentando acompanhar o lado crimínógeno das tecnologias. Assim, são várias as empresas de *software* especializado que diariamente criam novos e avançados mecanismos de defesa como forma de dirimir estes ataques e proteger os utilizadores e os seus equipamentos.

Para atenuar estes ataques e o impacto que a *Cibercriminalidade* tem na nossa sociedade, é urgente uma atuação conjunta dos vários Estados com as várias organizações da União Europeia e, igualmente, com as organizações e empresas internacionais. É fundamental que empresas como a *Google* e *Facebook* (pelas suas características e reconhecimento junto da sociedade) dêem o primeiro passo e colaborem com entidades como o *EC3/Europol* no combate a este tipo de crimes.

É também essencial que as medidas legislativas adotadas pela União Europeia sejam cumpridas (sem exceções) pelos Estados Membros; que sejam adotadas mais estratégias de cooperação internacional neste âmbito, onde as grandes nações como os Estados Unidos da América, a Rússia, a China, entre outras, possam cooperar. Como procurámos demonstrar, a legislação sobre este tema continua a ser insuficiente face aos novos desenvolvimentos tecnológicos e, conseqüentemente, face às novas formas de crime.

Concluimos, igualmente, que é necessário informar a população das mudanças tecnológicas que sofremos, os perigos que estas acarretam e o que podemos ou o que está a ser feito para nos proteger. Como podemos constatar ao longo deste estudo, uma boa parte dos utilizadores ainda não sabe os perigos que corre quando “navega” na *Internet*, por exemplo: quando utiliza o cartão de crédito para fazer uma compra *online*, ou quando atualiza os seus dados pessoais. Na maioria dos casos, o próprio utilizador nem se apercebe que foi vítima de um ataque desta natureza.

A nível nacional, denotamos que ainda não há consciência da dimensão que pode atingir o *Cibercrime*, do que pode acontecer, nem de como combater este fenómeno. É certo que o nível de *Cibercriminalidade* em Portugal é muito inferior quando comparado com grandes Estados do mundo, como os Estados Unidos da América, a Rússia ou a China, por exemplo.

É por isso cada vez mais importante a literacia informática em todas as camadas populacionais e a todos os níveis, desde o manejo dos utensílios, à seleção da

informação, passando pela compreensão das infraestruturas que a suportam. Só assim será possível tornar a sociedade em que vivemos, numa sociedade mais consciente e mais tecnologicamente preparada para os perigos que advêm das novas tecnologias.

Como refere Vicente Freire, “Dos governos, ou, em sentido mais amplo, do Estado espera-se que garantam⁵⁸⁵ uma rede segura, que disponha de capacidade de resposta aos incidentes, que garanta o ambiente e as condições de formação e investigação para melhoria da segurança no ciberespaço e que adote a colaboração internacional também como veículo e plataforma de resolução de problemas. Por outro lado, tem de consciencializar o público em geral da dimensão do problema e da responsabilidade individualizada de cidadãos e empresas e, também, garantir que haja desenvolvimento da lei no sentido de acompanhamento continuado da realidade do ciberespaço, em especial no que respeita aos ilícitos.”⁵⁸⁶

Concluindo, destacamos três pontos fundamentais no combate à Cibercriminalidade:

- Sensibilização dos utilizadores face aos novos fenómenos informáticos (proteção, perigos e meios de defesa).
- Colaboração nacional/internacional, e cooperação entre entidades governamentais e grandes empresas ligadas às novas tecnologias, como *Google* e *Facebook*.
- Formação especializada para acompanhar os desenvolvimentos tecnológicos e estar a par das novas ameaças. Neste âmbito é fundamental uma aposta constante na formação dos profissionais que diariamente lidam com estes ataques.

Mais difícil de solucionar será o enquadramento jurídico do *Cibercrime*. Como verificámos, as leis são tradicionalmente criadas para a proteção de objetos materiais e não de objetos imateriais, como os dados e informações digitais. Mas também, sobre este assunto, a Doutrina divide-se. Alguns autores defendem que este crime pode ser combatido analogamente através dos instrumentos penais tradicionais, enquanto outros autores defendem a adoção de novos instrumentos penais mais tecnológicos. Em nossa

⁵⁸⁵ Não se enumera tudo o que se espera mas apenas alguns fatores-chave.

⁵⁸⁶ Freire, Vicente, *Cibersegurança e Ciberdefesa: A Inevitabilidade de adoção de uma estratégia nacional*, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012, p.56.

opinião, a ausência de legislação especificamente tecnológica constitui uma grave lacuna.

Com esta dissertação esperamos ter conseguido dar um singelo contributo para as investigações que começam já a ser feitas e que ela seja um ponto de partida para novas reflexões, já que, nesta matéria, há um longo caminho a percorrer, quer pela doutrina quer pela jurisprudência.

Bibliografia

- 12.º Congresso de Prevenção do Crime e Justiça Criminal, [Em linha], Salvador (Brasil), 12 a 19 de abril de 2010, relatório elaborado pelo Secretariado. Disponível em http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf (consultado em 17.2.2015).
- Akdeniz, Yaman; Walker, Clive; Wall, David, *The Internet, Law and Society*, Longman, Pearson Education, 2000. ISBN: 0-582-35656-3.
- Almeida, Ana Tomás de, Psicóloga, entrevista [Em linha]. Disponível em <http://pplware.sapo.pt/informacao/cyberbullying-o-que-como-combater/>. (última consulta 2.11.2015).
- Almeida, Reginaldo Rodrigues de, *Sociedade Bit, Da Sociedade da Informação à Sociedade do Conhecimento*, 2ª ed., Quid Juris? Sociedade Editora, Lisboa, Setembro, 2004. ISBN: 972-724-220-0.
- Anastácio, Gonçalo, Porto, Manuel Lopes, *Tratado de Lisboa – Anotado e Comentado*, Direito da União Europeia, Almedina, 2012. ISBN: 978-972-404-613-6.
- Andrade, Miguel Almeida, *Nomes de Domínio na Internet, A Regulamentação dos Nomes de Domínio sob. PT*, CENTROATLANTICO.PT, Portugal, 2004.
- Ascensão, José de Oliveira, *Criminalidade Informática*, Direito da Sociedade da Informação, Coimbra: Coimbra Editora, 2001. ISBN: 972-32-0915-2.
- Ascensão, José de Oliveira, *Criminalidade Informática*, Direito da Sociedade da Informação, vol. II, Coimbra: Coimbra Editora, 2001. ISBN: 978-972-32-0994-5.
- Ascensão, José de Oliveira, *O Cibercrime*, in Direito Penal Económico e Financeiro, *Conferências do Curso Pós-Graduado de Aperfeiçoamento*, Coimbra Editora, 1ª edição, Agosto, 2012. ISBN: 978-972-32-2073-5.
- Astier, Stéphane, *Rumeurs sur internet*, in *legalis.net*, Jun.2005, 2.
- “Ataques informáticos bancos deixam especialistas em segurança em alerta máximo”, [Em linha], *Observador*. Disponível em <http://observador.pt/2014/08/31ataques-informaticos-bancos-deixam-especialistas-em-seguranca-em-alerta-maximo/> (consultado em 15.10. 2014).

- Augusto, Mário, *As Nações Unidas no Contexto do Direito Internacional*, Estudos e documentos, Novo Imbondeiro, Lisboa, 2004. ISBN: 972-8102-46-1.
- Australian Government, *Cyber Security Strategy*, Commonwealth of Australia, 2009. ISBN: 978-1-921241-99-4.
- “Autoridade da Concorrência”, *Revista de Concorrência e Regulação*, Instituto de Direito Económico Financeiro e Fiscal da Faculdade de Direito da Universidade de Lisboa, Ano IV, n.º 14/15, Abril/Setembro 2013. ISBN: 978-14-000-5801-3.
- Baran Nicholas, *Desvendando a superestrada da informação*, Editora Campus, 1995.
- Bauche, Gilles, *Tout savoir sur Internet*, Arléa, 1996.
- Bravo, Rogério, *Criminalidade Informática realidade portuguesa de 1992 a 1998*, [Em linha], Ciberjus, Lisboa, 1998. Disponível em <http://www.ciberjus.net/revista/criminalidade-informatica.htm> (última consulta 2.11.2015).
- Bravo, Rogério, *O Crime de Acesso Ilegítimo na Lei da Criminalidade Informática e na Ciberconvenção*, [Em linha], Direito na Rede n.º1, Ordem dos Advogados, Lisboa, 2004. Disponível em [http://www.academia.edu/2039178/O_Crime_de_Acesso_Ilegitimo_na_Lei_da_Criminalidade Informa tica e na CiberConvencao](http://www.academia.edu/2039178/O_Crime_de_Acesso_Ilegitimo_na_Lei_da_Criminalidade_Informatica_e_na_CiberConvencao) (última consulta 2.11.2015).
- Casey, Eoghan, *Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet*, Academic Press, 2000.
- Castells, Manuel, *A Galáxia Internet, Reflexões sobre Internet, Negócios e Sociedade*, 2004.
- Castro, Catarina Sarmiento e, “Proteção de Dados Pessoais na Internet”, in Gonçalves, Maria Eduarda, *Internet, Direito e Tribunais, Sub Judice, Justiça e Sociedade*, revista trimestral n.º35, Almedina, Setembro 2006.
- “Cibercrime global dominado por 50 grupos”, Estudo da *CrowdStrike*, [Em linha]. Disponível em <http://www.computerworld.com.pt/2014/01/23/cibercrime-global-dominado-por-50-grupos/>. (última consulta em 2.11.2015).

- “Cibercrime pode tornar-se tão perigoso como grupos terroristas”, [Em linha], *Visão*. Disponível em <http://visao.sapo.pt/fbi-cibercrime-pode-tornar-se-ao-perigoso-como-grupos-terroristas=f650033>. (última consulta em 2.10.2015)
- Clough, Jonathan, *Principles of Cybercrime*, Cambridge University Press, Cambridge, 2010.
- Código do Direito de Autor e dos Direitos Conexos, aprovado pelo Decreto-Lei n.º63/85, de 14 de março, e alterado pelas Leis n.ºs45/85, de 17 de setembro, e 114/91, de 3 de setembro, Decretos-Lei n.ºs332/97 e 334/97, ambos de 27 de novembro, e pelas Leis n.ºs50/2004, de 24 de agosto, 24/2006, de 30 de junho, e 16/2008, de 1 de abril.
- Código Penal e Legislação Complementar, de acordo com as Leis 32/2010, de 2 de setembro, e 40/2010, de 3 de setembro, 4.ª ed. (Actualizada e Aumentada), Coleção Códigos Quid Juris Sociedade Editora. ISBN:978-972-724-526-0.
- Código Penal, Textos da Lei, 5.ª ed., Almedina, 2015. ISBN: 978-972-406-091-0.
- Código de Processo Penal, *Direito Processual*, Almedina, 2014. ISBN: 978-972-405-122-2.
- Colin, Barry, *The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge*, [Em linha], 1996. Disponível em <http://www.cjimagazine.com/archives/cji4c18.html?id=415> (última consulta em 2.11.2015).
- “Comentário de Cecilia Malmström no âmbito do inquérito do Eurobarómetro”, [Em linha]. Disponível em http://europa.eu/rapid/press-release_IP-14-129_pt.htm (última consulta em 2.11.2015).
- Conceição, Ana Raquel, *Escutas Telefónicas, Regime Processual Penal*, Quid Juris, 2009.
- Cordeiro, Raul, “Ataques de DDoS, Medidas Preventivas”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012.
- Correa, Carlos M. (et. al.), *Derecho informático*, Depalma, Buenos Aires, 1987.
- Costa, A. M. Almeida, *Comentário Conimbricense do Código Penal*, Tomo II, Coimbra Editora, 1999.

- Costa, José de Faria, Moniz, Helena, *Algumas reflexões sobre a criminalidade informática em Portugal*, Boletim da Faculdade de Direito, Coimbra, Vol.73, 1997.
- Cyber Security Strategy, Commonwealth of Australia, 2009, [Em linha]. Disponível em <https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf> (última consulta em 3.11.2015).
- Davin, João, *A Criminalidade Organizada Transnacional, A Cooperação Judiciária e Policial na UE*, 2.^a edição revista e aumentada, Almedina, Novembro 2007. ISBN:978-972-40-3256-6.
- Denning, Dorothy, *Cyberterrorism, Testimony before the Special Oversight Panel of Terrorism Committee on Armed Services*, US House of Representatives, 23 May 2000.
- “Despedimento lícito por Comentários no Facebook”, OA – *Boletim da Ordem dos Advogados*, n.º 111, fevereiro 2014, p.16.
- Dias, Vera, *A Problemática da Investigação do Cibercrime*, Faculdade de Direito, IDPCC, Lisboa, 2010.
- “Do Centro de Competências em Cibersegurança e Privacidade da Universidade do Porto”, *Jornal Metro*, 5 de junho 2014, p. 15.
- Dufour, Arnaud, *A Internet*, Publicações Europa-América, Coleção “Saber”, n.º235, 1997.
- Eight United Nations Congress on the Prevention of Crime and the Treatment of Offenders, [Em linha], Nova Iorque, 1991. Disponível em https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf
- Eksted, V./Parkhouse, T./Clemente, D., *Commitments, mechanisms & governance*, 2012, in Ed. Klimburg, A., *NATO National Cyber Security Framework Manual*.
- Eng. Santos, Lino, FCCN/ CERT.PT, *Apresentação em ação de formação no Centro de Estudos Judiciários*.

- Entrevista a Rogério Bravo, Inspetor-Chefe, Polícia Judiciária de Lisboa, no dia 18 de fevereiro de 2014.
- Entrevista realizada a Reginaldo Rodrigues de Almeida, no dia 19 de maio de 2014.
- Esteves, Pedro, “Hacktivismo, Transpondo a Fronteira entre a Liberdade de Expressão e o Cibercrime”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012.
- Estonia Ministry of Defence, Cyber Security Strategy, 2008. Tallinn: *Cyber Security Strategy Committee*; e Wilson, C., *CRS Report for Congress, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Police Issues for Congress*, January 2008.
- Estudo Financial Times, [Em linha]. Disponível em <http://observador.pt/2014/08/31ataques-informaticos-bancos-deixam-especialistas-em-seguranca-em-alerta-maximo/>. (Consultado em 15.10.2014).
- Eucrim, *THE EUROPEAN CRIMINAL LAW ASSOCIATION’S FORUM*, 2014/4. Focus: EU Criminal Policy. Dossier particulier : Politique de droit pénal de l’UE. Schwerpunktthema : EU-Strafrechtspolitik. Max Planck Society for the Advancement of Science c/o Max Planck Institute for Foreign and International Criminal Law, Germany, 2015.
- European Commission Memo, [Em linha], Brussels, 9 January 2012. Disponível em [http://europa.eu/rapid/press-release MEMO-13-6 en.htm](http://europa.eu/rapid/press-release_MEMO-13-6_en.htm) (última consulta em 2.10.2015)
- EUROPOL, *High Tech Crimes Within the EU: Old Crimes New Tools, New Crimes New Tools, Threat Assessment 2007*, [Em linha], High Tech Crime Centre, 2007. Disponível em http://www.europol.europa.eu/publications/Serious_Crime_Overviews/HTCThreatAssesment2007.pdf. (consultado em 20.11.2014).
- “Europol lança grupo internacional contra cibercrime”, [Em linha], *Computerworld*. Disponível em <http://www.computerworld.com.pt/2014/09/01/europol-lanca-grupo-internacional-contra-cibercrime/>, (consultado em 15.12.2014).
- Evans, Dave, *A Internet das Coisas, como a próxima evolução da Internet está mudando tudo*, Cisco Internet Business Solutions Group (IBSG), abril 2011.

- Facon, I., *Les relations stratégiques Chine-Russie en 2005 : la réactivation d'une amitié pragmatique*, Fondation pour la Recherche Stratégique, 2006.
- “Feasibility Study for a European Cybercrime Centre”, Relatório Final, fevereiro de 2012.
- Ferdinand, Peter, *Sunset, sunrise: China and Russia construct a new relationship*, International Affairs, 2007.
- Fernandes, José Pedro Teixeira, “Utopia, Liberdade e Soberania no Ciberespaço”, in *idn Nação e Defesa, Instituto de Defesa Nacional, Cibersegurança*, Revista Quadrimestral, n.º133.
- Fiss, Owen, “In search of a new paradigm”, in *The Yale Law Journal*, vol. 104, n.º 7, maio, 1995.
- Franco, Alberto Silva, *O difícil processo de tipificação*, Boletim do Instituto Brasileiro de Ciências Criminais, n.º21, p.5 citado de Lavoretti, Wilson e Silva, José Geraldo, in *Crime Organizado na Atualidade*, Campinas – SP, Bookseller, 2000.
- Freire, Vicente, “Cibersegurança e Ciberdefesa: A Inevitabilidade de adoção de uma estratégia nacional”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012.
- Gabinete Cybercrime, Colóquio: *As crianças e a Internet, uso seguro, abuso e denúncia*, Procuradoria-Geral da República, 4 de outubro de 2013, Conclusões, ponto 2.
- Gandelman, Henrique, *De Gutenberg à Internet: direitos autorais na era digital*.
- Gates, Bill, *A Estrada do Futuro*. Editora: Cia das Letras, 1995.
- Geers, Keneth, *Strategic Cyber Security*, NATO Cooperative Cyber Defence Centre of Excellence, 2011.
- Gelbstein, Eduardo, “The War of Attrition in Cyber-Space or “Cyber-Attacks”, “Cyber-War” and “Cyber-Terrorism”, in “Conselho de Segurança da ONU”, *idn Nação e Defesa, Instituto de Defesa Nacional*, n.º135.
- Gerald, Ana Vaz, “Ciberterrorismo : cenário de materialização”, in *Revista da Faculdade de Direito da Universidade de Lisboa, Coimbra*, v.53 n.º1-2, 2012.
- Gomes, Mário M. Vargues, *O Código da Privacidade e da Protecção de Dados Pessoais na Lei e na Jurisprudência (Nacional e Internacional)*, Colecção

- direito das novas tecnologias, CENTROATLANTICO.PT, Portugal, 2006, ISBN: 989-615-022-2.
- Gonçalves, Maria Eduarda, *Direito da Informação*, Almedina, Coimbra, 1994. ISBN: 972-40-0810-x.
 - Gonçalves, Maria Eduarda, “Internet, Direito e Tribunais”, *Sub Judice, Justiça e Sociedade*, revista trimestral n.º35, Almedina, Setembro 2006.
 - Gouveia, Jorge Bacelar, *Legislação de Direito Constitucional*, 2.ª ed., Coimbra Editora, 2007. ISBN: 978-972-32-1538-0.
 - Gurnsey, John, *Copyright Theft*, Aslib Gower, Hampshire, 1995.
 - Hanneman, Henri W., *The patentability of computer software*, Kluwer Law and Taxation Publishers, Deventer, Holanda, 1985.
 - Henriques, Miguel Gorjão- (organização), *Tratado de Lisboa*, Direito da União Europeia, 6.ª ed., Almedina, 2015. ISBN:978-972-406-165-8.
 - IOCTA, *The Internet Organised Crime Threat Assessment 2015*, [Em linha]. Disponível em <https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015> (última consulta em 2.11.2015).
 - Janczewski, L./Andrew, M.C., *Cyberwarfare and Cyberterrorism*, USA/UK: IGI.
 - Judge Schjolberg, Stein, *A presentation at the Europol – INTERPOL Cybercrime Conference*, The Hague, The Netherlands, September 24-25, 2013, p.8.
 - Junqueiro, Raul, *A Idade do Conhecimento, A Nova Era Digital*, Editorial Notícias, 2002. ISBN: 978-972-461-356-7.
 - Kamal, A., *The Law of Cyberspace an invitation to the table of negotiations*, United Nations Institute of Training and Research, October, 2005.
 - Lavorenti, Wilson e Silva, José Geraldo, in *Crime Organizado na Atualidade*, Campinas – SP, Bookseller, 2000.
 - Macedo, Miguel, “O Desafio da Cibersegurança”, in *Segurança e Defesa*, Revista Trimestral, n.º21, Maio-Agosto 2012.
 - Magalhães, José, *Homo S@piens, Cenas da Vida no Ciberespaço*, Quetzal Editores, Lisboa, 2001. ISBN: 972-564-508-1.

- Magnin, Cédric J., *The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?*, LLM dissertation, Santa Clara University, June 2001.
- Malmström, Cecilia, conferência “Defining Cyber Security”, Bruxelas, a 9 de novembro de 2011.
- Marques, Ana Margarida; Anjos, Mafalda; Vaz, Sónia Queiróz, *101 Perguntas e Respostas do Direito da Internet e da Informática*, CENTROATLANTICO.PT, Portugal, 2002, ISBN: 972-8426-50- X.
- Marques, Garcia, Martins, Lourenço, *Direito da Informática*, Lições de Direito da Comunicação, Almedina, Novembro, 2000. ISBN: 972-40-1399-5.
- Marques, Garcia, Martins, Lourenço, *Direito da Informática*, 2ª ed. Refundida e Actualizada, Almedina, Coimbra, 2006. ISBN: 972-40-2859-3.
- Mota, José Luís Lopes da, Vice-Presidente da Eurojust, *Seminário da Eurojust*, Lisboa, 20.04.2006.
- Nelson, Bill, et al., *Cyberterror, Prospects and Implications*, Center for the Study of Terrorism and Irregular Warfare, 1999.
- Neto, Arnaldo Sobrinho de Moraes, *Cibercrime e Cooperação Penal Internacional: um enfoque à luz da Convenção de Budapeste*, Universidade Federal de Paraíba – UFPB, João Pessoa, 2009.
- Nimmer, Raymond T., Krauthaus, Patricia A., *Computer Software: protection of authorship and technology*, in *Law and Computers, International Congress of the Italian Corte Suprema di Cassazione*, 4, Vol. II., 1998.
- Nora, Dominique, *Os conquistadores do ciberespaço*, tradução, colecção Actualidades, n.º4, Terramar, Lisboa, 1996.
- Nota prática n.º2/2013, 3 de abril de 2013, “A obtenção do endereço IP – súmula da jurisprudência recente”, Procuradoria-Geral da República – Gabinete Cibercrime.
- Nugent, J.H./Raisinghani, M., *Bites and Bytes vs. Bullets and Bombs: A New Form of Warfare*, in Janczewski, L. /Andrew, M.C., *Cyberwarfare and Cyberterrorism*, USA/UK: IGI.
- OCDE, Organização para a Cooperação e Desenvolvimento Económico, “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data”, 1980; “Recommendation Concerning Guidelines for the Security of

- Information Systems”, 1992; “Manual on the Prevention and Control of Computer-related Crime”, 1994.
- *Office of the National Counterintelligence Executive*, “Espiões estrangeiros roubam segredos económicos americanos no ciberespaço”, novembro 2011.
 - O’ Hara, T.F., *Cyber warfare/Cyber terrorism*, U.S. Army War College Strategic Research Project, 2004.
 - Organização para a Cooperação de Shangai, [Em linha]. Disponível em <http://mundorama.net/2013/12/04/a-organizacao-de-cooperacao-de-xangai-origens-e-missao-por-paulo-duarte/>, *apud.*, Ferdinand, Peter, Sunset, sunrise: China and Russia construct a new relationship, International Affairs, 2007.
 - Owen, R.S., *Infrastructures of Cyber Warfare*, 2007, in Janczewski, L. /Andrew, M.C., *Cyberwarfare and Cyberterrorism*, USA/UK: IGI.
 - Pereira, Joel Timóteo Ramos, *Direito da Internet e Comércio Electrónico*, Quid Juris?, Sociedade Editora, Lisboa, 2001. ISBN: 972-724-113-1.
 - Pereira, Joel Timóteo Ramos, *Compêndio Jurídico da Sociedade da Informação*, Quid Juris?, Sociedade Editora, Lisboa, Outubro, 2004. ISBN: 972-724-225-1.
 - Pereira, Júlio, “Cibersegurança, O Papel do Sistema de Informações da República Portuguesa”, in Segurança e Defesa, Revista Trimestral, n.º21, Maio-Agosto 2012.
 - Piette-Coudol Thierry/ Bertrand André, *Internet et la loi*, Dalloz, Collection Dalloz Service, Paris, 1997.
 - Pinto, Maria do Céu, *O Papel da ONU na Criação de uma Nova Ordem Mundial*, prefácio, 2010, ISBN: 978-989-652-050-2.
 - Raínha, Paula; Vaz, Sónia Queiróz, *Guia Jurídico da Internet em Portugal*, ed., CENTROATLANTICO.PT, Portugal, 2001. ISBN: 972-8426-35-6.
 - Ramalho, David Silva, “A Investigação Criminal na Dark Web”, in *Revista de concorrência e regulação*, Coimbra, a.4n.14-15, Abr.-Set.2013.
 - Ramos, Armando R. Dias, *A novíssima Diretiva relativa ao cibercrime*, in Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014. ISBN: 978-989-8191-61-8.
 - “Relatório Anual de 2001”, citado pelo *Diário Digital* de 15 de maio de 2002.

- *Revista da Faculdade de Direito da Universidade de Lisboa*, Vol. LIII, n.º1 e 2, Coimbra Editora, 2012. ISSN: 0870-3116.
- Reynolds, George W., *Ethics in Information Technology*, Third Edition, Course Editions, USA, 2010. ISBN: 13:978-0-538-74622-9.
- Rheingold, Howard, entrevista à *Revista “Pública”*, de 15 de janeiro de 2006.
- Rocha, Manuel Lopes, *Direito da Informática nos Tribunais Portugueses*, Coleção Direito das Novas Tecnologias, CENTROATLANTICO.PT. ISBN: 972842609-7.
- Rossi, Clóvis, *Do Conselho Editorial da Folha de São Paulo*, [Em linha], 2 de novembro de 1997. Disponível em http://www1.folha.uol.com.br/fsp/1997/11/02/caderno_especial/1.html (consultado em 23.11.2015).
- Rovira, Enrique Del Canto, *Delincuencia Informática y Fraudes Informáticos*, Estudios de Derecho Penal, 33 Editorial Comares, Granada, 2002.
- Saavedra, Rui, *A Proteção Jurídica do Software e a Internet*, Sociedade Portuguesa de Autores, Publicações Dom Quixote, Lisboa, 1998.
- Santos, Paulo, Bessa, Ricardo et.al, *CYBERWAR o fenómeno, as tecnologias e os actores*”, FCA, Editora de Informática, Lda, 2008.
- Scherer, Michael; Shuster, Simon, *Time Magazine*, Berlim, 2013, in *Visão*, 16 de dezembro de 2013.
- Seminário “PROTEUS: Furto de Identidade Online Prevenção, Combate & Apoio à Vítima”, Polícia Judiciária, 29/30.10.2015.
- Sieber, Ulrich, *Documentación para una aproximación al Delito Informático*, Delincuencia Informática, IURA, Barcenona, 1992.
 - *Criminalidad Informática: Peligro y Prevención*, Delincuencia Informática, IURA-7, PPU, Barcelona, 1998, (tradução Elena Farré Trepas).
 - *Straftaten und Strafverfolgung im Internet*, in *Gutachten des Deutschen Juristentags*, Munich: C.H. Beck, 2012.
- Silva, Libório, Remoaldo, Pedro, *Introdução à Internet*, 2.ª ed., Editorial Presença, Lisboa, 1996.
- Silva, Vanessa Rossana Queiróz Nunes da, *A Fraude com Cartão Bancário em Portugal na Atualidade*, UAL - Universidade Autónoma de Lisboa, Relatório

- profissional apresentado para obtenção de grau de Mestre em Direito na Área de Ciências Jurídico-Criminais, Lisboa, 2013.
- “Smartphones sob ataque dos hackers”, *Jornal Metro*, 23 de outubro de 2014, p. 4.
 - Sousa, Constança Urbano de, *O espaço de liberdade, segurança e justiça da UE: desenvolvimentos recentes*, Departamento de Direito, EDIUAL, Universidade Autónoma Editora, Maio 2014. ISBN: 978-989-8191-61-8.
 - Théry, Gérard, *Les autoroutes de l'information*, Collection des Rapports Officiels, La Documentation Française, Paris, 1994.
 - “United Nations Crime Commission to Address the Protection of Children from Exploitation on the Web”, [Em linha]. Disponível em <http://www.unis.unvienna.org/unis/pressrels/2011/uniscp645.html>. (última consulta em 2.11.2015).
 - UNODC, United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime*, Draft, February 2013, United Nation, New York, 2013.
 - UNODC, United Nations Office on Drugs and Crime, *Summary of the United Nations Convention against transnational organized crime and protocols thereto*. [Em linha]. Disponível em <https://www.unodc.org/unodc/treaties/CTOC/> (última consulta em 2.11.2015)
 - Veiga, Pedro; Dias, Marta, *A Governação da Internet*, [Em linha], JANUS.NET e-journal of International Relations, nº1, Outono 2010. Disponível em http://janus.ual.pt/janus.net/pt/arquivo_pt/pt_vol1_n1_pdf/pt_vol1_n1.pdf (última consulta em 2.11.2015).
 - Venâncio, Pedro Dias, *Lei do Cibercrime*, Anotada e Comentada, Coimbra Editora, grupo Wolters Kluwer, Portugal, 2010. ISBN: 978-972-32-1906-7.
 - Verdelho, Pedro, *A convenção sobre cibercrime do conselho da Europa: repercussões na Lei Portuguesa*, in *Direito da sociedade da informação*, Mello, Alberto de Sá e, (et. al), Coimbra: Coimbra Editora, 1999-2006. ISBN: 978-972-32-1411-3.
 - Verdelho, Pedro, *Apresentação em ação de formação no Centro de Estudos Judiciários*.
 - Verdelho, Pedro; Bravo, Rogério (et. al.), *Leis do Cibercrime*, Vol. I, CENTROATLANTICO.PT, Portugal, 2003. ISBN: 972-8426-69-0.

- Verdelho, Pedro, *Cibercrime*, in *Direito da Sociedade da Informação*, vol. IV, Associação Portuguesa do Direito Intelectual, Coimbra Editora, 2003. ISBN:972-32-1169-6.
 - *apud.*, Diário Digital de 4 de janeiro de 2002.
 - *apud.*, Diário de Notícias de 25 de junho de 2002.
- Verdelho, Pedro, “Cibercrime e Segurança Informática”, in *Polícia e Justiça*, Revista do Instituto Superior de Polícia Judiciária e Ciências Criminais, III Série, n.º6, Julho-Dezembro 2005.
- Viana, Vítor Rodrigues, “Cibersegurança”, *idn Nação e Defesa*, Instituto da Defesa Nacional, Revista Quadrimestral, n.º133.
- Visão Estratégica do Air Force Cyber Command.
- Walker, C., *Cyber terrorism: legal principle and law in the United Kingdom*, Center for Criminal Justice Studies, School of Law, University of Leeds, 2006.
- Weimann, Gabriel, *Cyberterrorism: The sun of all fears?*, 28 Studies in conflict and Terrorism 129.
- Wilson, C., CRS Report for Congress, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Police Issues for Congress*, January 2008.
- Workshop “A Prevenção e o combate à cibercriminalidade – A experiência nacional, europeia e internacional”, Direcção Geral de Política de Justiça, 21 de novembro de 2013.
- Y., Masuda, *The Information Society*, Tokyo: Institute for the Information Society, 1981.
- “YouTube para crianças”, *Jornal Metro*, 19 de março 2014, p. 7.

Legislação (Nacional e Internacional)

- Comissão Europeia, Comunicado de imprensa, de 30 de setembro de 2010, [Em linha]. Disponível em http://europa.eu/rapid/press-release_IP-10-1239_pt.htm, (consultado em 11.12.2014).
- Comissão Europeia, Comunicado de Imprensa, “Cibercriminalidade: cidadãos da UE preocupados com a segurança dos dados pessoais e dos pagamentos em linha”, [Em linha], Bruxelas, 9 de julho de 2012. Disponível em

http://europa.eu/rapid/press-release_IP-12-751_pt.htm?locale=pt (última consulta em 3.11.2015).

- Comissão Europeia, Comunicado de Imprensa, “Centro Europeu de Cibercriminalidade – um ano depois”, [Em linha], Bruxelas, 10.2.2014. Disponível em http://europa.eu/rapid/press-release_IP-14-129_pt.htm. (última consulta 3.11.2015).
- (COM (2000) 890 final), Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões, “Criar uma Sociedade da Informação mais segura reforçando a segurança das infraestruturas de informação e lutando contra a cibercriminalidade”, Bruxelas, 26.1.2001.
- (COM (2001) 298 final), Comunicação da Comissão ao Conselho, Parlamento Europeu, Comité Económico e Social e Comité das Regiões, “Segurança das redes e da informação: Proposta de abordagem de uma política europeia”, Bruxelas, 6.6.2001.
- (COM (2005) 229 final), Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões, “i2010 - Uma sociedade da informação europeia para o crescimento e o emprego”, [Em linha], Bruxelas, 1.6.2005. Disponível em <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:EN:PDF> (última consulta em 3.11.2015).
- (COM (2006) 251 final), Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões, “Estratégia para uma sociedade da informação segura – diálogos, parcerias e maior poder na intervenção”, [Em linha], Bruxelas, 31.5.2006. Disponível em <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52006DC0251&from=EN> (última consulta em 3.11.2015).
- (COM (2007) 267 final), Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões, “Rumo a uma Política geral de luta contra o Cibercrime”, Bruxelas, 22.5.2007.
- (COM (2008) 199 final), Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões: “Preparar o

futuro digital da Europa; revisão intermédia da iniciativa i2010”, [Em linha], Bruxelas, 17.4.2008. Disponível em

[http://eur-](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0199:FIN:ES:PDF)

[lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0199:FIN:ES:PDF](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0199:FIN:ES:PDF)

(última consulta em 3.11.2015).

- (COM (2009) 149 final), Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, relativa à “proteção das infraestruturas críticas da informação - Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência”, Bruxelas, 30.3.2009.
- (COM (2009) 277 final), Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada “Governo da Internet: as próximas etapas”, Bruxelas, 18.6.2009.
- (COM (2010) 2020 final), Comissão Europeia, Comunicado de Imprensa, Europa 2020 - Estratégia para um crescimento inteligente, sustentável e inclusivo, Bruxelas, 3.3.2010.
- (COM (2010) 245 final), Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, “Uma Agenda Digital para a Europa”, Bruxelas, 19.5.2010.
- (COM (2011) 681 final), Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, “Responsabilidade social das empresas: uma nova estratégia da EU para o período de 2011-2014”, [Em linha], Bruxelas, 25.10.2011. Disponível em [http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com\(2011\)0681_/com_com\(2011\)0681_pt.pdf](http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com(2011)0681_/com_com(2011)0681_pt.pdf) (última consulta em 3.11.2015).
- (COM (2012) 140 final), Comunicação da Comissão ao Conselho e ao Parlamento Europeu, “Luta contra a criminalidade na era digital: criação de um Centro Europeu da Cibercriminalidade”, Bruxelas, 28.3.2012.
- (JOIN (2013) 1 final), Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, “Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido”, Bruxelas, 7.2.2013.

- Conselho da União Europeia, Comunicado de Imprensa, 3010.^a reunião do Conselho, “Assuntos Gerais”, [Em linha], Luxemburgo, 26 de abril de 2010. (8967/10 (Presse 89)). Disponível em http://europa.eu/rapid/press-release_PRES-10-89_pt.htm (última consulta em 3.11.2015).
- Convenção da Liga dos Estados Árabes, [Em linha]. Disponível em <http://www.era-comm.eu/Cybercrime/library.html> (última consulta em 3.11.2015)
- Convenção das Nações Unidas contra o Tráfico Ilícito de Estupefacientes e Substâncias Psicotrópicas, Viena – Áustria, 20 de dezembro de 1988.
- Council of Europe, Cyberterrorism – the use of the Internet for terrorist purposes, [Em linha], 2007. Disponível em https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (última consulta em 3.11.2015).
- Decisão n.º 276/1999/CE do Parlamento Europeu e do Conselho, adota um plano de ação comunitário plurianual para fomentar uma utilização mais segura da internet através do combate aos conteúdos ilegais e lesivos nas redes mundiais, (JOUE L 162/1, de 1.7.2003).
- Decisão n.º 2000/375/JAI do Conselho, de 29 de maio de 2000, sobre o combate à pornografia infantil na Internet, (JOCE L 138, de 9.6.2000).
- Decisão n.º 2009/371/JAI do Conselho, de 6 de abril de 2009, que cria o Serviço Europeu de Polícia, (Europol), (JOUE L 121/37, de 15.5.2009).
- Decisão n.º 1151/2013/CE do Parlamento Europeu e do Conselho de 16 de junho de 2003, que altera a Decisão n.º 276/1999/CE que adota um plano de ação comunitário plurianual para fomentar uma utilização mais segura da internet através do combate aos conteúdos ilegais e lesivos nas redes sociais, (JOUE L 162/1, de 1.7.2003).
- Decisão-Quadro 2001/413/JAI do Conselho de 28 de maio de 2001, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, (JOCE L 149/1, de 2.6.2001).
- Decisão-Quadro 2004/68/JAI do Conselho, de 22 de dezembro de 2003, relativa à luta contra a exploração sexual de crianças e a pornografia infantil, (JOUE L 13/44, de 20.1.2004).

- Decisão-Quadro 2005/222/JAI do Conselho, de 24 de fevereiro, relativa a ataques contra os sistemas de informação, (JOUE L 69/67, de 16.3.2005).
- Decisão-Quadro 2008/841/JAI do Conselho, de 24 de outubro de 2008, relativa à luta contra a criminalidade organizada, (JOUE L 300/42, de 11.11.2008).
- Decisão-Quadro 2009/848/JAI do Conselho, de 30 de novembro de 2009, relativa à prevenção e resolução de conflitos de exercício de competência em processo penal, (JOUE L 328/42, de 15.12.2009).
- Decreto-Lei n.º252/94, de 20 de outubro, Diário da República, I Série A, n.º 243, de 20.10.1994, relativa à Proteção Jurídica dos Programas de Computador.
- Decreto-Lei n.º334/97 de 27 de novembro, Diário da República, I Série A, n.º275, 27.11.1997.
- Decreto-Lei n.º7/2004, de 7 de janeiro de 2004, relativo a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno, e que transpõe para o ordenamento jurídico português a Diretiva 2000/31/CE.
- Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. (JOCE L 281/31, de 23.11.95).
- Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade da informação, em especial do comércio eletrónico, no mercado interno (Diretiva sobre o comércio eletrónico). (JOCE L 178/1, de 17.7.2000).
- Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas). (JOCE L 201/37, de 31.7.2002).
- Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho. (JOUE L 335/1, de 17.12.2011).

- Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho. (JOUE L 218/8, de 14.8.2013).
- European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European Agenda on Security, Strasbourg, 28.4.2015. (COM (2015) 185 final).
- IP 10/1239, *Comissão Europeia*, “Comissão reforça as defesas da Europa contra os ataques informáticos”, [Em linha], Bruxelas, 30.9.2010, Disponível em http://europa.eu/rapid/press-release_IP-10-1239_pt.htm. (consultado em 15.10.2014).
- IP/12/317, Comissão Europeia, Comunicado de Imprensa, “Criar um Centro Europeu da Cibercriminalidade para combater o crime informático e defender os consumidores *online*”, Bruxelas, 28.3.2012.
- Legislação europeia sobre justiça, liberdade e segurança, [Em linha]. Disponível em http://eur-lex.europa.eu/search.html?OBSOLETE_LEGISUM=false&name=summary-eu-legislation:justice_freedom_security&qid=1446659006682&type=named&SUM_2_CODED=2308&SUM_1_CODED=23&SUM_3_CODED=230806 (última consulta em 3.11.2015).
- Lei n.º10/91, de 29 de abril de 1991, referente à Lei da Proteção de Dados Pessoais face à Informática, Diário da República, I Série A, n.º98, 29.4.1991, alterada pela Lei n.º28/94, de 29 de agosto.
- Lei n.º 109/91, de 17 de agosto, Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, Diário da República, I Série A, n.º188, de 17.8.1991.
- Lei n.º67/98, de 26 de outubro, referente à Lei da Proteção de Dados Pessoais e à Livre Circulação desses dados, transpõe para a ordem jurídica portuguesa a Diretiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de

- 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- Lei n.º 15/2001, de 5 de junho, reforça as garantias do contribuinte e a simplificação processual, reformula a organização judiciária tributária e estabelece um novo regime geral para as infrações tributárias, Diário da República, I Série A, n.º130, de 5.6.2001.
 - Lei n.º 16/2008, de 1 de abril, Transpõe para a ordem jurídica interna a Diretiva n.º 2004/48/CE, do Parlamento Europeu e do Conselho, de 29 de abril, relativa ao respeito dos direitos de propriedade intelectual, procedendo à terceira alteração ao Código da Propriedade Industrial, à sétima alteração ao Código do Direito de Autor e dos Direitos Conexos e à segunda alteração ao Decreto -Lei n.º 332/97, de 27 de novembro, Diário da República, 1.ª série, n.º64, de 1.4.2008.
 - Lei n.º109/2009, de 15 de setembro de 2009, Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão-Quadro n.º2005/222/JAI, do Conselho de 24 de fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa, Diário da República, 1.ª série, n.º179, de 15.9.2009.
 - Lei n.º82/2013, de 6 de dezembro, Transpõe a Diretiva n.º2011/77/UE do Parlamento Europeu e do Conselho, de 27 de setembro, relativa ao prazo de proteção do direito de autor e de certos direitos conexos, e altera o Código do Direito de Autor e dos Direitos Conexos, aprovado pelo Decreto-Lei n.º63/85, de 14 de março, Diário da República, 1.ª série, n.º237, 6.12.2013.
 - MEMO/12/221, Frequently Asked Questions: the new European Cybercrime Centre, [Em linha], Brussels, 28 march 2012. Disponível em http://europa.eu/rapid/press-release_MEMO-12-221_en.htm (última consulta em 3.11.2015).
 - MEMO/10/597, EU-U.S. Summit 20 november 2010, Lisbon – Joint Statement, [Em linha], Brussels, 20 november 2010. Disponível em http://europa.eu/rapid/press-release_MEMO-10-597_en.htm (última consulta em 3.11.2015).
 - MEMO 13/6, European Commission Memo, Frequently ask questions: The European Cybercrime Center EC3, [Em linha], Brussels, 9 january 2012.

Disponível em [http://europa.eu/rapid/press-release MEMO-13-6_en.htm](http://europa.eu/rapid/press-release_MEMO-13-6_en.htm).
(consultado em 17.12.2014).

- Protocolo Adicional relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, Estrasburgo, 28 de janeiro de 2003. Resolução da Assembleia da República n.º 91/2009 e ratificado pelo Decreto do Presidente da República n.º 94/2009, Diário da República, 1.^a série, n.º 179, de 15 de setembro de 2009.
- Recomendação R(89) 9, sobre a criminalidade informática que estabelece diretrizes para os legisladores nacionais respeitantes à definição de certos crimes informáticos.
- Recomendação R(95) 13, relativa a problemas da lei processual penal ligados às tecnologias da informação, 19 de maio de 1997, (JOCE C 150).
- Recomendação 3/99, relativa à conservação dos dados referentes ao tráfego, por parte dos fornecedores de serviços Internet, para efeitos de aplicação da lei, 7.9.1999, (5085/99/PT/FINAL).
- 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.
- Regulamento (CE) n.º 1007/2008 do Parlamento Europeu e do Conselho de 24 de setembro de 2008, altera o Regulamento n.º 460/2004, que cria a Agência Europeia para a Segurança das Redes e da Informação, no que respeita à duração da Agência.
- Resolução n.º 45/121, de 14 de dezembro de 1990, [Em linha]. Disponível em <http://www.un.org/documents/ga/res/45/a45r121.htm> (última consulta em 3.11.2015).
- Resolução n.º 55/63, de 4 de dezembro de 2001, [Em linha]. Disponível em http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf (última consulta em 3.11.2015).
- Resolução n.º 56/121, de 23 de janeiro de 2002, [Em linha]. Disponível em http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf (última consulta em 3.11.2015)
- Resolução n.º 65/230, da Assembleia Geral das Nações Unidas, de 21 de dezembro de 2010, [Em linha] Criação de um grupo intergovernamental aberto

de peritos em matéria de cibercrime, junto do GDC (Gabinete para a Droga e a Criminalidade). Disponível em

<http://register.consilium.europa.eu/doc/srv?f=ST+12109+2013+INIT&l=pt>, p.5 (última consulta em 5.11.2015).

- Resolução 2007/068/01 do Conselho, relativa a segurança e à resiliência das infraestruturas das Tecnologias da Informação e das Comunicações.
- Resolução da Assembleia Geral das Nações Unidas n.º 64/221, de 21 de dezembro de 2009, [Em linha], sobre cibersegurança. Disponível em http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/64/211 (última consulta em 3.11.2015).
- Resolução da Assembleia da República n.º23/89, Convenção Europeia de Extradução, Diário da República, I Série A, n.º191, de 21.8.1989.
- Resolução da Assembleia da República n.º 88/2009, Diário da República, 1.ª série - n.º 179 - 15 de setembro de 2009, [Em linha]. Disponível em <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> (última consulta em 3.11.2015).
- Resolução do Conselho de Ministros, de 7 de fevereiro de 2012, em que o Governo aprovou um Plano de Racionalização das Tecnologias de Informação e Comunicação na Administração Pública (RCM n.º12/2012).
- US National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23), [Em linha]. Disponível em <https://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative> (última consulta em 3.11.2015).

Jurisprudência (Nacional e Internacional)

- Acórdão de 20 de outubro de 2010, [Em linha], processo n.º 78/07.6JAFAR.E2.S1, 3.ª Secção, STJ, Lisboa 20-10-2010. Disponível em <http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/50feedd7db6f406a80257885004d09e0?OpenDocument> (última consulta em 2.11.2015).
- Judgement of the German Bundesgerichtshof of 1 December 2000 (1 StR 184/00, BGH MMR 2001, pp.228 et seqq.)

- Parecer n.º13/96 do Conselho Consultivo da Procuradoria Geral da República, publicado no DR, II, n.º286, de 12.12.97, p.15247 ss.
- Parecer 4/2001, relativo ao Projeto de Convenção do Conselho da Europa sobre Cibercriminalidade, 22.3.2001, Bruxelas, p.2.
- Tribunal de Grande Instância de Paris, em Sentença de 14 de agosto de 1996, publicada com anotação de F. Olivier/ F. Barbry, em La Semaine Juridique, edição geral, Juris-Classeur Périodique, 1996, II, n.º22727, pp.441 e ss.
- Tribunal de Primeira Instância de Bruxelas, em Sentença de 16-10-96, in Dalloz, Recueil, 26 de junho de 1997, n.º25, 1997, caderno jurisprudência, pp.322 e ss.

Documentos eletrónicos (Internet)

- Agência Efe, [Em linha]. Disponível em www.efe.com (última consulta em 2.11.2015).
- Antonio Forzieri, “EMEA Cyber Security conduit for confidence organization Symantec”, [Em linha]. Disponível em www.worldnewspaperonline.com. (última consulta em 2.11.2015).
- Atividades da União Europeia, [Em linha]. Disponível em http://europa.eu/publications/reports-booklets/general-report/index_pt.htm (última consulta em 2.11.2015).
- Conceito de Vishing e Smishing, [Em linha]. Disponível em <https://security.intuit.com/phishing.html> (última consulta em 3.11.2015).
- “Coreia do Norte formou 500 *hackers* para guerra com EUA”, [Em linha], Diário Digital de 7 de outubro de 2004. Disponível em www.diariodigital.sapo.pt/news.asp?section_id=18&id_news=142942 (última consulta em 3.11.2015).
- Council of Europe, Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime, [Em linha]. Disponível em <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG> (consultado em 17.02.2015).
- “Cyber Atlantic 2011”, [Em linha]. Disponível em <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis->

- [cooperation/cce/cyber-atlantic/cyber-atlantic-2011](https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011) (última consulta em 2.11.2015).
- “Cyber Europe 2010”, [Em linha]. Disponível em <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010/ce2010report> (última consulta em 2.11.2015).
 - “Cyber Europe 2012”, outubro de 2012, [Em linha]. Disponível em <http://www.anacom.pt/render.jsp?contentId=1139478#.VjfwotLhDDc> (última consulta em 2.11.2015).
 - “ENISA e Europol cooperam conta a cibercriminalidade”, 30.6.2014, [Em linha]. Disponível em <http://inteligenciaeconomica.com.pt/?p=22282>, (consultado em 15.12.2014).
 - Gabinete Nacional de Segurança, *Cyber Newsletter*, n.º 35/2014, [Em linha]. Disponível em <http://www.gns.gov.pt/new-ciberseguranca/newsletter.aspx> (consultado em 17.12.2014).
 - Gabinete Nacional de Segurança, *Cyber Newsletter*, n.º37/2014, 10 de outubro de 2014, [Em linha]. Disponível em <http://www.gns.gov.pt/new-ciberseguranca/newsletter.aspx> (última consulta em 3.11.2015).
 - Gabinete Nacional de Segurança, *Cyber Newsletter*, n.º38/2014, 17 de outubro de 2014, [Em linha]. Disponível em <http://www.gns.gov.pt/new-ciberseguranca/newsletter.aspx> (última consulta em 3.11.2015).
 - Gabinete Nacional de Segurança, *Cyber Newsletter*, n.º40/2014, 31 de outubro de 2014, [Em linha]. Disponível em <http://www.gns.gov.pt/new-ciberseguranca/newsletter.aspx> (última consulta em 3.11.2015).
 - Sítio oficial Hatewatch, [Em linha]. Disponível em <http://www.hatewatch.org>. (última consulta em 2.11.2015).
 - Identity Protection, [Em linha]. Disponível em <http://www.identityprotection.com/home> (última consulta em 2.11.2015).
 - Informação da OCDE, [Em linha]. Disponível em <http://www.cybercrimelaw.net/OECD.html>, (consultado em 17.02.2015).
 - Inquérito do Eurobarómetro da Comissão Europeia, [Em linha]. Disponível em www.europa.eu/rapid/press-release_IP-12-751_pt.htm (última consulta em 2.11.2015).

- “Inquérito Kaspersky”, *Jornal de Notícias*, 22 de outubro de 2014, [Em linha]. Disponível em http://www.jn.pt/PaginaInicial/Tecnologia/Interior.aspx?content_id=4194874 (consultado em 22.10.2014).
- LanGuard Scan, [Em linha]. Disponível em <http://www.gfi.com/languard/> (última consulta em 2.11.2015).
- Liga Anti Difamação, [Em linha]. Disponível em <http://adl.org> (última consulta em 2.11.2015).
- Microsoft PhotoDNA, página da Internet disponibilizada pela *Microsoft* com a explicação do *PhotoDNA*, [Em linha]. Disponível em www.microsoft.com/en-us/news/presskits/photodna/. (última consulta em 3.11.2015)
- Microsoft Security Essentials, [Em linha]. Disponível em www.microsoft.com (última consulta em 2.11.2015).
- Nmap, [Em linha]. Disponível em <http://www.insecure.org> (última consulta em 2.11.2015).
- “Organização de Cooperação de Xangai engrossa fileiras”, [Em linha]. Disponível em http://portuguese.ruvr.ru/news/2014_09_11/Organizacao-de-Cooperacao-de-Xangai-engrossa-fileiras-4918/ (consultado em 2.11.2014).
- Orla Cox, gestora da *Symantec*, [Em linha]. Disponível em www.symantec.com (última consulta em 3.11.2015).
- Perry Barlow “Declaration of the Independence of Cyberspace”. Disponível em <https://projects.eff.org/~barlow/Declaration-Final.html> (consultado em 23.11.2015).
- Portal bullying, [Em linha]. Disponível em <http://www.portalbullying.com.pt/>
- Relatório do grupo Aho, [Em linha]. Disponível em http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm, (consultado em 12.11.2014).
- SeguraNet, “Navegar em Segurança”, [Em linha]. Disponível em <http://www.seguranet.pt/> (última consulta em 3.11.2015).
- Sítio eletrónico da Presidência Dinamarquesa do Conselho da Europa, [Em linha]. Disponível em <http://eu2012.dk/en/NewsList/Juni/Uge-26/cybercrime> (última consulta em 3.11.2015)

- The EU Economy: 2007 Review, [Em linha]. Disponível em http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf (consultado em 12.11.2014).
- The Terrorism Research Center, [Em linha]. Disponível em <http://www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf> (última consulta em 3.11.2015).
- United Nations Office on Drugs and Crime (UNODC), [Em linha]. Disponível em <http://www.unodc.org> (última consulta em 3.11.2015).
- United States – Computer Emergency Readiness Team (US-CERT), [Em linha]. Disponível em www.us-cert.gov (última consulta em 3.11.2015).
- US Department of Homeland Security, [Em linha]. Disponível em www.dhs.gov (última consulta em 3.11.2015).

Anexo 1 – Glossário⁵⁸⁷

Glossário

Anonymicer – Programa alemão para a navegação anónima. É semelhante ao *Anonymizer*, com a particularidade de ser totalmente grátis, permitindo ainda remeter mensagens de email de forma anónima.

Anonymizer – Permite ocultar o *browser* atrás do *proxy* do servidor ou atrás do *proxy* do próprio programa. <http://www.anonymizer.com>

Anonymous – São um grupo de “hackers” anónimo que atua na *Internet* e luta pela liberdade.

Auto-estrada da Informação – Entende-se o projeto de ligar em rede o maior número possível de sítios informatizados e de lares, para uma difusão personalizada e interativa de aplicações *multimedia* de qualquer natureza.

Backup – Cópias de segurança, que permitem guardar no disco rígido do computador, ou em qualquer formato digital, toda a nossa informação, que em caso de avaria ou deterioração da primeira versão nos permite aceder à cópia desses dados.

Bits – Dígitos binários. Um sistema é construído a partir de duas unidades de informação: 0 ou 1. Cada uma delas é um *bit*.

Botnets – Rede de computadores comprometidos (também conhecidos como *zombies*) controlados por uma pessoa ou organização, que se destina a ser usada para atividades ilícitas. Uma vez criada, a rede de computadores infetados que constituem a “botnet” pode ser ativada sem o conhecimento dos utilizadores dos computadores a fim de lançar um ciberataque em grande escala, o que geralmente tem o potencial de provocar danos graves, como por exemplo: a perturbação de serviços de sistema de importância pública significativa, ou importantes custos financeiros, ou a perda de dados pessoais ou informações sensíveis.

⁵⁸⁷ Todos os conceitos aqui presentes encontram-se definidos e devidamente citados ao longo do texto. Apenas foram incluídos no presente anexo para que fosse mais fácil a sua consulta pelo leitor.

Bundling – Prática utilizada nos primeiros computadores em que estes eram desenvolvidos e comercializados juntamente com os programas adaptados às necessidades específicas dos utilizadores.

Bytes – Conjunto formado por oito *bits*. *Bit* é a menor unidade digital de informação, representada por 0 ou 1.

Chat – Troca de mensagens em tempo real por utilizadores da *Internet*.

Cibercrime – Por *Cibercrime* entende-se todos os crimes praticados com recurso ou por intermédio de tecnologias da informação, processamento e comunicação.

Cibercriminalidade – Refere-se, geralmente, a um amplo leque de diferentes atividades criminosas que envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais. A *Cibercriminalidade* inclui as infrações tradicionais (por exemplo, fraude, falsificação e roubo de identidade), infrações relativas aos conteúdos (por exemplo, distribuição de material pedo pornográfico em linha ou incitamento ao ódio racial) e crimes respeitantes exclusivamente a computadores e sistemas informáticos (por exemplo, ataques contra os sistemas informáticos, recusa de serviço e *software* malicioso).

Ciberespaço – “Ciber” deriva do termo grego *kybernan*, que significa navegar ou controlar. Conjunto das redes de computadores interligados à *Internet*.

Cibersegurança – Todo o tipo de atividade, a título preventivo ou repressivo, destinado a diminuir os incidentes de segurança e a perceber a sua autoria.

Cloud (*cloud computing*) – Computação em nuvem, tradução do conceito inglês *cloud*. O conceito de “computação em nuvem” refere-se à utilização da memória e das capacidades de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da *Internet*.

Computer crimes – Dizem apenas respeito à criminalidade informática propriamente dita.

Cookie – Pequeno arquivo que fica armazenado no computador do utilizador e guarda todas as informações importantes sobre a sua navegação. O *cookie* permite que um sítio tenha um histórico da navegação do utilizador e, assim, personalize o conteúdo do sítio

de acordo com o perfil de cada *Internauta*, mas também pode ser perigoso, na medida em que o responsável pelo sítio pode ficar a conhecer determinadas preferências e informações de carácter pessoal do utilizador.

Cracker – Pessoa com conhecimento de programação e segurança, que invade sistemas externos existentes na *Internet*, com o objetivo de alterar ou remover dados.

Criptografia – Origem do grego “kryptós” que significa escondido, oculto, mais “grápho” que significa grafia, escrita. É a arte ou a ciência de escrever em cifra ou em código. Conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que apenas o destinatário o decifre e compreenda.

CrowdStrike – É um fornecedor global de tecnologia e serviços focados na identificação de ameaças avançadas e de ataques direcionados à segurança. Sítio oficial disponível: <http://www.crowdstrike.com>.

Cyberstalking – É um conceito de origem recente para o qual ainda não existe uma definição certa. No entanto, pode ser definido como um abuso que envolve ameaças e assédio doentio, em que alguém persegue de uma maneira assustadora e constante uma outra pessoa, através dos meios informáticos (seja através do telemóvel ou das redes informáticas).

Dados informáticos – “Qualquer representação de factos, informações ou conceitos sob uma forma suscetível de processamento num sistema informático, incluindo os programas aptos a fazerem um sistema informático executar uma função”. Definição presente na alínea b), do artigo 2.º da Lei n.º109/2009, de 15 de setembro.

Dados pessoais – Quaisquer informações, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativas a uma pessoa singular identificada ou identificável, que será o titular dos dados.

Dados de tráfego – São “os dados informáticos relacionados com uma comunicação efectuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajecto, a hora, a data, o tamanho, a duração ou o tipo de serviço subjacente”. Definição presente na alínea c), do artigo 2.º da Lei n.º109/2009, de 15 de setembro.

Darknet – É uma rede virtual estabelecida entre vários utilizadores, inacessível a terceiros, e que funciona através de uma rede de telecomunicações pública, neste caso a *Internet*, que visa a partilha de informações e ficheiros em formato digital sem, contudo, permitir que, quer os endereços de *IP* dos seus membros, quer o teor das comunicações entre si estabelecidas, possam ser descobertos.

Denial of Service (DoS) – (Negação de Serviço) Ataque que consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços. Impedimento intencional do acesso aos recursos ou o retardamento do seu acesso por um determinado período de tempo. Basicamente o ataque caracteriza-se por explorar vulnerabilidades e através disto obter acesso privilegiado a máquinas que preferencialmente operem em redes de banda larga. Os sistemas operacionais preferidos para utilização são o *Solaris* e *Linux* devido à existência de *rootkits* e *sniffers* para esses sistemas.

Distributed Denial-of-Service (DDoS) – (negação de serviço distribuída). Tal como o ataque de “negação de serviço” tem como objetivo a quebra de um serviço de um sítio por esgotamento dos seus recursos, levado a cabo por vários clientes ao mesmo tempo, aumentando as probabilidades de sucesso. Neste caso, o atacante controla várias máquinas/clientes que efetuam os pedidos.

Download – Transferência de um ficheiro para o computador. Fazer *download* significa copiar um determinado ficheiro do servidor de um sítio da *Internet* para o computador pessoal.

E-Book – Livro escrito ou disponibilizado em formato eletrónico. Os formatos mais utilizados são em *PDF* (*Adobe Reader*) e *DOC* (*Microsoft Word*). *E-Book* também pode significar um livro eletrónico; título autoral (livros, estudos, artigos) que é compilado na forma de *software* e disponibilizado, de forma gratuita ou onerosa, na *Internet*.

E-Business – Qualquer empreendimento baseado na *Internet*. Transações comerciais ou financeiras efetuadas entre entidades via *Internet*.

ECHELON – É definido como “um sistema global de intercepção de comunicações privadas e económicas”.

E-Commerce – Chamado comércio eletrónico. Forma de realizar negócios entre empresas e consumidor (B2C) ou entre empresas (B2B), usando a *Internet* como plataforma de troca de informações, encomenda e realização das transações financeiras.

E-Learning (ou ensino eletrónico) – Corresponde ao ensino não presencial através da *Internet*.

E-Procurement – A palavra “procurement” significa adquirir, comprar. Consiste numa aplicação ou num *website* que tem por objetivo a aquisição de mercadorias, produtos ou serviços, geralmente suprimentos para posterior fornecimento a outros interessados.

Fidonet – Rede digital que não opera em tempo real, mas apenas estabelece ligações quando necessário.

Firewall – Sistema de proteção contra a saída de dados ou a entrada de interferências provenientes de um sistema exterior. Ponto de conexão da rede com o mundo externo, tudo o que chega passa pelo *firewall*, que decide o que pode ou não entrar, dependendo do nível de segurança criado pela entidade. O *firewall* analisa o tráfego entre a rede interna e a rede externa em tempo real, permitindo ou bloqueando o tráfego de acordo com as regras definidas previamente. Todavia, o *firewall* não protege de infeção com *vírus*, *trojans* decorrentes de *downloads*, anexos a mensagens de correio eletrónico, entre outros casos.

Flaming – O fenómeno *online* de *flaming* ocorre quando o utilizador perde o auto controlo e escreve uma mensagem que emprega linguagem depreciativa, obscena ou indecorosa.

GPS – Nascido nos Estados Unidos da América, durante a Guerra Fria, para fins militares e destinado a guiar aeronaves e mísseis, é composto por 24 satélites *Navstar*, em seis órbitas diferentes, percorrendo a órbita da Terra em cada 12 horas. O *GPS* é hoje utilizado em múltiplos sistemas de navegação e orientação, da navegação aérea à automóvel e às bombas, sendo agora também utilizado na localização de chamadas de telemóveis.

Grooming – Por *grooming* entende-se a atuação de adultos que, através das tecnologias de informação e comunicação, propõem a uma criança um encontro, com a finalidade de cometer crimes de natureza sexual.

Habilus – Na sequência da instalação da *Intranet*, foi introduzido na rede informática dos Tribunais, um programa designado “habilus”, o qual tem simplificado o trabalho dos oficiais de justiça, com a padronização da maioria dos atos, designadamente com formulários redigidos pela *DGAJ*, com a automatização da distribuição, com a criação de bases de dados dos elementos identificativos de cada processo, seus intervenientes, residenciais e endereços de correio eletrónico de mandatários. É igualmente através deste sistema que é possível o acesso ao registo informático de execuções.

Hacker – Pessoa que procura aceder a sistemas sem autorização, usando técnicas próprias no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros.

Hacking – Infiltração não autorizada em sistemas de informação.

Hacktivismo – Pode ser definido como a infiltração não autorizada em sistemas de informação, e *activismo* (vertente política), isto é, a ação militante, tendo em vista alcançar um objeto político ou social

Hardware – São as unidades físicas que integram um computador, por exemplo, CPU, monitor, teclado, circuitos.

Hoaxes – São *emails* (mensagens de correio eletrónico), na maioria dos casos com remetente de empresas conhecidas ou de órgãos governamentais, mas que na verdade comportam mensagens falsas, carregadas de vírus.

Honey Pot – Acaba por ser um dos componentes principais de todo o sistema de proteção, pois é este tipo de ambiente que deverá “enganar” o “hacker” ou atacante da rede. Assim, quando o *hacker* atacar a rede deverá “cair” dentro do “Honey pot” e ficar de algum modo convencido que está na rede real. Por isso, torna-se necessário que, de algum modo, este “Honey Pot” mostre ao *hacker* o ambiente real da rede de um modo muito convincente.

Host – Computador ligado à *Internet* onde um *website* é alojado para poder ser acedido pelos internautas. Computador central, também designado por servidor, onde se encontra gravado (alojado) o conjunto de programas e ficheiros de um ou mais sítios.

HTTP – *Hypertext Transport Protocol*. Protocolo que define como dois programas ou servidores devem transferir entre si comandos ou informações relativas à *Internet*. É

uma abreviatura usada no início do endereço de qualquer sítio do WWW (exemplo <http://www.quidjuris.pt>).

IDzap – Serviço gratuito que esconde determinadas informações, tais como conteúdo do computador, endereço IP e evita a gravação de cookies. Disponível em <http://www.idzap.com>

INCYDER – (*International Cyber Developments Review*). É uma nova base de dados que contém documentos de âmbito legal e policial adotada por organizações internacionais ligadas à *Cibersegurança*, com notícias sobre os desenvolvimentos nesta área. Esta base de dados tem sido desenvolvida e apresentada pela *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, com sede em Tallinn, Estónia. Esta nova base *Web Incyder* encontra-se aberta ao público e de forma gratuita em www.ccdcoe.org/incyder.html. Abrange regulações de, pelo menos, quinze órgãos internacionais, incluindo *NATO, APEC, ITU, UE, OECD, UN* e *SCO*.

Infraestrutura crítica – Pode ser entendida como um conjunto de elementos, sistemas ou partes destes situados nos Estados Membros, essenciais para a manutenção das funções sociais vitais, da saúde, da segurança e do bem-estar económico e social das pessoas, como centrais energéticas, redes de transportes ou redes governamentais, cuja perturbação ou destruição teria um impacto significativo num Estado Membro, devido à impossibilidade de continuar a assegurar tais funções.

Internauta – Pessoa que navega (visita vários sítios) na *Internet*.

Intranet – Rede interna de informações baseada na tecnologia da *Internet*. É usada por qualquer tipo de organização (empresa, entidade ou órgão público) que deseje partilhar informações apenas entre os seus utilizadores registados, sem permitir o acesso de outras pessoas. O que o utilizador vê é um interface igual ao da *Internet*.

IP – Abreviatura de *Internet Protocol*. Uma das linguagens, ou protocolos, mais importantes da *Internet*, responsável pela identificação das máquinas e redes e pelo encaminhamento correto de mensagens entre elas.

IP Spoofing – Ataque em que um sistema assume ilicitamente a personalidade de outro sistema, usando o seu endereço de identificação na *Internet*. Normalmente costumam

ser utilizados em ataques de *Deny of Service*, e para realizar autenticações fraudulentas através de endereço de IP em redes que aceitam esse tipo de autenticação.

ISP (Internet Service Provider) – Provedor de acesso à *Internet*. Entidade que faculta o acesso dos utilizadores à *Internet*.

Juice Jacking – Invasão de aparelhos informáticos que utilizam um cabo com porta USB para carregar a bateria. Um cabo de USB é utilizado, quer para carregar a bateria dos aparelhos quer para transmitir dados. Enquanto estes aparelhos carregam a bateria, um dispositivo malicioso é utilizado para invadir o sistema tecnológico dos mesmos e furtar, bloquear ou apagar toda a informação contida no telemóvel.

Kaspersky Lab – É uma empresa russa produtora de *software* de segurança para a *Internet*, contra ameaças de vírus, *hackers*, *spam*, *trojans* e *spyware*.
www.kaspersky.com

Link – *ligação*; apontador para outra fonte de informação.

Mailbombing – Um utilizador da *Internet* lança uma “mailbomb” a uma determinada vítima, enviando-lhe um elevado número de mensagens de correio eletrónico sem conteúdo útil, com o objetivo de sobrecarregar (ou, pelo menos, perturbar) o computador recetor.

Mainframe – Um computador de grande porte, dedicado normalmente ao processamento de uma vasta quantidade de informação. Uma vez que são equipamentos que ocupam muito espaço e necessitam de muita manutenção, foram substituídos por servidores de computadores pessoais e servidores *Unix* (sistema operativo), que têm custos significativamente mais baixos e que necessitam de menor manutenção.

Malware – *Malicious software* (vírus informático).

Modelo Multi-stakeholder – Este modelo preconiza uma colaboração, intervenção e partilha de responsabilidades entre governos, o setor privado nas suas várias dimensões, a sociedade civil onde as *Organizações Não Governamentais* tem um papel chave e os cidadãos.

National Cyber Alert System – Um sistema de identificação, análise e valoração de vulnerabilidades e ameaças às redes e sistemas. Recolhendo informação de todos os

utilizadores, este sistema dirige-se também a todos os utilizadores, a quem pretende fornecer dados e ferramentas essenciais para agir no *Ciberespaço*.

Newsletters ou e-letter – Notícias ou comunicações eletrónicas, como, por exemplo, boletins de atualização de *websites*, boletins periódicos, etc.

Nmap – É um varredor de *hosts*, computador ligado à *Internet* onde um *website* é alojado para poder ser acedido pelos internautas. Computador central, também designado por servidor, onde se encontra gravado, alojado o conjunto de programas e ficheiros de um ou mais sítios que usa recursos avançados para verificar o estado do “alvo”. Trata-se de um programa gratuito disponível para os seguintes sistemas operativos: *Linux* e *Windows*, *Mac OS*, *Solaris*, *FreeBSD* e *OpenBSD*, a partir do sítio oficial <http://www.insecure.org>.

Nomes de Domínio – Ou também chamados de *Domain Names*. Nome como determinada entidade ou computador é identificado pelo servidor de nomes na *Internet* (exemplo: www.quidjuris.pt, o domínio é “pt”. Por sua vez, “quid juris” é o subdomínio e “www” é a World Wide Web).

Password – Palavra chave ou código de acesso.

Phishing – (ou, em Português, “Ciber-iscagem”). Por *phishing* entendem-se as tentativas fraudulentas de obtenção de informações sensíveis, como senhas e dados do cartão de crédito, através de uma comunicação eletrónica, utilizando uma identidade falsa que se faz passar por verdadeira. O utilizador é assim levado a introduzir os seus dados pessoais num sítio que julga ser de confiança, quando na verdade está a fornecê-los a uma pessoa, ou organização, que os utilizarão de forma maliciosa.

Sextortion – Nova forma de exploração sexual, que liga os crimes pedófilos aos meios tecnológicos.

Shunning – Sucede quando um utilizador da *Internet* se recusa a receber mensagens de outra pessoa utilizadora da *Net* (ou, mais genericamente, quando utiliza um programa de computador conhecido como um “kill file” para automaticamente desviar quaisquer mensagens de correio eletrónico de um endereço especificado).

Site/Sítio – ou “servidor *Web*”, em sentido amplo, são os termos que designam um computador de uma certa dimensão e capacidade, ligado diretamente à rede *Internet*,

onde se encontram as páginas (*home pages*) que contêm a informação disponível aos utilizadores da rede. Cada sítio é identificado por um dado *endereço*, aqui designado “nome de domínio” (*domain name*).

Smishing – Tal como no “Phishing”, *Smishing* usa as mensagens de texto para enganar os utilizadores. Normalmente, a mensagem de texto contém um URL ou número de telefone. O número de telefone tem geralmente um sistema de resposta automática. E tal como acontece nos casos de “Phishing” requer uma ação por parte do utilizador, que este faça algo. É comum a mensagem ser proveniente de um número “5000”, em vez de um número verdadeiro de telefone, isto acontece porque a mensagem é enviada de um *email* e não de um número telefone.

Sniffer – Programa que monitoriza o tráfico em rede. Os *hackers* usam os *sniffers* para capturar dados transmitidos na rede. A esta técnica também é dado o nome de *Sniffing*.

Sniffing – Consiste em introduzir um programa/ferramenta na rede conhecida como “sniffer” que lê e decodifica todos os pacotes de dados na rede, ganhando acesso a vários ficheiros de dados da rede, a registos de *passwords*, a conteúdos de email e podendo eventualmente alterá-los ou enviá-los para o exterior.

Software – *Software* do computador é um termo usado para contrastar com o de *hardware*. Tem um sentido amplo, já que abrange não só o “programa de computador”, isto é, o seu elemento principal, mas ainda a descrição detalhada do programa (gráficos e diagramas esquemáticos, a partir dos quais as instruções do programa foram codificadas para criar o programa), bem como a documentação escrita auxiliar deste, (instruções operativas para o utilizador e manual do utilizador) e outro material de apoio - que pode apresentar-se em suporte de papel ou informático – relacionado com o programa.

Spam – Toda e qualquer correspondência eletrónica não solicitada e/ou não autorizada. Embora o artigo 22.º do Decreto-Lei n.º7/2004, de 7 de Janeiro enfoque, as mensagens não solicitadas no âmbito de marketing direto, o *spam* é muito mais amplo, abrangendo toda a forma de receção de mensagens não solicitadas.

Spyware – São programas espiões que enviam informações do computador do utilizador e inspecionam dados pessoais, como os documentos e histórico da navegação na *Internet*. Inclusive, tudo o que for digitado no teclado do próprio computador ou

clicado com o rato (*inputs* do utilizador), pode ser monitorizado pelo *spyware*. Alguns tipos de *spyware* têm um mecanismo que faz imediata conexão com o respetivo servidor logo que o internauta fique *online*. Paralelamente altera parâmetros de configuração do sistema e instala outros tipos de *software*.

Surface Web – Pode ser definida como a parte da *Internet* que é geralmente acessível através dos motores de busca, como sejam o *Google*, o *Bing* ou o *Yahoo*, isto é, será o conjunto de páginas detetadas e escolhidas pelos motores de busca para integrarem os resultados de uma pesquisa.

TCP/IP – As máquinas ligadas à rede *Internet* comunicam utilizando “uma linguagem de comunicação” comum chamada TCP/IP (*Transmission Control Protocol/Internet Protocol*), que assegura a interoperabilidade entre os computadores heterogéneos que estão ligados à rede.

Trojans Horses – (*Cavalos de Troia*) não são vírus, mas programas que são instalados em computadores com intenções maliciosas e utilizados para abrir portas para que o computador possa ser atacado remotamente. O seu objetivo é causar algum dano ao computador onde esteja instalado, apagando arquivos, pastas ou prejudicando a sua funcionalidade. Na sua maioria, os *trojans* não são detetados pelos programas de antivírus. Uma vez instalado, o *trojan* pode capturar informações do utilizador. Após colher essas informações, pode remeter as mesmas para o seu criador e/ou autodestruir-se, eliminando todos os vestígios da sua passagem.

Unbundling – Contrário da prática *bundling*. Prática em que o *software* passou a ser desenvolvido e comercializado como produto autónomo, isto é, passou a ser desenvolvido e comercializado separadamente dos computadores.

Unix – Sistema operacional desenvolvido e utilizado em estações de trabalho de alto desempenho. Permite o uso simultâneo de vários utilizadores.

Upload – O contrário de *download*; transferir o ficheiro do computador do utilizador para um outro computador remoto.

Vírus – *Software* malicioso que tem a função de auto-replicar-se e infetar partes do sistema operativo ou dos programas de aplicação, com o objetivo de causar a perda ou o dano nos dados.

Vírus de arquivos ou programas – São aqueles que infetam ficheiros de programas. São arquivos que têm em regra as extensões *COM*; *EXE*; *OVL*; *DLL*; *DVR*; *SYS*; *BIN* e *BAT*.

Vírus de Boot – São vírus que infetam a área de sistema de um disco.

Vírus informáticos – São um *software* malicioso que tem a função de auto-replicar-se e infetar partes do sistema operativo ou dos programas de aplicação, com o objetivo de causar perda ou dano nos dados guardados nos computadores.

Vírus de Macro – São vírus que infetam os arquivos dos programas *Microsoft Office*, *Word*, *Excel*, *PowerPoint* e *Access*. Todos estes vírus usam a linguagem de programação interna do programa, que foi criada para permitir que os utilizadores automatizem determinadas tarefas.

Vírus Polimórficos – Utilizam técnicas de criptografia para construir a sequência de bytes (conjunto formado por oito bits. *Bit* é a menor unidade digital de informação, representada por 0 ou 1). A cada cópia gerada, uma nova combinação é utilizada para criptografar essa sequência. De forma que um único vírus pode ter inúmeras formas diferentes, que são decodificadas por chaves contidas numa pequena parte do vírus, sempre que necessário.

Vírus de Stealth – Utiliza técnicas para ocultar as alterações executadas, e enganar o antivírus, como por exemplo, fazendo um *backup* dos arquivos alterados.

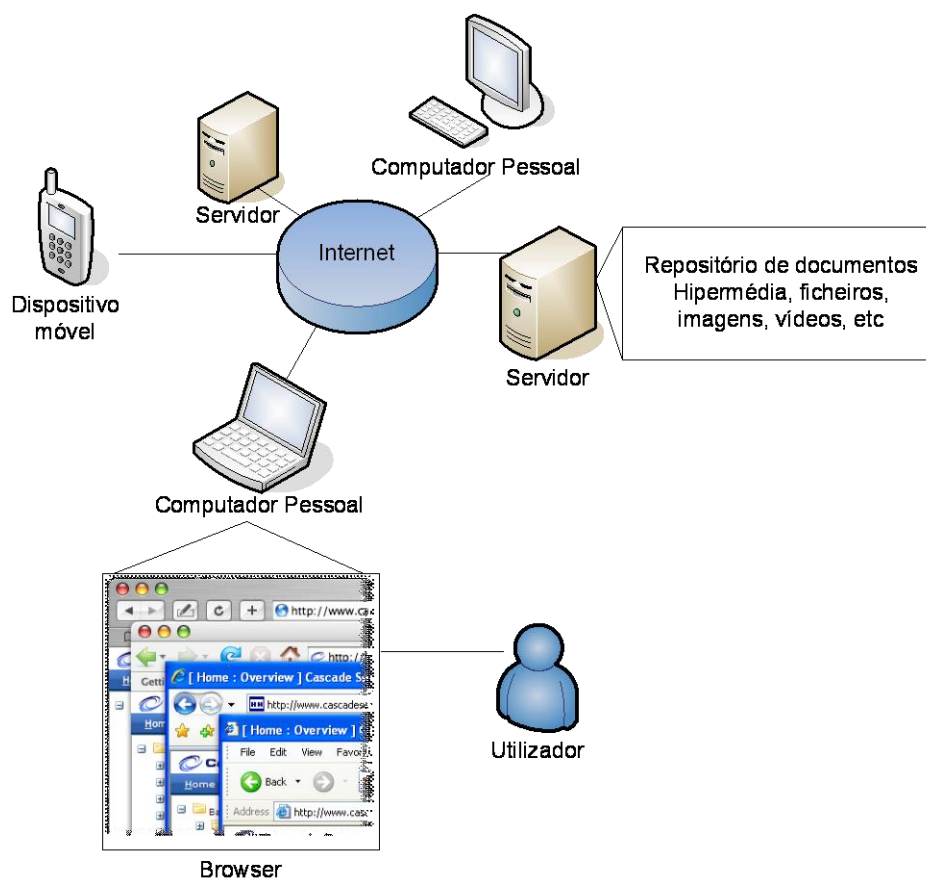
Vishing – É uma versão do método criminal “Phishing”. Neste caso o criminoso tenta solicitar a informação pessoal do utilizador através do telefone. O *Vishing* apoia-se em “engenhos sociais” para enganar o utilizador a fornecer informações pessoais que, posteriormente, possam ser usadas pelo criminoso para aceder às contas dos utilizadores.

Wireless – Expressão genérica que designa sistemas de telecomunicações, nos quais as ondas eletromagnéticas – e não fios – encarregam-se do transporte dos sinais.

World Wide Web – (Rede de Alcance Mundial. É também definida como *WWW*). Conjunto interligado de documentos e arquivos que fazem parte da *Internet* e se encontram armazenados em servidores *http*.

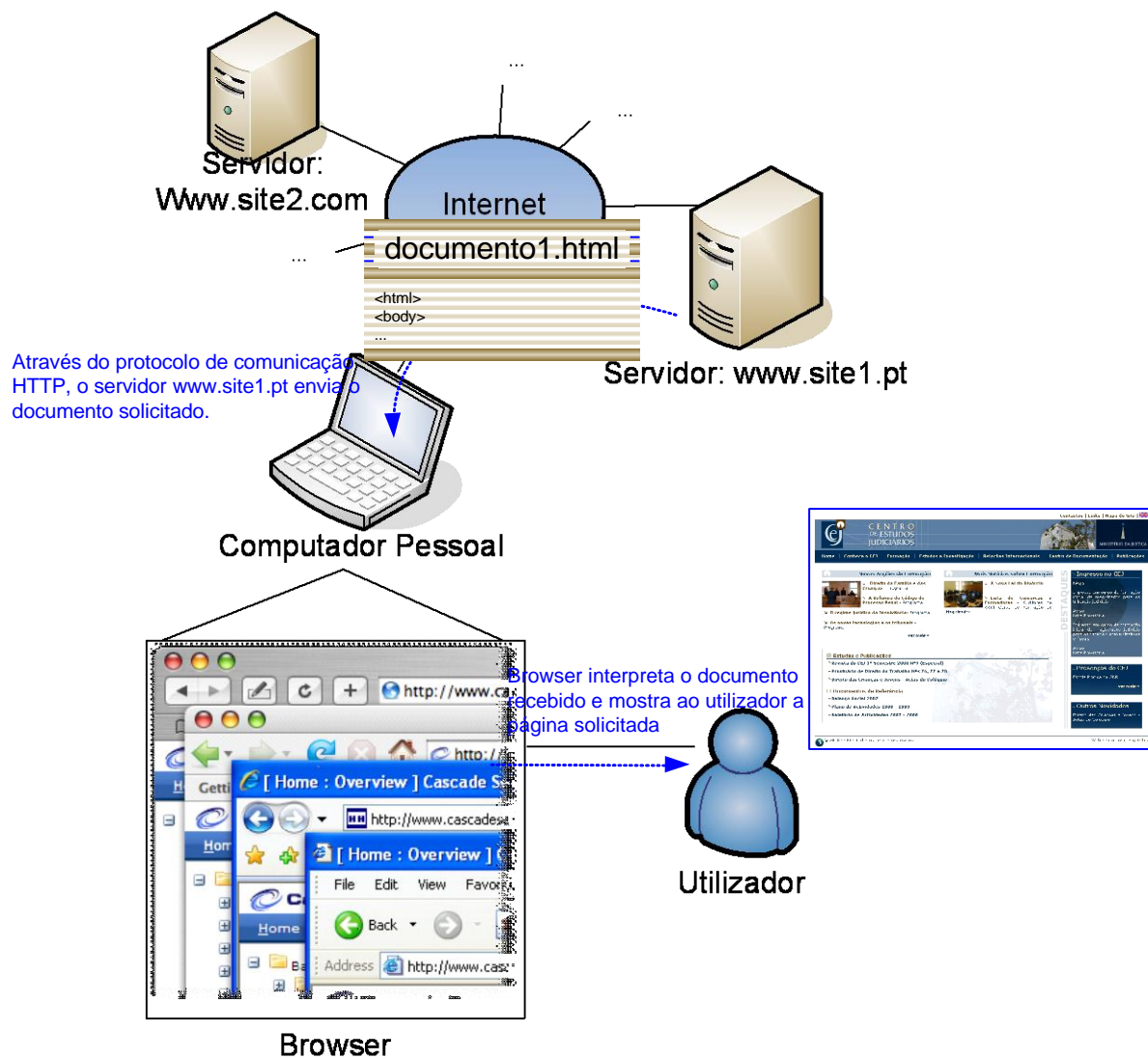
Anexos 2 – Figuras

Figura 1 – Esquema exemplificativo “World Wide Web”⁵⁸⁸



⁵⁸⁸ Imagem cedida por Eng. Lino Santos, FCCN/ CERT.PT, Apresentação em ação de formação no Centro de Estudos Judiciários.

Figura 2 – Esquema exemplificativo de comunicação entre “cliente-servidor”⁵⁸⁹



⁵⁸⁹ Imagem cedida por Eng. Lino Santos, FCCN/ CERT.PT, Apresentação em ação de formação no Centro de Estudos Judiciários.

Figura 3 – Exemplo de um ataque de “Phishing” através do correio eletrónico⁵⁹⁰

Phishing (continuação)

De: B.Bradesco S.A [mailto:bradescopessoaafisica@www.bradesco.com.br]

Enviada: terça-feira, 26 de Agosto de 2008 5:57

Para: nome@netvisao.pt

Assunto: nome, Comunicado Importante

Caro, cliente Bradesco.

Houve um problema interno de informações em nosso banco de dados, onde as chaves de segurança, não foram atualizadas, ocorrendo problemas ao seu acesso pelo Internet Banking e outros canais de conveniência Bradesco.

Estamos lançando uma atualização do Módulo de Segurança Bradesco para corrigir esta falha.

Ao tentar o acesso via Bradesco Internet Banking, Caixas Eletrônicas e Fone Fácil suas chaves de segurança constarão como inexistentes, impossibilitando o acesso.

A Chave, gerada pelo dispositivo abaixo, será agregada ao processo já existente, sem substituição das senhas atuais (Senha de 04 números e Frase Secreta para utilização nos acessos ao Bradesco Internet Banking).

Para corrigir este problema, basta clicar no caminho abaixo, e concluir a atualização acessando o internet banking Bradesco.

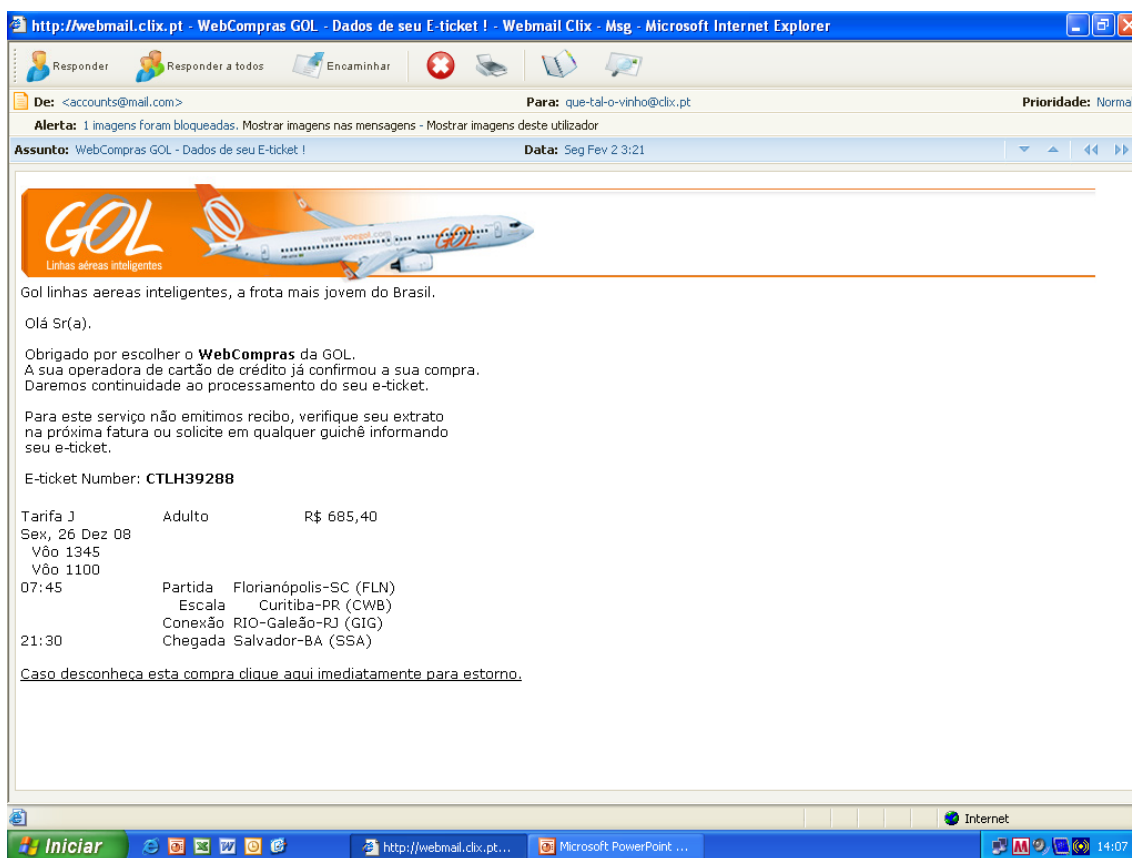
<https://www.bradesco.com.br/atualizacaoadeseguranca>

Em caso de dúvida, contatar a central Bradesco, pelo e-mail atendimento@bradesco.com.br, de segunda a sexta-feira das 07:00 às 20:00 horas

© 2008 Banco Bradesco S.A. Todos os direitos reservados.

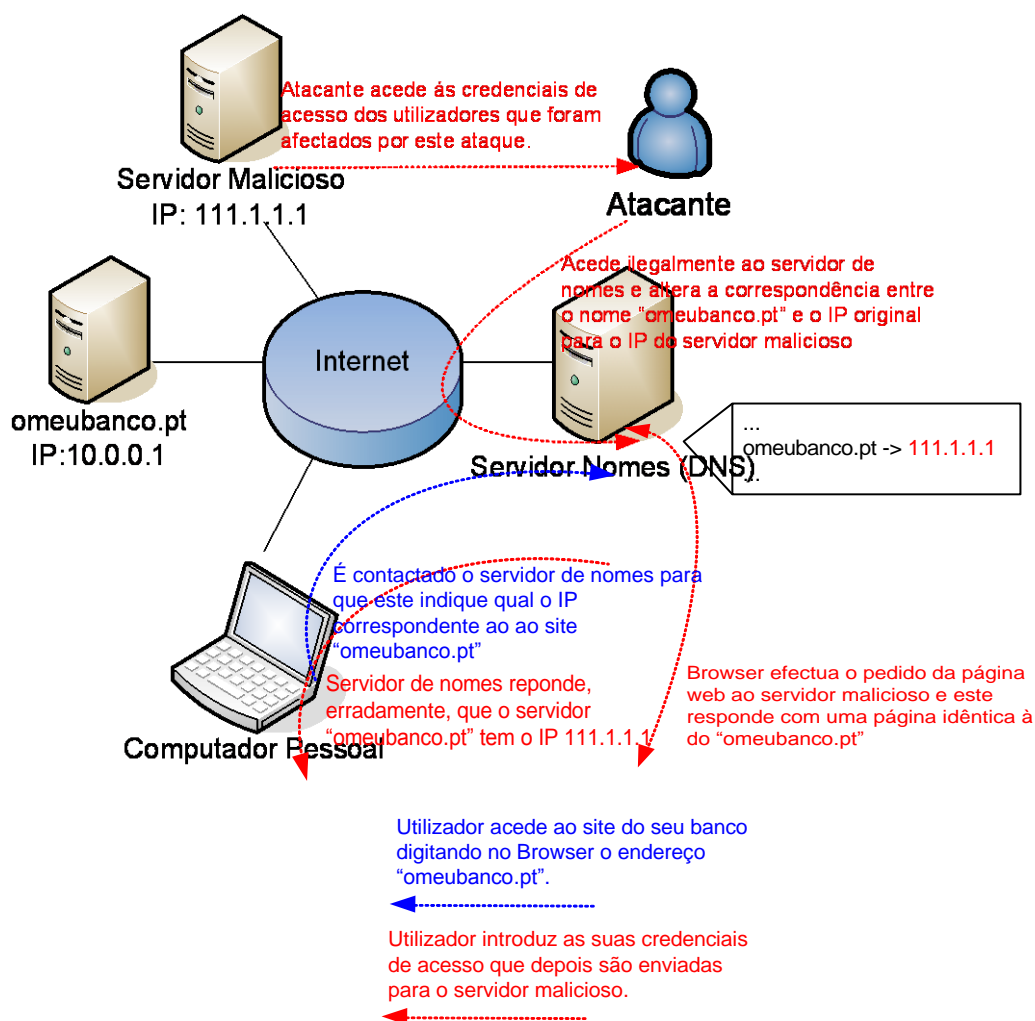
⁵⁹⁰ Imagem cedida por Eng. Lino Santos, FCCN/ CERT.PT, Apresentação em ação de formação no Centro de Estudos Judiciários.

Figura 4 – Exemplo de um falso *email* com o intuito de confirmar os dados bancários do utilizador (*Phishing*)⁵⁹¹



⁵⁹¹ Imagem cedida por Pedro Verdelho, Apresentação em ação de formação no Centro de Estudos Judiciários.

Figura 5 – Exemplo de “Pharming” enquanto *modus operandi*⁵⁹²



⁵⁹² Imagem cedida por Eng. Lino Santos, FCCN/ CERT.PT, Apresentação em ação de formação no Centro de Estudos Judiciários.

Figura 6 – Exemplo de Transmissão de Vírus através do correio eletrónico⁵⁹³

De: SERVIDOR <servidor@server.com>
Para: @clix.pt
Data/Hora: 2008/11/28 21:43:49
Assunto: Atualização

ATUALIZAÇÃO DO SERVIDOR DE E-MAIL

Nome do arquivo: anti-spam.scr

Tamanho do Download: 660 KB

Data de Publicação: 25/11//05

Versão: 1.0

Download:

[anti-spam.scr](#)

É extremamente importante
que se faça este download

Ferramenta anti-spam

O servidor apresenta uma nova atualização. Cujo o objetivo é garantir a segurança no seu e-mail e ficar livre de e-mails comerciais. A atualização foi lançada em 25/11/08.

A mensagem deste e-mail está sendo enviada pelo servidor de seu e-mail.

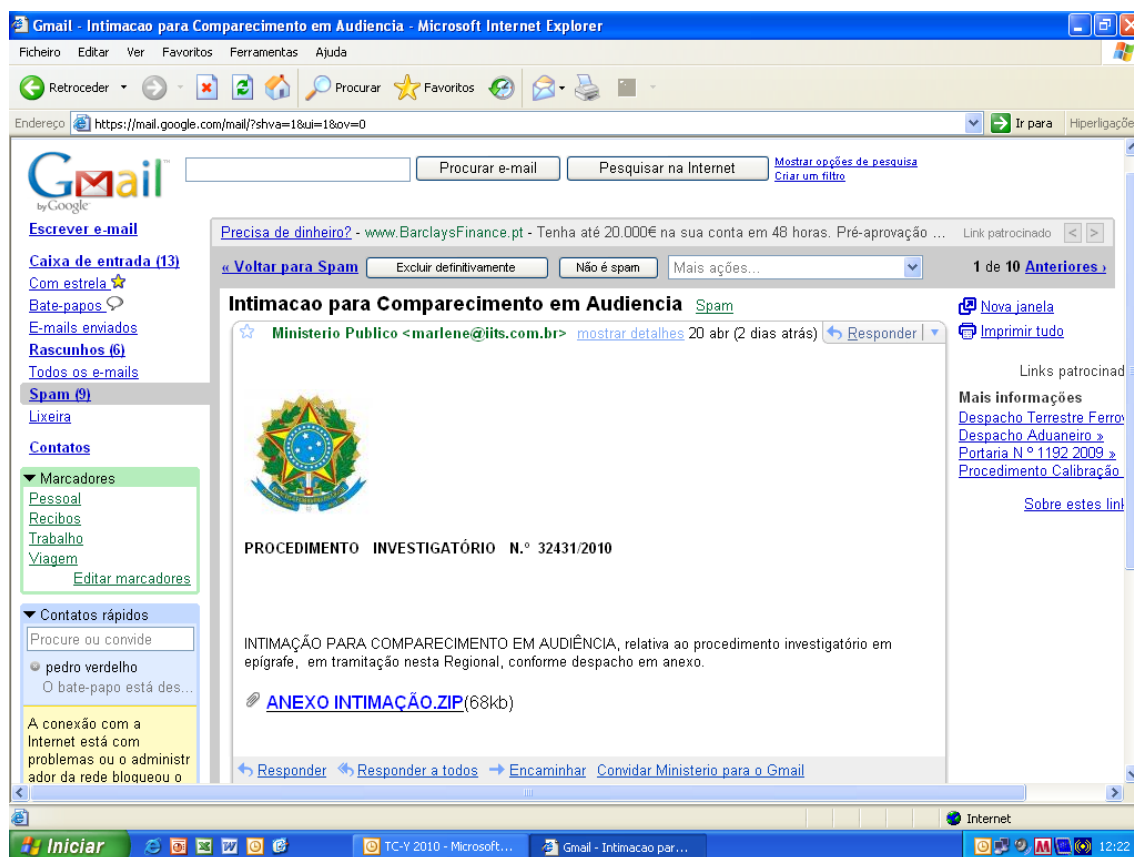
⁵⁹³ Imagem cedida por Pedro Verdelho, Apresentação em ação de formação no Centro de Estudos Judiciários.

Figura 7 – Exemplo de uma notificação eletrónica falsa do “Superior Tribunal de Justiça”⁵⁹⁴



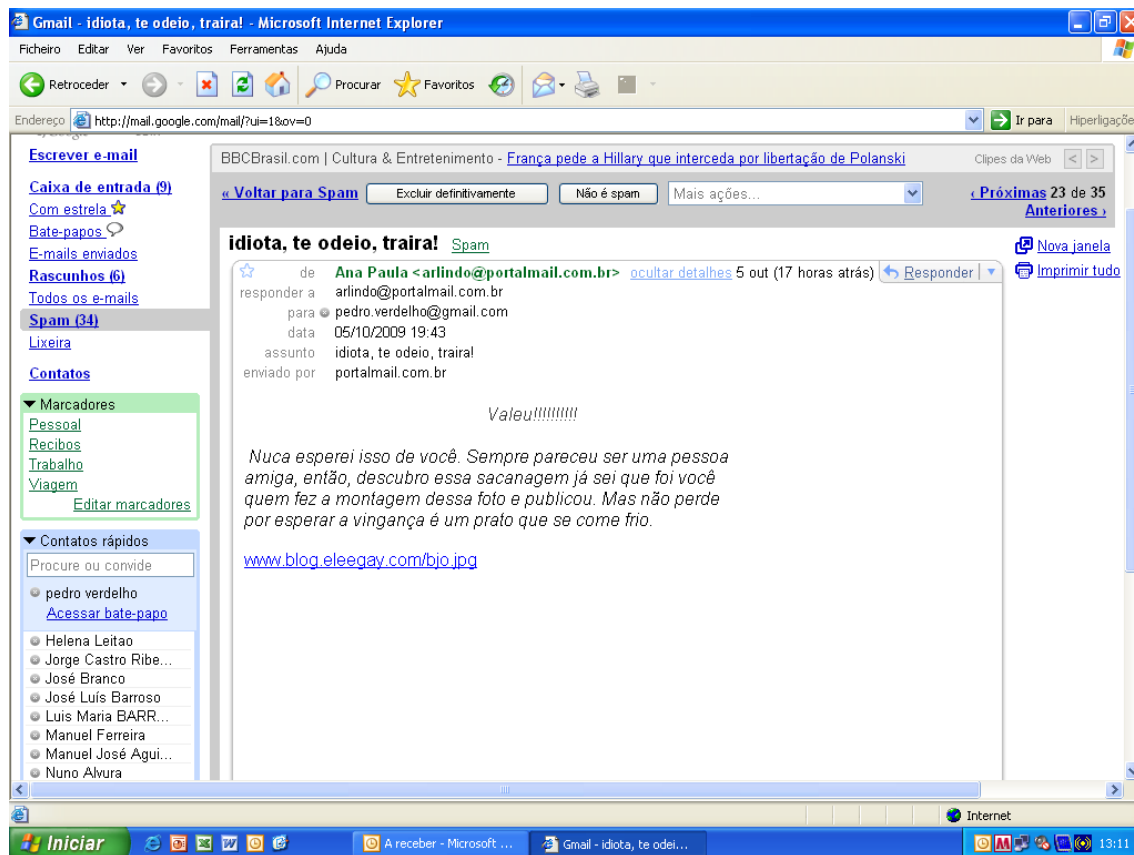
⁵⁹⁴ Escreveu-se “Superior Tribunal de Justiça” propositadamente, tal como aparece no *email* supra. Imagem cedida por Pedro Verdelho, Apresentação em ação de formação no Centro de Estudos Judiciários.

Figura 8 – Exemplo de uma notificação eletrônica falsa do Ministério Público⁵⁹⁵



⁵⁹⁵ Imagem cedida por Pedro Verdelho, Apresentação em ação de formação no Centro de Estudos Judiciários.

Figura 9 – Exemplo de transmissão de mensagem “spam” através do correio eletrônico⁵⁹⁶



⁵⁹⁶ Imagem cedida por Pedro Verdelho, Apresentação em ação de formação no Centro de Estudos Judiciários.