Universidade do Minho
Escola de Direito

Pedro Levi Vieira de Oliveira Heitor

Contributo para a Compreensão das Causas de Exclusão de Ilicitude e da Culpa no Crime de Acesso Ilegítimo

Outubro de 2015

UMinho | 2015 Pedro Oliveira Heitor **Contributo para a Compreensão das Causas de Exclusão de Ilicitude e da Culpa no Crime de Acesso Ilegítimo**

Universidade do Minho
Escola de Direito

Pedro Levi Vieira de Oliveira Heitor

Contributo para a Compreensão das Causas de Exclusão de Ilicitude e da Culpa no Crime de Acesso Ilegítimo

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho Efetuado sob a orientação do
Professor Doutor Fernando Eduardo Batista Conde Monteiro
e do
Professor Doutor António Luís Duarte Costa

Outubro de 2015

Declaração

Nome: Pedro Levi Vieira de Oliveira Heitor

Endereço eletrónico: pedro_oliveira_heitor@hotmail.com

Número do Cartão de Cidadão: 13295970 4ZY5

Título dissertação: Contributo para a Compreensão das Causas de Exclusão de Ilicitude e da Culpa no Crime de Acesso Ilegítimo

Orientadores: Professor Doutor Fernando Eduardo Batista Conde Monteiro e Professor Doutor António Luís Duarte Costa

Ano de conclusão: 2015

Designação do Mestrado: Mestrado em Direito e Informática

Universidade do Minho, 29 de Outubro de 2015

Assinatura: _____

Agradecimentos

O trabalho aqui expandido foi possível porque reuniu o contributo de várias pessoas. Foi um trabalho solitário mas que contou com a total confiança, disponibilidade e estímulo de muitas pessoas. Deixo aqui o meu obrigado a todas elas, mas em especial aos meus muito prezados amigos e colegas Tiago Amorim Alves, Sandra Silva, Roberto Cangueiro e Juliana Soares e Sousa.

Ao Professor Doutor Fernando Eduardo Batista Conde Monteiro e Professor Doutor António Duarte Costa agradeço por aceitarem sem reservas a direção desta dissertação, apoiando-me a todo o tempo para o seu término.

Ao Professor e Mestre Pedro Freitas, o meu agradecimento profundo pelo constante apoio, partilha de conhecimentos e valiosos contributos em todo este processo.

Sou muitíssimo grato aos meus pais, pelos sacrifícios feitos de forma a proporcionarem-me a melhor educação possível, ensinando-me os valores humanos e intelectuais essenciais à prossecução dos meus objetivos académicos e profissionais.

"A paz é o fim que o direito tem em vista, a luta é o meio de que se serve para o conseguir. (...) O direito não é uma teoria, mas uma força viva. Por isso a justiça sustenta numa das mãos a balança em que pesa o direito, e na outra a espada de que se serve para o defender. A espada sem a balança é a força brutal; a balança sem a espada é a impotência do direito. Uma não pode avançar sem a outra, nem haverá ordem jurídica perfeita sem que a energia com que a justiça aplica a espada seja igual à habilidade com que maneja a balança."[1]

[1] IHERING, Rudolf von, *A luta pelo direito*, 17.ª ed., Editora Forense, Rio de Janeiro, 1999, p. 1.

CONTRIBUTO PARA A COMPREENSÃO DAS CAUSAS DE EXCLUSÃO DE ILICITUDE E DA CULPA NO CRIME DE ACESSO ILEGÍTIMO

RESUMO

Este trabalho de investigação tem como objetivo apresentar um contributo para a compreensão das causas de exclusão de ilicitude e da culpa no crime de acesso ilegítimo.

Quanto à estrutura da presente dissertação, esta assenta em três capítulos.

No Capítulo I abordamos o crime de acesso ilegítimo através de um enquadramento histórico e dogmático. Assim, são analisados os primórdios deste tipo de ilícito, a sua evolução e quais os mecanismos legais que foram criados para fazer face ao mesmo. Fornecemos também uma análise dogmática do acesso ilegítimo no presente, bem como uma análise conceptual dos termos *Hack*, *Hacker* e *Hacking*. Avançamos ainda com uma proposta de taxonomia de *Hackers*, tendo por base o tipo de acesso (legítimo ou ilegítimo) praticado por estes e as suas intenções (benignas ou malignas) e terminamos com a análise da 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 e as suas implicações neste tipo de ilícito.

No Capítulo II debruçamo-nos essencialmente sobre Segurança Informática. Elaboramos algumas considerações sobre Segurança Informática e Cibersegurança, analisamos técnica e juridicamente os sistemas de proteção ativa e passiva, bem como o fenómeno do *Hack Back,* que é um dos vetores da nossa investigação. Efetuamos ainda uma alusão quanto aos conceitos de *Pentests* e *BackTrack*, enquanto ferramentas para a prática de tal fenómeno.

Por fim, no Capítulo III, elaboramos uma análise de uma hipótese prática, onde percorremos os vários tipos justificadores e os motivos que afastam a culpa de forma a permitir a compreensão ao nível da ilicitude e da culpa no crime de acesso ilegítimo.

CONTRIBUTE FOR THE COMPREHENSION OF THE CAUSES OF EXCLUSION OF UNLAWFULNESS AND GUILT IN THE CRIME OF ILLEGAL ACCESS

SUMMARY

This research work aims to present a contribute for the comprehension of the causes of exclusion of unlawfulness and guilt in the crime of illegal access.

As for the structure of this dissertation, it is based on three chapters.

In Chapter I, we approach the crime of illegal access through a historical and dogmatic framework. Thus, we analyze the beginnings of this type of offense, how it evolved and which legal mechanisms were created to address it. We also provide a dogmatic analysis of illegal access at present, as well as a conceptual analysis of the terms *Hack*, *Hacker* and *Hacking*. We go forward with a proposal for a taxonomy of *Hackers*, based on the type of access (legitimate or illegitimate) practiced by these and their intentions (benign or malignant) and finish with the review of Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA and its implications on this type of offense.

In Chapter II we focus primarily on IT Security. We elaborate some considerations about IT Security and Cyber Security, we analyze technically and legally active and passive protection systems, as well as the phenomenon of *Hack Back*, which is one of the vectors of our investigation. We carry out a description about the concepts of *Pentests* and *BackTrack* as tools to practice that phenomenon.

Finally, in Chapter III, we prepare an analysis of a practical case, where we go through the various justifying types and the motives that rule out guilt in order to allow an understanding at the level of unlawfulness and guilt in the illegal access crime.

ÍNDICE

LISTA DE ABREVIATURAS

Al. - Alínea

Art.º - Artigo

Arts. - Artigos

C.C. - Código Civil

Cf. - Confrontar; conferir

C.P. - Código Penal

C.P.P. - Código de Processo Penal

C.R.P. - Constituição da República Portuguesa

E.U.A. - Estados Unidos da América

Ibid. - *Ibidem*, no mesmo lugar

I.e. - *Id est*, isto é

Op. cit. - Obra citada

P. - Página

Pp. - Páginas

Ss. - Seguintes

V.g. - *verbi gratia*; por exemplo

LISTA DE IMAGENS

LISTA DE TABELAS

INTRODUÇÃO

O recurso exponencial às tecnologias da informação e comunicação no quotidiano traz consigo inúmeras potencialidades e desafios. Inevitavelmente, esta evolução originou – e origina – a cada momento, novos problemas e, para o que a presente investigação aspira analisar, fenómenos de delinquência cometidos com o recurso a essas tecnologias e aos quais o Direito não ficou indiferente. É premente, contudo, uma análise dogmática mais profunda desta problemática, com vista a fornecer um contributo ambicioso para a compreensão das causas de exclusão de ilicitude e da culpa no âmbito de tais ilícitos e, especificamente, no crime de acesso ilegítimo, o que se justifica também pela, ainda, parca doutrina e jurisprudência sobre esta matéria.

Inicialmente, os mencionados fenómenos de delinquência eram punidos pela Lei n.º 109/91, de 17 de Agosto – Lei da Criminalidade Informática e, posteriormente, pela Lei n.º 109/2009, de 15 de Setembro, a qual aprovou a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho da União Europeia, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adaptou o Direito interno à Convenção sobre Cibercrime do Conselho da Europa. Nestas disposições normativas, consta o tipo legal de crime informático denominado como Acesso Ilegítimo e que, segundo o art.º 6.º da Lei n.º 109/2009, consiste em "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". Atualmente, a par de outros crimes informáticos, regista-se um crescimento na prática deste crime, o qual inúmeras vezes constitui um *gateway crime* para outros tipos de crimes informáticos, demonstrando que o crime de acesso ilegítimo se pode propor a diversos alvos e a diversas finalidades.

Paralelamente, um fenómeno igualmente crescente é o da segurança informática ativa. Este fenómeno consiste em técnicas de segurança informática que, na decorrência de um ataque, se propõem não só a defender os sistemas que são alvo do ataque, mas também, a reagir, de forma proactiva,

obtendo até informações sobre o atacante ou eventualmente recolhendo provas. Não obstante, atualmente, há mesmo quem advogue a possibilidade de desencadear um "contra-ataque", de forma a aceder ao sistema informático do atacante, a intercetar os seus dados, ou até mesmo a afetar/danificar o mesmo (fenómeno este conhecido como *hack back*).

Assim, não só se impõe a análise de algumas destas técnicas informáticas, como também uma reflexão técnico-jurídica sobre a segurança informática ativa a fim de aqui se averiguar a relevância destes comportamentos ao nível da ilicitude e da culpa. Importa, por conseguinte, trazer à colação da investigação proposta, temas como o *hacking* (*lato* e *stricto sensu*), o "ciber(h)ativismo", o *hack-back*, os *pentests* efetuados por peritos em segurança informática e ainda o *backtrack*. Tais temas transportam, por vezes, certas dificuldades de compreensão, nomeadamente no que toca à classificação de determinados comportamentos (*v.g.*, na dicotomia *hacking vs* acesso ilegítimo) ou à solução jurídica que deverá ser aplicada quanto ao fenómeno do *hack-back*.

Ora, face ao crescimento de tais fenómenos, e à já aludida parca doutrina e jurisprudência que versam sobre os mesmos, a presente dissertação tem como objetivo primordial não só uma análise dogmática do crime de acesso ilegítimo, para dirimir dificuldades de compreensão deste tipo legal de crime, como também, demonstrar como estes fenómenos se efetivam na prática. Será ainda atribuído o devido destaque às diversas mudanças legislativas que ocorreram na classificação do tipo legal de crime do acesso ilegítimo com vista a uma melhor compreensão sobre este assunto.

Destarte, será fornecida na presente dissertação uma investigação de uma específica hipótese prática, de forma a ilustrar e a densificar o tema proposto, bem como, para aferir da relevância dos aludidos comportamentos ao nível da ilicitude ou da culpa. Tal desiderato implica, pois, uma análise que recairá, em traços gerais, sobre a hipótese em que o acesso não autorizado é praticado como reação a um ataque informático (referimo-nos, pois, ao *hack back*).

Neste caso, atendendo à inerente motivação do contra-ataque, que poderá ser eventualmente a de acautelar um bem jurídico superior aos protegidos pela norma do art.º 6.º da Lei n.º 109/2009 ou até mesmo quando o facto típico é praticado sem consciência da respetiva ilicitude, importa desde logo o estudo do eventual recurso às causas de justificação e de exculpação e a respetiva análise dos seus elementos, tendo em vista fornecer um contributo para a compreensão das causas de exclusão da ilicitude e da culpa no crime informático de acesso ilegítimo.

CAPÍTULO I - O CRIME DE ACESSO ILEGÍTIMO - ENQUADRAMENTO (HISTÓRICO E DOGMÁTICO)

1. Fontes e evolução histórica

No seguimento da Recomendação 9/89 do Conselho Europeu[2], o ordenamento jurídico português foi pioneiro em prever e punir os ilícitos cometidos com recurso às tecnologias de informação e comunicação[3], através da Lei n.º 109/1991, de 17 de Julho (Lei da Criminalidade Informática)[4]. Apesar deste marco temporal nos parecer longínquo ou remoto, a verdade é que o uso da Internet e de tais tecnologias era já algo bastante recorrente, o que naturalmente potenciou o crescimento acentuado da criminalidade informática – pelo que tal fenómeno não é tão recente quanto se julga.

Nesse sentido, cumpre referir, o crime de acesso ilegítimo - vetor da presente dissertação - foi também um dos primeiros fenómenos[5] de criminalidade informática a surgir no panorama informático-penal e é ainda um dos mais emblemáticos crimes nesse mesmo plano, talvez pelo espírito ("demasiado") curioso inerente à personalidade humana em descobrir aquilo que é oculto. Um dos primeiros agentes a ser condenado por este tipo de ilícito (que nos E.U.A. se denomina *Illegal Access*) terá sido Ian Murphy (conhecido como *Captain Zap*), por ter acedido ilegitimamente aos sistemas informáticos da *AT&T´s* em 1981. Seguir-se-iam outros casos, tais como o do grupo dos *414´s*, um grupo de jovens delinquentes que em 1983 acedeu ilegitimamente aos sistemas informáticos do *Los Alamos National Laboratory*, do *Sloan-Kettering Cancer Center*, e do *Security Pacific Bank* e cujos membros viriam a ser condenados pela justiça norte-americana*,* o de Kevin Mitnick, também condenado em 1988 por, entre outras coisas, aceder a sistemas informáticos empresariais (e cuja atividade criminosa serviu inclusive de base para a

[2] *Vide* EUROPEAN COMMITTEE ON CRIME PROBLEMS AND COUNCIL OF EUROPE, *Computer-related Crime: Recommendation No. R. (89) 9 on Computer-related Crime and Final Report of the European Committee on Crime Problems*, Council of Europe, Pub., 1990, disponível em: http://www.oas.org/juridico/english/89-9&final%20Report.pdf, consultado a 15 de Setembro de 2014.

[3] A propósito da criminalidade informática (e atento o intuito criminoso convencional que preside neste tipo de ilícitos), esta pode ser caracterizada como "old wine in new bottles" – cf. GRABOSKY, P.: "Virtual Criminality: Old Wine in New Bottles?*",* SLS, núm. 10, 2001, p. 243.

[4] Disponível em: http://www.cnpd.pt/bin/legis/nacional/lei_10991.htm, consultado a 15 de Setembro de 2014.

[5] *Vide* TRIGAUX, Robert, "A history of hacking", disponível em: http://www.sptimes.com/Hackers/history.hacking.html, consultado a 10 de Junho de 2015.

produção cinematográfica *Hackers 2*) e ainda o caso do jovem Julian Assange, que em 1995 se declarou culpado de 24 acusações pela prática do crime acesso ilegítimo[6].

Ora, a par da cobertura mediática dada aos casos referidos, um fator que largamente aumentou a visibilidade do fenómeno da criminalidade informática foi o lançamento do filme *War Games*, no qual é feita a alusão a um jovem adolescente que, com o intuito de descobrir novos videojogos, descobre acidentalmente o acesso (remoto) a um sistema militar que detém o controlo do lançamento de mísseis balísticos intercontinentais dos E.U.A. e acaba por causar um incidente que coloca o mundo à beira de uma guerra nuclear – gerando consequentemente um temor generalizado na sociedade das eventuais capacidades técnicas dos delinquentes informáticos para colocar o mundo em tal cenário. Em razão dessas circunstâncias, a sociedade (e os jovens em especial) tomou então conhecimento da prática crescente de crimes informáticos, e conjuntamente com a proliferação do uso dos computadores e do acesso à internet, o número de adolescentes a praticar o crime de acesso ilegítimo a sistemas informáticos cresceu exponencialmente. Os novos ataques informáticos renovaram o frenesim mediático (gerando uma espécie de ciclo vicioso), e elevaram os agentes da criminalidade informática ao estrelato. Nesta sequência, surge em 1984 o *Comprehensive Crime Control Act*, o qual continha entre as suas normas o *Counterfeit Acess Device and Computer Fraud and Abuse Act*[7] – cujas provisões foram pioneiras (embora limitadas), em combater e punir a criminalidade informática nos E.U.A.

Mais tarde, também o Conselho Europeu, motivado pelo acentuado crescimento da prática de crimes informáticos, pelo seu carácter transfronteiriço e pela consequente necessidade de uma resposta rápida e adequada ao problema, viria a elaborar a Recomendação 9/89, com vista à harmonização do direito interno comunitário e promoção da cooperação judiciária nessa matéria, recomendando os Estados-Membros a legislar em matéria de criminalidade informática, seguindo o relatório sobre criminalidade

[6] *Vide* LEIGH, David e HARDING, Luke, "Julian Assange: the teen hacker who became insurgent in information war", disponível em: http://www.theguardian.com/media/2011/jan/30/julian-assange-wikileaks-profile, consultado a 10 de Junho de 2015.
[7] *Vide Comprehensive Crime Control Act,* disponível em: https://www.ncjrs.gov/pdffiles1/Digitization/123365NCJRS.pdf, consultado a 11 de Junho de 2015.

informática elaborado pelo Comité Europeu para os Problemas Criminais do Conselho da Europa.

No mencionado relatório constava um catálogo com um conjunto mínimo de crimes a prever e punir, entre os quais figurava o crime de "acesso não autorizado", sugerindo como tipo legal "o acesso ilícito a um sistema informático ou rede através da violação de medidas de segurança"[8]. O mesmo relatório explicitava que o interesse ou bem jurídico a proteger seria, em primeira linha, o da segurança dos sistemas informáticos, consagrando assim a inviolabilidade do domicílio informático[9], mas também sugeria como alternativa, no sentido de qualificar o ilícito, a restrição da aplicação a critérios subjetivos relacionados com a conduta do agente (intenções desonestas ou danosas).

Por essa via, o ordenamento jurídico português também não ficou indiferente ao fenómeno da criminalidade informática e viria a adotar as recomendações europeias. A Assembleia da República Portuguesa concebeu então a denominada Lei da Criminalidade Informática (Lei n.º 109/91, que vigorou até 2009), a qual previu e puniu (entre outros) o crime de acesso ilegítimo, no seu art.º 7.º - precisamente de forma a proteger os sistemas ou redes informáticos - e o qual abaixo se reproduz:

1- Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

2- A pena será a de prisão até três anos ou multa se o acesso for conseguido através de violação de regras de segurança.

3- A pena será a de prisão de um a cinco anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei;

b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

4- A tentativa é punível.

5- Nos casos previstos nos nºs 1, 2 e 4 o procedimento penal depende de queixa.

[8] Tradução nossa do texto original: "The access without right to a computer system or network by infringing security measures", disponível em: http://www.oas.org/juridico/english/89-9&final%20Report.pdf, p. 51, consultado a 12 de Junho de 2015.

[9] Algo que encontra um certo paralelismo (ainda que rudimentar) com a violação do direito de propriedade (art.º 62.º da C.R.P.) e do direito à reserva da intimidade da vida privada (art.º 26.º n.º 1 da C.R.P. e art.º 80.º do C.C.), mas também com a violação do princípio da inviolabilidade do domicílio e da correspondência (art.º 34.º da C.R.P.)

Analisando de perto a norma - e em específico o seu n.º 1 - podemos observar que esta contempla um elemento objetivo e um elemento subjetivo. Quanto ao elemento objetivo, concordamos com a opinião de PEDRO VERDELHO, o qual afirma que o elemento objetivo do tipo contido na norma "é preenchido por qualquer ato que permita ao agente aceder a um sistema ou rede informática (…)"[10]. Relativamente ao elemento subjetivo ("intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos") seguimos o entendimento perfilhado por GARCIA MARQUES e LOURENÇO MARTINS[11]: este elemento exige que a própria ação seja dolosa e, por sua vez, que a negligência seja um fator de exclusão da punição. Assim, a todo o momento seria fundamental aferir a motivação do agente que acedeu ilegitimamente a um sistema informático e o resultado de tal acesso – na medida em que, só havendo um benefício ou uma vantagem ilegítima, poderia então haver lugar à punição do agente. Ademais, as vantagens ou benefícios não teriam de ser entendidos num sentido económico/patrimonial mas antes num sentido jurídico, conforme defende BENJAMIM SILVA RODRIGUES[12]. Naturalmente que a presença de tal elemento subjetivo, dificultou a condenação pelo crime de acesso ilegítimo - conforme a jurisprudência o demonstrou[13] -, porque não raras vezes o agente do acesso ilegítimo pratica tal ilícito por mera diversão, visando o auto-engrandecimento pessoal, glorificando as suas capacidades técnicas, aptas a violar regras de segurança informática e a aceder de forma não-autorizada com sucesso a um sistema informático, e nem por isso implicando necessariamente qualquer benefício ou vantagem tutelados pela norma em apreço. Igualmente, o próprio prejuízo emergente do acesso ilegítimo não está contemplado na norma[14]. Destarte, o art.º 7.º da pretérita Lei da Criminalidade Informática conferia uma tutela extremamente restrita face ao crime de acesso ilegítimo, algo que no nosso entender impunha

[10] Cf. VERDELHO, Pedro, «Cibercrime», in *Direito da Sociedade da Informação* IV (sem data), p. 366.
[11] Tal como defendido por MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática,* Coimbra, Almedina, 2006.
[12] Cf. RODRIGUES, Benjamim Silva, *Da Prova Penal, Tomo IV (Da Prova – Electrónico-Digital e da Criminalidade Informático-Digital)*, Lisboa: Rei dos Livros, 2011, p. 159.
[13] *Vide* Acórdão da 9.ª Vara Criminal de Lisboa, de 19-06-1997, 3.ª Secção, Processo 1/97, *in* ROCHA, Manuel Lopes, *Direito da Informática nos Tribunais Portugueses (1990-1998)*, Centro Atlântico, pp. 17-26 e Acórdão do Tribunal da Relação do Porto, de 08-01-2014, Processo n.º 1170/09.8JAPRT.P2, disponível em: http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/b54faf2d4330b8d480257c6e004ff2df?OpenDocument consultado a 15 de Junho de 2015.
[14] Cf. MARQUES, Garcia e MARTINS, Lourenço, *Direito da Informática*, Almedina, 2006, pág. 529.

um grave sacrifício do bem jurídico em causa – o da inviolabilidade dos sistemas informáticos – questão que analisaremos posteriormente[15].

Ainda sobre as restantes previsões da norma em apreço, cumpre também adiantar algumas (breves) considerações. Os n.ºs 2 e 3 da norma constituem qualificações que acarretam o agravamento da moldura abstrata aplicável ao crime de acesso ilegítimo, isto é, são previstas circunstâncias em que o juízo de censura a emitir sobre uma conduta concreta deve ser mais intensificado. Em termos de prevenção, a conduta que o n.º 2 pune tem por base a exigência de ser restabelecida a confiança comunitária nas tecnologias e nos respetivos mecanismos de segurança (*passwords*, *firewalls*, *pins*, etc.). Em termos de reação estatal, a norma tem por objetivo alcançar uma punição mais acentuada do acesso ilegítimo, que implicou a violação das regras de segurança (sinal de um maior desrespeito do agente pela reserva da vida privada e pela inviolabilidade dos sistemas informáticos). Quanto ao n.º 3, se através do acesso ilegítimo se tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais [al. a)], ou obtiver benefício ou vantagem patrimonial de valor consideravelmente elevado [al. b)] (excedendo assim as 200 Unidades de Conta) a pena será a de prisão de um a cinco anos. Quanto a este preceito, diga-se, a doutrina[16] avançou algumas críticas bastante pertinentes, pois a norma não terá sido redigida de acordo com o art.º 202.º do C.P. Relativamente ao n.º 4, a norma previa a punição da tentativa, algo que se afigura coerente, pois o crime de acesso ilegítimo, mesmo na sua forma tentada, deve também ser punido, precisamente porque o bem inviolabilidade do sistema informático poderia ter sido posto em causa. Relativamente ao último número da norma (n.º 5), este determina o crime de acesso ilegítimo quanto à sua natureza[17] e qual será o procedimento para promover a investigação de tal ilícito.

Decorridos dez anos da entrada em vigor da Lei da Criminalidade Informática, e face à evolução das técnicas e tecnologias informáticas, tomaria

[15] P. 18.
[16] Cf. FREITAS, Pedro, "Breves nótulas sobre o crime de acesso ilegítimo previsto na Lei do Cibercrime" (artigo apresentado no IV Simpósio de Segurança Informática e Cibercrime, Instituto Politécnico de Beja, 2013).
[17] Crime de natureza semipúblico nas circunstâncias previstas no n.º 1, 2 e 4, cujo procedimento está previsto no art.º 113.º do C.P.; Crime público nas circunstâncias previstas no n.º 3, o que significa que o procedimento criminal inicia-se mesmo sem a queixa do ofendido.

lugar, em Budapeste, a Convenção sobre o Cibercrime[18], a qual seria adotada a 23 de Novembro de 2001. Foi uma iniciativa político-criminal fundamental, constituindo o primeiro tratado internacional em termos de previsão, combate e sancionamento da criminalidade informática a nível mundial. Neste sentido, ROGÉRIO BRAVO descreve, de forma admirável, a Convenção sobre o Cibercrime como "(…) um princípio orientador com vista à criação de legislação nacional e dirige-se a um mundo dito virtual, sendo que os seus efeitos no ordenamento interno poderão ser comparados aos de um upgrade. (…) Acreditamos que com a CiberConvenção o objectivo pretendido seja o de proceder a um upgrade, ou seja, não tanto uma revisão de source code de alguns dos preceitos eventualmente em vigor na maioria dos países que assinaram aquele tratado, mas uma autêntica release, uma versão nova, baseada numa versão mais antiga e testada. Trata-se de uma mudança que afecta o trabalho em rede, conforme as limitações e a largura de banda posta à disposição do sistema servidor"[19].

Debruçando-nos um pouco sobre a Convenção, vislumbramos três grandes vertentes: Direito Penal Material, Direito Processual e Cooperação Internacional. Ademais, tal como exposto no seu preâmbulo[20], a Convenção tem por objetivo a harmonização de todas as legislações dos Estados signatários (que é o caso da República Portuguesa) de modo a que estes tomem medidas para prevenir e combater a criminalidade informática (em especial, os atos praticados contra a confidencialidade, integridade e disponibilidade dos sistemas, redes e dados informáticos), prevendo e punindo os comportamentos aludidos na Convenção, mas também para desenvolverem mecanismos de deteção de combate à criminalidade informática, de modo a

[18] Também conhecida como Convenção de Budapeste, atento o local da sua realização. Disponível in: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese.pdf, consultado a 15 de Junho de 2015.

[19] Cf. BRAVO, Rogério "O Crime de acesso ilegítimo na Lei da Criminalidade Informática e na Ciberconvenção" in *Direito na Rede n.º 1* [*on-line*], Ordem dos Advogados, Lisboa, 2004, disponível em: http://www.academia.edu/2039178/O_Crime_de_Acesso_Ilegi_timo_na_Lei_da_Criminalidade_Informa_tica_e_na_CiberConvenc_a_o, consultado a 15 de Março de 2014.

[20] Nos seus precisos termos: "(…) a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados, prevendo a criminalização desses comportamentos, tal como se encontram descritos na presente Convenção, e a criação de competências suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e a acção penal relativamente às referidas infracções, tanto ao nível nacional como ao nível internacional, e adoptando medidas que visem uma cooperação internacional rápida e fiável".

facilitar a deteção, investigação e ação penal mas também a cooperação internacional em matéria de investigação de tal fenómeno.

Ora, no que diz respeito ao acesso ilegítimo, este surge, destacado diga-se, no Capítulo II, Secção 1, Título I ("Infracções contra a confidencialidade, integridade e disponibilidade dos sistemas informáticos e dados informáticos") da Convenção, que no seu art.º 2.º refere: "Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticado intencionalmente, o acesso ilícito a um sistema informático no seu todo ou a parte dele. Para que se verifique a infracção penal, qualquer uma das Partes pode exigir que ela seja cometida por meio da violação das medidas de segurança com intenção de obter dados informáticos ou com qualquer outra intenção, ou ainda que esteja relacionada com um sistema informático conectado a outro sistema informático"[21].

Destarte, cumpre desde já referir que as partes signatárias da Convenção obrigaram-se[22] a criar mecanismos de combate e sancionamento dos agentes do crime de acesso ilegítimo – algo de que o nosso ordenamento jurídico estaria já aprovisionado, através da Lei n.º 109/91. As inovações que entendemos merecerem destaque na Convenção (em relação ao já aludido Relatório do Comité Europeu para os Problemas Criminais do Conselho da Europa), para além das alterações de ordem sistemática, são as abaixo explicitadas:

É exortada a punição do "acesso ilícito a um sistema informático no seu todo ou a parte dele" ao invés da punição do "acesso ilícito a um sistema informático ou rede através da violação de medidas de segurança" – o que significa que o núcleo de proteção é o acesso intencional e ilegítimo à totalidade ou parte do sistema informático. Consequentemente, é alargado o âmbito da punição e bem assim, é conferida a possibilidade aos Estados signatários de punir o acesso ilegítimo mesmo sendo este praticado sem a violação de medidas de segurança (o que na prática jurídico-penal constitui um avanço, pois nem sempre o acesso ilegítimo se realiza mediante a violação de

[21] (Sublinhado nosso)
[22] "Deverá"

regras de segurança – como sucede, *v.g.*, quando existe um acesso físico do agente a um computador[23]). Aliás, verifica-se também que a Convenção deixa à consideração dos Estados signatários a consagração de elementos tipificadores subjetivos do acesso ilegítimo (nomeadamente a intenção de obter dados informáticos ou outras intenções ilegítimas, ou também a existência de um sistema informático conectado a outro sistema informático) contrariando assim a lógica do art.º 7.º da Lei da Criminalidade Informática, o que acabou por originar alterações na previsão e punição de tal ilícito no ordenamento jurídico português, tal como se demonstrará[24].

Mesmo no tocante à punibilidade da tentativa do crime de acesso ilegítimo, nada é referido na Convenção, pelo que se presume que também a sua consagração fica sujeita à discricionariedade dos Estados Signatários. Por fim, surge também na Convenção, no seu art.º 6.º, a punição do "uso abusivo de dispositivos" – tal significa que os Estados signatários obrigam-se a legislar tendo em vista a tipificação como infrações penais "a produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de (…) um dispositivo, incluindo um programa informático, essencialmente concebido ou adaptado para permitir a prática de uma das infrações previstas nos artigos 2º a 5º da presente Convenção ou de uma palavra-passe, um código de acesso, ou dados similares que permitam o acesso a todo ou a parte de um sistema informático, visando a sua utilização na prática de qualquer uma das infrações previstas nos artigos 2º a 5º da presente Convenção". Em suma, a Convenção obriga as partes a punir qualquer forma de disponibilização de dispositivos, programas informáticos bem como palavras passes, códigos de acesso ou dados similares aptos à realização do crime de acesso ilegítimo. Tal comando implicaria alterações na Lei Portuguesa, como também se demonstrará[25].

Cumpre ainda referir, conforme a construtiva crítica avançada por PEDRO FREITAS, que denota-se uma certa indeterminação no que toca à

[23] *Vide* parágrafo 50 do Relatório Justificativo da Convenção sobre o Cibercrime.
[24] P. 15 e ss.
[25] P. 15 e ss.

concretização do bem legalmente protegido[26] na Convenção do Cibercrime. De facto, apesar do crime de acesso ilegítimo estar inserido no âmbito das infrações contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos[27], inexiste uma definição do bem jurídico aí em causa. Nas palavras do referido Autor: "Poder-se-ia dizer que este passo dado pela Convenção é pois benéfico por auxiliar na tarefa de delimitação do bem jurídico tutelado. Mas seria uma conclusão precipitada. Na verdade, a conclusão deverá ser outra, sobretudo se se puser em causa a relação de tutela das normas penais propostas na Convenção com o conjunto dos bens jurídicos mencionados no referido título 1, isto é, se se puser em crise a ideia de que cada uma das condutas descritas visa proteger simultaneamente a confidencialidade, a integridade e a disponibilidade de sistemas informáticos e dados informatizados. A ser assim, não poderia ser outra a conclusão que, apesar de haver um esforço de delimitação, de entre a panóplia de bens jurídicos tutelados e/ou tuteláveis pelo direito penal, não estaria atingido o grau suficiente de concreção e materialidade do bem jurídico tutelado exigível para que possa dar por legitimada a intervenção penal"[28] – algo com o que concordamos plenamente, embora o mesmo Autor forneça também, em forma de esclarecimento, o texto plasmado no parágrafo 44 do Relatório Justificativo da Convenção sobre Cibercrime[29] que refere: "O termo "Acesso ilícito" abrange basicamente a infracção relativa às perigosas ameaças e atentados à segurança (isto é, confidencialidade, integridade e disponibilidade) dos sistemas informáticos e dados informatizados. A necessidade de protecção reflete os interesses de organizações e indivíduos em gerir, operar e controlar os seus sistemas de forma livre e tranquila". Analisaremos este assunto posteriormente, no tópico "Acesso ilegítimo no presente - análise dogmática"[30].

Mais tarde, e na sequência da Convenção sobre o Cibercrime, o Conselho da União Europeia viria também a emitir a Decisão-Quadro

[26] *I.e.*, bem jurídico, que é a "(…) expressão de um interesse da pessoa ou da comunidade, na manutenção ou integridade de um certo estado, objecto ou bem em si mesmo socialmente relevante e por isso juridicamente reconhecido como valioso" cf. DIAS, DIAS, Jorge de Figueiredo, *Direito Penal, Parte Geral, Tomo I*, Coimbra, 2.ª ed., 2007, p. 114.
[27] *Vide* Capítulo II, Secção 1, Título I da Convenção do Cibercrime.
[28] Cf. FREITAS, Pedro, *op. cit.;* (sublinhado nosso).
[29] Relatório Justificativo da Convenção sobre Cibercrime (versão portuguesa) disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_Portugese-ExpRep.pdf, consultado a 15 de Junho de 2015.
[30] P. 15 e ss.

2005/222/JAI do Conselho de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação[31] tendo em vista, entre outros considerandos, "reforçar a cooperação entre as autoridades judiciárias e outras autoridades competentes, nomeadamente as autoridades policiais e outros serviços especializados responsáveis pela aplicação da lei nos Estados-Membros, mediante uma aproximação das suas disposições de direito penal em matéria dos ataques contra os sistemas de informação". A decisão estatuiu também, desde logo, no seu art.º 2.º, sob a epígrafe "Acesso ilegal aos sistemas de informação" que "Os Estados-Membros devem tomar as medidas necessárias para assegurar que o acesso intencional, não autorizado, à totalidade ou a parte de um sistema de informação seja punível como infracção penal, pelo menos nos casos que não sejam de menor gravidade" mas também que "Os Estados-Membros podem decidir que os comportamentos referidos no n.º 1 são puníveis apenas quando a infracção tiver sido cometida em violação de uma medida de segurança." Tal faculdade dada aos Estados-Membros, segue a lógica do estatuído na Convenção sobre o Cibercrime i.e., que os Estados-Membros poderão punir o acesso ilegítimo mesmo sendo este praticado sem a violação de medidas de segurança, embora pareça aqui conceder alguma margem para classificar ou não como ilícitos os acessos ilegítimos de menor gravidade.

Acresce ainda que a Decisão, no seu art.º 7.º, sob a epígrafe "Circunstâncias agravantes", dispõe que "Cada Estado-Membro deve tomar as medidas necessárias para assegurar que a infracção referida no n.o 2 do artigo 2.o e as referidas nos artigos 3.o e 4.o sejam passíveis de pena privativa de liberdade com duração máxima de, pelo menos, dois a cinco anos quando forem praticadas no âmbito de uma organização criminosa, tal como definida na Acção Comum 98/733/JAI, independentemente do nível da pena nesta referido" e ainda que "Um Estado-Membro pode também tomar as medidas a que se refere o n.º 1 nos casos em que a infracção em causa tenha causado danos graves ou lesado interesses essenciais". Tal disposição indica que o crime de acesso ilegítimo deve ser mais severamente punido no caso de o

[31] Disponível em: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:PT:HTML#ntr1-L_2005069PT.01006701-E0001, consultado a 15 de Junho de 2015.

mesmo ser praticado no âmbito de uma organização criminosa e ainda que, no caso de dano grave ou lesão de interesses essenciais derivados do acesso ilegítimo, os limites da moldura penal podem ser também aumentados, o que significa que estes elementos tipificadores subjetivos, pelo menos no que diz respeito aos interesses essenciais, surgem agora como circunstâncias modificativas agravantes.

Em 2009, e por força da Convenção sobre o Cibercrime e da Decisão-Quadro 2005/222/JAI, o Legislador Português viria a elaborar um novo diploma (Lei n.º 109/2009, de 15 de Setembro[32]) para prever e punir a criminalidade informática, intitulado Lei do Cibercrime, que revogou expressamente a Lei n.º 109/91, de 17 de Agosto (Lei da Criminalidade Informática). Tal diploma é o que nos dias de hoje regula a matéria da criminalidade informática no ordenamento jurídico português. Aqui chegados, cumpre então analisar mais profundamente a previsão e punição do crime de acesso ilegítimo no presente.

2. Acesso ilegítimo no presente – Análise dogmática

Na Lei do Cibercrime, é o art.º 6.º que se ocupa do crime de acesso ilegítimo. Tal preceito manteve parcialmente a estrutura do art.º 7.º da revogada Lei da Criminalidade Informática, contendo a seguinte redação:

1 - 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.

2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.

3 - A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.

4 - A pena é de prisão de 1 a 5 anos quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou

[32] Designação mais restritiva do que a anterior designação da lei; cf. Recomendação 9/89 do Conselho Europeu e Relatório sobre criminalidade informática, elaborado pelo Comité Europeu para os Problemas Criminais do Conselho da Europa (língua inglesa), disponível em: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis, consultado a 15 de Junho de 2015.

b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

5 - A tentativa é punível, salvo nos casos previstos no n.º 2.

6 - Nos casos previstos nos n.os 1, 3 e 5 o procedimento penal depende de queixa.

Em primeiro lugar, urge desde já explicitar o objeto da ação no crime de acesso ilegítimo, que será o próprio sistema informático e cuja definição está presente na alínea a) do art.º 2.º da Lei do Cibercrime, designadamente: "qualquer dispositivo ou conjunto de dispositivos interligados ou associados, em que um ou mais de entre eles desenvolve, em execução de um programa, o tratamento automatizado de dados informáticos, bem como a rede que suporta a comunicação entre eles e o conjunto de dados informáticos armazenados, tratados, recuperados ou transmitidos por aquele ou aqueles dispositivos, tendo em vista o seu funcionamento, utilização, protecção e manutenção". Está bom de ver que foi suprimido da norma o conceito de rede informática anteriormente previsto na Lei n.º 109/91 e, simultaneamente, o conceito de sistema informático contém agora um teor bem mais amplo do que aquele que constava na Lei n.º 109/91, abarcando assim outras tecnologias como os *smartphones*, que detêm já capacidades idênticas às de um computador (enquanto que na Lei da Criminalidade Informática o sistema informático era tão somente "um conjunto constituído por um ou mais computadores, equipamento periférico e suporte lógico que assegura o processamento de dados"[33])[34]. Assim, e para efeitos de caracterização do ilícito, atendendo ao facto que o "sistema informático" é objeto de proteção da norma, o crime de acesso ilegítimo será então um crime informático em sentido estrito.

Embora o Legislador Português mantenha no art.º 6.º a classificação da violação de regras de segurança como uma circunstância modificativa agravante[35] (no citado n.º 3) e não como um elemento objetivo tipificador (à semelhança do que sucedia na Lei da Criminalidade Informática) podemos

[33] Art.º 2.º, al. b), da Lei n.º 109/91, de 17 de agosto
[34] Sobre esta matéria, sugere-se a leitura do parágrafo 46 do Relatório Justificativo da Convenção sobre o Cibercrime.
[35] Como alude Maria João Antunes "A moldura penal resultante do preenchimento de determinado tipo legal de crime pode vir a ser modificada, por efeito das chamadas circunstâncias modificativas, agravantes ou atenuantes. (…)". Quanto às circunstâncias modificativas agravantes, a Autora define-as como aquelas que "alteram a moldura penal, elevando-a num dos limites ou nos limites mínimo e máximo" cf. ANTUNES, Maria João*, Consequências jurídicas do crime,* 1.ª ed., Coimbra Editora, 2013, p. 39.

ainda assim constatar que houve uma modificação profunda na descrição do tipo legal do crime de acesso ilegítimo. O Legislador Português decidiu então seguir a previsão mais restrita do ilícito dada pela Convenção sobre o Cibercrime e [talvez para apaziguar os conflitos na doutrina e jurisprudência pela ausência de punição do acesso ilegítimo praticado por mera "diversão" (sem a obtenção de qualquer vantagem ou benefício ilegítimo)] retirou o elemento tipificador subjetivo existente, *i.e.*, o n.º 1 do referido preceito não tipifica como elemento subjetivo a obtenção de qualquer benefício ou vantagens ilegítimas pelo agente. Com efeito, o âmbito de aplicação da norma foi deveras alargado, abarcando todo o acesso não autorizado a um sistema informático (seja o acesso a parte ou a todo o sistema), pelo que não se tem em consideração a intenção do agente – assim, para efeitos de caracterização da conduta típica punível, esta traduz-se no simples ato de aceder sem permissão legal ou autorização a um sistema informático[36] (só se exige portanto o chamado "dolo genérico"). Tal modificação legislativa também não está imune de críticas e neste sentido merece destaque a reserva de PEDRO DIAS VENÂNCIO, que tendo como referências os arts. 43.º e 73.º n.º 4 da C.R.P., expõe: "(…) [face] aos comportamento típicos da comunidade cibernautica, a punição do "acesso legítimo" nos casos de inexistência de um qualquer a dolo específico eticamente censurável para ir contra aquilo uma prática comummente aceite, e que para muito tem sido um factor de desenvolvimento tecnológico e crescimento da sociedade da informação que não pode ser descurado. Por outro lado, não se salvaguardando expressamente os actos que se insiram em actividade de ensino e investigação científica, a aplicação literal do texto legal, poderia levará penalização criminal da generalidade das práticas de ensino e investigação científica na área da segurança dos sistemas informáticos"[37].

[36] É o que sucede nas normas homólogas do ordenamento jurídico alemão (§ 202ª STGB) e do ordenamento jurídico francês (art.º 323.º n.º 1 do *Code Pénal*).

[37] Cf. VENÂNCIO, Pedro Dias, «O Crime de Acesso Ilegítimo», JusJornal, N.º 1179, 18 de Fevereiro de 2011, Editora Coimbra Editora, grupo Wolters Kluwer disponível em: http://jusjornal.wolterskluwer.pt/Content/Document.aspx?params=H4sIAAAAAAAAEAO29B2AcSZYlJi9tynt_SvVK1-B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVmVdZhZAzO2dvPfee--999577733ujudTif33_8_XGZkAWz2zkrayZ4hgKrIHz9-fB8_IorZ7LOnb3bk2Xtw8Asv87opquVnezu7OzsP9x7gg-L8-mk1fXO9yj87z8om_38A82aBqjUAAAA%3DWKE, consultado a 30 de Outubro de 2014

Quanto ao bem jurídico tutelado pelo art.º 6.º, diga-se que também aqui não há uma posição unânime. De entre as várias posições[38], seguimos a de PEDRO FREITAS que entende como matéria protegida a inviolabilidade dos sistemas informáticos. De facto, e segundo o Autor, será "o único bem jurídico capaz de congregar as incontáveis realidades sociais"[39], pois "Há um conjunto de bens jurídicos em relação aos quais o crime de acesso ilegítimo poderá funcionar como crime de perigo (eventualmente abstrato), antecipando assim a sua tutela penal: referimo-nos, desde logo, ao direito à privacidade, de um lado, e à segurança do sistema informático, de outro, embora pudéssemos a estes adicionar igualmente outros como o património, por exemplo. Mas não nos podemos olvidar as particulares aporias que se colocam ao enquadrar dogmaticamente esta incriminação legal no domínio dos crimes de perigo. Não só a definição concreta do interesse ou bem que se visa tutelar, mas também a circunstância de apenas se justificar (constitucionalmente) o seu uso quando se preencham dois requisitos adicionais, como o de se visar a tutela de bens jurídicos de importância significativa e a descrição típica da conduta seja o mais precisa e minuciosa possível, servem de pressupostos destinados a salvaguardar o respeito do princípio da legalidade e da culpa – traves-mestras do modelo político-criminal vigente nos Estados de Direito democrático. Assim somos a concluir, na falta de suficiente concreção da constelação de bens jurídicos que se colocam em perigo com o acesso ilegítimo a um sistema informático, ou dito de outra forma, perante o complexo heterogéneo de interesses que se candidatam à tutela penal, *v.g.* reserva da vida privada, segredo comercial, profissional, industrial ou dados confidenciais, segurança, entre outros, que apenas a "inviolabilidade dos sistemas informáticos" se prestará a revelar uma corporização material-teleológica dogmaticamente compatível com a função (ou funções) desempenhada(s) pelo bem jurídico".

Uma outra inovação presente no art.º 6.º é o seu n.º 2. Este preceito teve por base a orientação presente na Convenção sobre o Cibercrime, que no seu art.º 6.º incentiva à punição do "uso abusivo de dispositivos", *i.e.* (e como já referido) os Estados signatários obrigam-se a punir qualquer forma de disponibilização de dispositivos, programas informáticos bem como *passwords*,

[38] Para um melhor entendimento, cf. FREITAS, Pedro, *op. cit.*
[39] *Ibid.*

códigos de acesso ou dados similares aptos à realização do crime de acesso ilegítimo. Assim, o Legislador Português atuou em conformidade com a Convenção e decidiu também punir a difusão (produção, venda ou distribuição) de tais programas ou dados informáticos, por serem atos preparatórios para diferentes tipos de criminalidade informática, inclusive para a prática do crime de acesso ilegítimo. Estamos pois perante uma antecipação da tutela penal – pois estatui-se a incriminação de factos que pela sua natureza são atos preparatórios do crime – e, simultaneamente, perante uma consumpção impura, pois o ilícito previsto no n.º 2 é um meio para praticar outro ilícito, mas é aplicada a norma do crime-meio, porque o crime principal (n.º 1) – crime resultado – é consumido pelo crime meio.

Quanto aos números 3 e 4 do art.º em apreço, estamos perante formas qualificadas do crime de acesso ilegítimo (à semelhança do que sucedia na Lei da Criminalidade Informática, nos seus nºs. 2 e 3). O número 3 prevê o alargamento dos limites da moldura penal abstratamente aplicável (pena de prisão até 3 anos ou multa) caso o acesso ilegítimo tenha sido efetuado com violação das regras de segurança. Já a alínea a) do n.º 4 prevê um agravamento ainda mais substancial da moldura penal (pena de 1 a 5 anos de prisão) quando o agente "tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei" e na alínea b), quando "O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.", o que indica a especial censurabilidade destas condutas. Quanto a esta última disposição, PEDRO FREITAS bem salienta que "o legislador português (…) ao recorrer à formula "o benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado" estará a pressupor um *prius* ou condição básica anterior de obtenção de benefício ou vantagem, o que se revela duplamente errado: por um lado, no texto legal de 1991 não se exigia a obtenção de benefício ou vantagem para o preenchimento típico do n.º 1, o que por si já levava a considerar não aconselhável a tentativa de compatibilizar num só tipo de legal de crime uma estrutura típica de resultado cortado com uma qualificação própria de um crime de resultado, que acontecia, sublinhe-se, somente quando o valor fosse consideravelmente elevado; por outro lado, a redação atual do artigo 6.º, n.º 1, não exige qualquer

elemento subjetivo adicional para além do dolo do tipo, o que torna, no mínimo, estranha a opção legislativa de agravamento da moldura abstrata nos moldes em que o faz no número 4, al b), do mesmo artigo"[40].

Quanto ao n.º 5 do preceito analisado, este refere que a tentativa de acesso ilegítimo será punível, salvo nos casos do n.º 2 (difusão ou introdução em sistemas informáticos de dispositivos ou dados informáticos ali enumerados, aptos à execução do crime de acesso ilegítimo). Tal menção expressa da punibilidade da tentativa afastava o regime dos arts. 22.º e 23.º do Código Penal, o que implica - pelo menos quanto ao n.º 1 - que a tentativa da prática do "simples" acesso ilegítimo, não é punível.

Por último, em relação ao n.º 6, este também segue a lógica do n.º 5 da revogada Lei da Criminalidade Informática, pois caracteriza o crime de acesso ilegítimo como um crime de natureza semipúblico. Como tal, o procedimento[41] criminal iniciar-se-á com a queixa do ofendido no caso do acesso ilegítimo na sua forma simples (n.º 1), quando o acesso tenha sido cometido com violação das regras de segurança (n.º 3) ou na tentativa do acesso ilegítimo (n.º 5). No entanto, interpretando a norma apreende-se que o acesso ilegítimo cometido sob as formas qualificadas previstas no n.º 4, aí tal ilícito assumirá a natureza de crime público, pelo que o procedimento criminal iniciar-se-á mesmo sem a queixa do ofendido, o que se justifica pela necessidade da ação do Estado de reparar a lesão consumada, punindo, desta feita, a conduta especialmente censurável e reestabelecendo, a final, a confiança comunitária nos sistemas informáticos.

3. *Hack, Hacker* e *Hacking* – Análise conceptual

Tendo em vista uma melhor compreensão dos tópicos da presente dissertação, é imprescindível fornecer desde já uma breve clarificação dos conceitos de *hack* (ato), *hacker* (sujeito) e *hacking* (conduta). Conforme já aludido, o crime de acesso ilegítimo foi um dos primeiros fenómenos de criminalidade informática a surgir no panorama informático-penal. Naturalmente

[40] Cf. FREITAS, Pedro, *op. cit.,* p. 17.
[41] Procedimento esse previsto no art.º 113.º do C.P.

que o acesso informático (na sua forma ilícita) lança as suas raízes no acesso informático legítimo ou lícito. Mas mesmo o próprio acesso informático legítimo, por sua vez, tem a sua génese no surgimento das ferramentas informáticas, (em especial da programação computacional[42]) e, por via da criatividade e do engenho humano, desde logo foram concebidos através de tais ferramentas, de forma deliberada ou por mero acaso, verdadeiras "partidas" ou "truques" informáticos, entre os quais, o ato de aceder a um sistema informático, seja por via remota ou física. Destarte, embora a expressão *hack*, reporte-se na língua inglesa ao verbo *to hack*, que no seu sentido original significa cortar ou golpear[43], numa fase mais contemporânea e associado ao uso das tecnologias informáticas, o uso do termo *hack* tornou-se contudo recorrente para caracterizar partidas ou truques, convencionais ou informáticos, inofensivos ou danosos, praticados pelos alunos do *Massachusetts Institute of Technology* (*MIT*) na fase pioneira da programação (décadas de 1950 e 1960)[44]. Consequentemente, *hack* seria a descrição positiva empregue na habilidade em desenvolver soluções criativas e efetivas para problemas técnicos[45]. Ora, naturalmente que a utilização de tais "partidas" e "truques" rapidamente se tornou na base da ciência computacional, que através da tentativa e do erro desenvolveram inúmeras linguagens e técnicas informáticas, programas de computador, sistemas informáticos, etc., mas também, se tornaram vetores para o desenvolvimento da atividade criminosa dos delinquentes cibernéticos.

Face a esse circunstancialismo histórico, a expressão *hack*[46] também pode ser utilizada no sentido de caracterizar a reconfiguração ou reprogramação de um sistema informático, seja de forma autorizada ou não autorizada pelo seu proprietário ou administrador (conforme seja um sistema informático privado ou de livre acesso ao público). Essa mesma reconfiguração ou reprogramação pode simultaneamente ser uma simples correção ou até mesmo uma melhoria de um determinado problema computacional, ou então

[42] "Computer programming is a way of instructing electronic machines to perform tasks, solve problems and provide human interactivity" *cf.* BEBBINGTON, Shaun, "What is computer programming?", disponível em: http://yearofcodes.tumblr.com/what-is-programming, consultado a 2 de Julho de 2015.
[43] Noção disponível em: http://www.thefreedictionary.com/hack, consultado a 28 de Julho de 2015.
[44] *Vide* RAYMOND, Eric *et al.* "The Meaning of 'Hack'", disponível em: http://www.catb.org/jargon/html/meaning-of-hack.html, consultado a 31 de Maio de 2015 e PETERSON, Institute Historian T. F., *Hack, hacker, hacking; Hacking ethics*" *in Nightwork: a history of hacks and pranks at MIT (updated edition)*. Cambridge, Mass.: MIT Press, 2011, p. 6.
[45] YAR, Majid, *Cybercrime and Society*, SAGE Publications, 2013.
[46] "*Hack:* desenrascar*",* cf. ZÚQUETE, André*, Segurança em Redes Informáticas.* 3.ª ed., Lisboa: FCA - Editora de Informática, 2010*,* p. 9.

poderá ser uma solução mais "rústica" para o mesmo tipo de problema, como se de um "remendo" se tratasse. Além de que, *hack* é um termo também utilizado para descrever a modificação de um programa (ou até de um dispositivo) para conceder o acesso a recursos ou funções que não estariam acessíveis a quem pratica o *hack* em causa ou a um terceiro. Aliás, provavelmente aqui se encontra a base técnica para executar o *hack* enquanto ato ilícito (seja enquanto crime-meio ou crime-fim). No entanto, é preciso efetuar uma importante ressalva: é que o uso de tal termo, de forma pejorativa, *i.e.*, o uso do termo *hack* para caracterizar condutas criminógenas é erróneo, pois a utilização de *hacks* enquanto atos maliciosos era já outrora designado como *breaking*[47] - expressão que embora ainda seja utilizada para descrever tal fenómeno, atualmente se designa como *cracking*[48]. Posto isto, no panorama informático, *crack* não é mais que a modificação de *software* para remover ou desactivar funcionalidades que são consideradas indesejáveis pela pessoa que procede ao *cracking* de tal *software*, *v.g.*, proteções anti-cópia. O termo *crack* será assim o meio/ferramenta informática para atingir o fim de efetuar o *cracking* com sucesso do *software*. Esta imprecisão terminológica poderá ter sido potenciada em grande parte pelos *mass-media*, que falharam em entender a dicotomia *hack vs crack*. Certo é que esta imprecisão terminológica manteve-se até aos dias de hoje. Cumpre ainda referir que *hack* é uma expressão utilizada para designar a prática de fraude nos videojogos para atingir melhores *performances* ou resultados[49], o que geralmente acarreta apenas a expulsão da conta do utilizador do videojogo em questão. Também há quem utilize a expressão para caracterizar quer o acesso ilícito, quer a clonagem de um perfil pessoal, *v.g.*, numa rede social. Certo é que a definição de *hack* não é estanque, pois pode reportar-se a situações ou fenómenos ainda mais recentes[50]. Contudo, para os fins da presente investigação, utilizaremos a

[47] "The origin of the term probably lies in the activity burglars perform in the still of the nigh." cf. KEVELSON, Morton, "Isepic", *Ahoy!*, 1986, pp. 71–73, disponível em: https://archive.org/stream/Ahoy_Issue_22_1985-10_Ion_International_US#page/n71/mode/2up, consultado a 20 de Junho de 2015.

[48] Expressão que se reporta não só a ilícitos relacionados com o património "digital" (como a contrafação ou reprodução ilegítima de programa protegido) mas também a diferentes ilícitos informáticos, inclusive o crime de acesso ilegítimo, mas que é mais comumente associada aqueles.

[49] Usualmente também é utilizada a expressão *cheat* neste contexto.

[50] *V.g.:* http://legalhackers.org/, consultado a 20 de Março de 2015 e http://hackforchange.org/ consultado a 28 de Julho de 2015. Também neste sentido: LIU, Lily, "When Hacking Is Actually a Good Thing: The Civic Hacking Movement", disponível em: http://www.huffingtonpost.com/lily-liu/when-hacking-is-actually-_b_3697642.html, consultado a 23 de Fevereiro de 2015

expressão para descrever o ato de aceder a um sistema, seja de forma lícita ou ilícita.

Quanto ao termo *hacker*[51], em primeiro lugar torna-se pertinente atentar para o *Oxford Dictionary of Computing*[52], que disponibiliza duas definições do termo. Uma definição (mais recente e porventura atualista) define *hacker* como "uma pessoa que tenta violar a segurança de um sistema informático por acesso remoto, em especial tentando adivinhar ou obter uma *password*"[53]. Numa versão anterior, *hacker* caracterizava-se como "uma pessoa com um conhecimento instintivo que lhe permitia desenvolver *software* aparentemente por tentativa e erro"[54]. Também por esta via e segundo esta definição (e para os fins da presente dissertação), podemos apresentar como sinal distintivo na dicotomia *hacker* e *cracker*[55] as próprias intenções do agente, sendo aquele o que acede legitimamente a um sistema e este o que acede ilegitimamente a um sistema[56]. Enquanto o intuito dos *crackers* é sempre malicioso, o dos *hackers* poderá não o ser, pois em regra e tendo em conta a "ética *hacker*"[57], estes geralmente têm mais interesse em adquirir conhecimento acerca dos sistemas

[51] Quanto a esta clarificação terminológica, recomenda-se a leitura do artigo redigido por POPPI, Ricardo, "Internet e sua normatividade no contexto da cultura hacker", disponível em: http://www.arcos.org.br/artigos/internet-e-sua-normatividade-no-contexto-da-cultura-hacker/, consultado a 10 de Junho de 2015. Ademais, cumpre efetuar também uma referência ao célebre pioneiro da ciência computacional, Ken Thompson e à palestra por si proferida na entrega do *Turing Award* em 1983. Em tal exposição ("Reflections on Trusting Trust"), o Investigador elabora uma alusão ao *hacking*, descrevendo uma vulnerabilidade de segurança (ou *exploit*) o qual denomina de *Trojan horse* (um conhecido tipo de *backdoor attack*). Ademais, Ken Thompson faz uma notável consideração acerca dos denominados *hackers*, que desde já se reproduz: "After trying to convince you that I cannot be trusted, I wish to moralize. I would like to criticize the press in its handling of the "hackers," the 414 gang, the Dalton gang, etc. The acts performed by these kids are vandalism at best and probably trespass and theft at worst. It is only the inadequacy of the criminal code that saves the hackers from very serious prosecution. The companies that are vulnerable to this activity, (and most large companies are very vulnerable) are pressing hard to update the criminal code. Unauthorized access to computer systems is already a serious crime in a few states and is currently being addressed in many more state legislatures as well as Congress. There is an explosive situation brewing. On the one hand, the press, television, and movies make heroes of vandals by calling them whiz kids. On the other hand, the acts performed by these kids will soon be punishable by years in prison. I have watched kids testifying before Congress. It is clear that they are completely unaware of the seriousness of theft acts. There is obviously a cultural gap. The act of breaking into a computer system has to have the same social stigma as breaking into a neighbor's house. It should not matter that the neighbor's door is unlocked. The press must learn that misguided use of a computer is no more amazing", cf. THOMPSON, Ken "Reflections on Trusting Trust", disponível em: https://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf, consultado a 28 de Julho de 2015.

[52] *Vide* DAINTITH, John e WRIGHT, Edmund (eds), *A Dictionary of Computing*, 6.ª ed., 2010, p. 227.

[53] Tradução nossa do texto original "a person who attempts to breach the security of a computer system by access from a remote point, especially by guessing or otherwise obtaining a password", *Ibid.*

[54] Tradução nossa do texto original "a person who had an instinctive knowledge enabling him or her to develop software apparently by trial and error", noção disponível em http://www.oxfordreference.com/view/10.1093/oi/authority.20110803095914534, consultado a 23 de Outubro de 2015.

[55] Quanto a este termo, veja-se a definição de *cracking* proposta por Ralph D. Clifford : "gain unauthorized access to a computer in order to commit another crime such as destroying information contained in that system", cf. CLIFFORD, Ralph D., *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime*, 3.ª Ed., Carolina Academic Press, 2011.

[56] *Vide* STAMATELLOS, Giannis, *Computer Ethics: A Global Perspective,* Jones and Bartlett Publishers, 2007, pp 16-17.

[57] *Vide* HIMANEN, Pekka, *The Hacker Ethic and the Spirit of the Information Age*, Nova York, Random House, 2001 e SCOTT, Brett, "The hacker hacked", disponível em: http://aeon.co/magazine/technology/how-yuppies-hacked-the-original-hacker-ethos/, consultado a 24 de Outubro de 2015.

computacionais e usar tal conhecimento no domínio da segurança informática[58] ou *quid sapit*, para brincadeiras desmaliciosas. Deste modo, o termo *hacker*[59] nem sempre será pejorativo, pois poder-se-á referir a um programador talentoso ou um perito em segurança informática enquanto *cracker* é alguém que, através do acesso ilegítimo ou outro tipo de ilícito informático, almeja um propósito verdadeiramente malicioso. Diga-se contudo que tais sujeitos envolvidos neste tipo de atividade (*hacking*) não possuem necessariamente uma elevada capacidade técnica[60]. Para os objetivos da presente dissertação, *hacker* será o indivíduo que usa *hacks* para aceder a um sistema informático, seja de forma legítima ou ilegítima (*i.e.*, utilizaremos a caracterização de *hacker* em sentido amplo[61]).

Também neste sentido[62] vai JOSÉ ANTÓNIO ALVES DE MATOS, o qual expõe: "Hacker - Comum e erradamente confundido com pirata informático, o hacker é um indivíduo cuja paixão é a de explorar todos os detalhes de vários sistemas. Os hackers informáticos são normalmente considerados peritos naquilo que fazem. Entusiasmam-se com todo o trabalho que se apresente como um desafio intelectual, como quebrar códigos ou entrar em sítios considerados de alta segurança. Embora a sua conotação social-cibernética seja de marginalização, os hackers regem-se por rígidos códigos de ética, cujas directrizes apontam para a não utilização das informações conhecidas para proveito próprio ou para prejudicar alguém. O verdadeiro hacker apenas utiliza os seus conhecimentos para demonstrar que existem lacunas nos programas e nos sistemas de segurança considerados infalíveis. A primeira linha de conduta de um hacker é: "vê tudo. Aprende tudo. Não alteres nada"[63].

---

[58] Exemplos de *websites* e/ou empresas que se dedicam a esse fim: https://www.hacking-lab.com/index.html, consultado a 28 de Julho de 2015, https://www.securizame.com/, consultado a 28 de Julho de 2015 e http://www.eccouncil.org/, consultado a 28 de Julho de 2015.

[59] "*hacker:* sujeito desenrascado e habilidoso*",* cf. ZÚQUETE, André*, op. cit.,* p. 9.

[60] Caso dos *script kiddies*, que analisaremos posteriormente (p. 28).

[61] Pois entendemos que o conceito de *hackers* em sentido estrito exclui os *crackers*, agentes envolvidos na prática de crimes informáticos.

[62] Traz-se aqui à colação também a seguinte definição, que se afigura bastante pertinente: "A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s). Among professional programmers, depending on how it used, the term can be either complimentary or derogatory, although it is developing an increasingly derogatory connotation. The pejorative sense of *hacker* is becoming more prominent largely because the popular press has coopted the term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is cracker" – Definição disponível em: http://www.webopedia.com/TERM/H/hacker.html, consultado a 20 de Março de 2015.

[63] MATOS, José António Alves de, *Dicionário de Informática e Novas Tecnologias*, FCA – Editora de Informática, Lisboa, 2009, p. 173.

Seguindo a mesma esteira, existe, no nosso entendimento, uma necessidade – vital – de averiguar o real intuito do *hacker*[64] para perceber se estamos perante *hacking* ou *cracking*, pois, como demonstrado, *hacking* poderá não envolver necessariamente um intuito malicioso ou ilícito, enquanto *cracking* sempre o envolverá. Assim, e quanto à definição do termo *hacking*[65], é importante referir que este é um conceito notoriamente mais denso do que o conceito de acesso ilegítimo pois, como já avançado, o *hacker* poderá estar habilitado a entrar no sistema informático e ainda assim está a executar a prática do denominado *hacking* e não propriamente um acesso ilegítimo – pois estando aquele autorizado, tal acesso é naturalmente legitimo. Mas acontece que também o acesso ilegítimo poderá ser uma modalidade do *hacking,* pois tendo em conta a já exposta imprecisão terminológica sedimentada na sociedade entre *hack* e *crack* (este último também conhecido como *break*), há que atribuir este sentido àquela expressão (como que procedendo a uma interpretação sistemática). Clarifiquemos: "(…) todo o acesso ilegítimo é hacking mas nem todo o hacking é acesso ilegítimo"[66] - o acesso ilegítimo será tão-somente uma mera disciplina do *hacking* - pois existe sempre um acesso a um sistema informático alheio. Não obstante, o que é verdadeiramente crucial

[64] Em sentido inverso, salientamos a opinião de Art Bowker: "Initially the term came to refer to individuals who pushed technology to its limits. Hacking was making technology (hardware/software) do more, more efficiently, etc. However, somewhere along the mix it began to be used as a term to describe individuals exploiting technology for illegal purposes. Latter the term crackers came to refer to hackers who did bad things, such as breaking into systems, causing damage, stealing data, etc. We also had the "color" system if you will, in part no doubt due to the old adage in Western movies, good and bad guys wear different colored hats. Yep you guessed it you have White Hat hackers (good guys) and Black Hat Hackers (bad guys). Of course, you also then have the Grey Hat Hackers (good or bad, depending upon what they are doing). As an old John Wayne fan I never really paid much attention to what hat he was wearing but that is beside the point. (…) In my opinion, hackers have come to enjoy a unique position in our society. For instance, there is no such thing as a "white hat" embezzler, drug dealer, or bank robber. The closest think I can think of is maybe Robin Hood, where he was a criminal but his ends justified his means (steal from the rich and give to the poor). I suppose there was some romanticizing about train/bank robberies, Jessie James or even Bonnie and Clyde. But in the end we still consider them criminals when all is said and done. We just don't have other offender groups being described by their head apparel. I also am amazed being a hacker is viewed by some as the best pathway to becoming an IT security expert. It is sort of like someone being a burglar or robber as a path to a career as security professional. I guess these folks think honest hard work and education just doesn't look as good as I was a criminal on a resume*"* cf. BOWKER, Art*, "*Hackers, Crackers, Tramps and Thieves*",* disponível em: http://www.corrections.com/news/article/28572-hackers-crackers-tramps-and-thieves, consultado a 10 de Março de 2014.

[65] Importa referir a seguinte clarificação acerca do termo: "There are two definitions of hacking. The first definition refers to the hobby/profession of working with computers. The second definition refers to breaking into computer systems. While the first definition is older and is still used by many computer enthusiasts (who refer to cyber-criminals as "crackers"), the second definition is much more commonly used. In particular, the web pages here refer to "hackers" simply because our web-server logs show that every one who reaches these pages are using the second definition as part of their search criteria*"* cf. MONTA, Maria Elena, "Illegal but ethical", disponível em: https://maryellenmontagenethics.wordpress.com/2015/07/28/illegal-but-ethical/, consultado a 28 de Julho de 2015 e ainda, neste mesmo sentido: "Hacking is about exploring. Hacking is about going where no one else has gone before. It is about finding new corners in cyberspace. It is about discovering new worlds, and finding different solutions. A good hack is about doing something better than it's ever been done before", noção disponível em: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/interviews/steele.html, consultado a 28 de Julho de 2015.

[66] Ideia avançada no capítulo "Acesso Ilegítimo vs Hacking" do artigo "A punição do hacking no ordenamento jurídico português*"* por nós elaborado e pelo colega Roberto Cangueiro, do Mestrado em Direito e Informática da Escola de Direito da Universidade do Minho, no âmbito do *IV Forum de expertos y jóvenes investigadores en Derecho y nuevas tecnologias,* Salamanca, Março de 2015.

na distinção entre os conceitos será o facto de existir ou não autorização nesse ato de aceder. Torna-se fundamental entender o intuito que preside nesse mesmo ato, porque poderemos estar perante fins constitucionalmente consagrados (exemplos: arts. 21.º, 43.º e 73.º n.º 4 da C.R.P.) e/ou eventualmente verificar-se uma causa de exclusão da ilicitude ou da culpa – o que averiguaremos[67]. Em suma, e tendo em conta os objetivos da presente investigação, o *hacking* é a própria conduta de aceder (seja de forma legitima ou ilegítima) a um sistema informático e como tal é uma atividade (mais ampla) que se pode subdividir em duas grandes atividades, no acesso legítimo (ou *ethical hacking*[68]) e no acesso ilegítimo.

4. *Hackers* – Taxonomia proposta

Antes de mais, é crucial referir que não há uma única taxonomia para definir os vários tipos de *hackers*[69]*.* Tal facto assenta não só nas "variáveis" empregues na elaboração das diversas taxonomias, mas também, nas próprias demarcações efetuadas pelos diversos subgrupos de *hackers* para se distanciarem uns dos outros ou para excluírem especificamente um subgrupo com o qual não concordam. ERIC S. RAYMOND, Autor do "The New Hacker's Dictionary"[70], tendo por base o resultado da conduta, refere que "hackers constroem coisas, crackers danificam-nas"[71]. Um outro Autor, DOUGLAS WILHELM, defende que tais subgrupos podem ser definidos pelo estatuto jurídico-criminal das suas atividades[72].

---

[67] *Vide* Capítulo III (p. 51).

[68] Neste sentido, cumpre aqui fazer a referência ao Autor Steven Levy, o qual fornece os primeiros princípios da "ética *hacker*": "1- Access to computers—and anything which might teach you something about the way the world works—should be unlimited and total; 2 - All information should be free. 3 - Mistrust authority—promote decentralization; 4 - Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race or position; 5- You can create art and beauty on a computer; 6- Computers can change your life for the better." – cf. LEVY, Steven *Hackers: heroes of the computer revolution*, O'Reilly Media, 2010, pp. 27-38. Mais tarde, Steven Mizrach, numa redação mais atualista, forneceu princípios basilares da "ética *hacker*", ligeiramente diferentes, mas ainda na senda do entendimento perfilhado por Steven Levy - cf. MIZRACH, Steven, "Is there a Hacker Ethic for 90s Hackers", disponível em: http://www2.fiu.edu/~mizrachs/hackethic.html, consultado em 10 de Março de 2015

[69] Pois existem diferentes taxonomias, elaboradas por diversos Autores, cf. LEUKFELDT, Rutger e STOL, Wouter, *Cyber Safety: An Introduction*, The Hague, The Netherlands, Eleven International Publishing, 2012., p. 105 e ss.

[70] *Vide* RAYMOND, Eric S., "The New Hacker's Dictionary", disponível em: http://www.proselex.net/Documents/The%20New%20Hacker's%20Dictionary.pdf, consultado a 30 de Julho de 2015.

[71] Tradução nossa do texto original "hackers build things, crackers break them" cf. RAYMOND Eric S., "*H*ow To Become A Hacker", disponível em: http://www.catb.org/esr/faqs/hacker-howto.html, consultado a 30 de Julho de 2015.

[72] Cf. WILHELM, Douglas, *Professional Penetration Testing*, Syngress Press, 2010, p. 503.

Da nossa parte, tendo por base o tipo de acesso (legitimo ou ilegítimo) e as intenções dos *hackers* (benignas ou malignas), enunciamos a seguinte taxonomia:

Black hat hackers - aqueles que se dedicam, entre outros crimes, ao acesso ilegítimo com o intuito malicioso, *i.e.*, ao acesso de sistemas informáticos tendo por objetivo a obtenção de benefícios ou vantagens ilegítimos, tais como, *v.g.*, ganhos pecuniários ou o acesso a informação confidencial ou então causar prejuízo ou dano (ou até destruição) nos mesmos – também designados como *crackers*. Face ao número colossal de ataques informáticos[73] é previsível que este subgrupo seja um dos mais numerosos. Os *black hat hackers* envolvidos na prática do crime de acesso ilegítimo e aos quais se dá destaque são Jonathan James, Adrian Lamo, Kevin Poulsen e como já referido Kevin Mitnick;

White hat hackers – aqueles que utilizam o seu talento técnico para promover a segurança informática ou outras intenções benignas como a partilha do conhecimento. No domínio do *hacking,* cumpre referir que poderão estar ou não autorizados a aceder ao sistema informático mas, por uma ou outra via, sempre diferem dos *black hat hackers* porque não almejam a obtenção de benefícios ou vantagens ilegítimos nem tampouco causar dano ou prejuízo. Contudo, e à luz do já analisado art.º 6.º da Lei do Cibercrime, estes poderão ser classificados como agentes do crime de acesso ilegítimo, ao acederem sem autorização a um sistema informático. Muitas das vezes, este tipo de *hackers* prestam serviços a empresas tecnológicas enquanto *ethical hackers*[74] certificados (havendo inúmeros cursos online ou presenciais para esse efeito de certificação) por forma a testarem aos mais variados níveis os sistemas informáticos das mesmas[75]. No entanto, outros *white hat hackers* operam sem autorização de tais empresas, tentando por essa via criar inovações ou aperfeiçoar bens digitais (o que por certo será de legalidade discutível, mas importa sempre uma análise caso-a-caso). De qualquer das formas, a par dos *blue hat hackers*, será o grupo que mais tende a seguir a

[73] *Vide* IC3 (Parceria entre o FBI e o *National White Collar Crime Center*) "*2014 Internet Crime Report*", disponível em: http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf, consultado a 29 de Julho de 2015.
[74] Também são designados como *blue hat hackers*, cuja definição se encontra adiante.
[75] *V.g.,* através dos *pentests* cuja clarificação se encontra presente na p. 46.

chamada "ética *hacker*" Deste subgrupo destacam-se Richard Stallman, Steve Wozniak e Linus Torvalds (os quais não cometeram qualquer tipo de acesso ilegítimo);

Grey hat hacker – sujeitos que combinam características de um *black hat hacker* com as de um *white hat hacker*, *i.e.* (no que concerne ao acesso legítimo ou ilegítimo) aqueles que acedem sem autorização a sistemas informáticos, identificando falhas de segurança e comunicando a existência de vulnerabilidades[76] ao proprietário do sistema, concedendo a este tempo para reparar a falha. Caso o *grey hat hacker* ofereça os seus serviços para a reparação das falhas mediante uma retribuição pecuniária ou mediante o acesso a um cargo na empresa visada, aí já deve o mesmo ser classificado como um *black hat hacker*. Por certo que se poderá dizer que estamos perante uma "zona cinzenta" mas normalmente o acesso ao sistema informático é feito de forma não-autorizada. Embora normalmente um *grey hat hacker* não atue com vista à obtenção de benefícios ou vantagens ilegítimas, poderá agir contra a Lei (acesso ilegítimo) e contra o próprio código de conduta *hacker* (a já aludida "ética *hacker*")[77];

Blue hat hackers – Na maior parte dos casos, são peritos de segurança informática que são convidados por uma ou mais empresas para testarem[78] produtos ou sistemas informáticos, procurando falhas, erros, *bugs*, etc., antes do produto ou sistema ser lançado oficialmente;

Script kiddies – sujeitos que não possuem conhecimentos de programação ou suficiente capacidade técnica e limitam-se a usar ferramentas, técnicas ou *scripts*[79] programados por outros;

Hacktivists – sujeitos envolvidos no *hacking* com propósitos sociais ou políticos (benignos ou malignos) tais como a promoção de uma causa política

[76] Vulnerabilidades conhecidas como *zero-day threats*, *zero-hour attacks* ou *day-zero attacks*, que são simplesmente vulnerabilidades desconhecidas (exceto, neste caso, para o *grey hat hacker*).
[77] *Vide* MOORE, Robert, *Cybercrime: Investigating High-Technology Computer Crime*, 1.ª ed., Cincinnati, Ohio: Anderson Publishing, 2006.
[78] Também através dos referidos *pentests.*
[79] Desde já se fornece a seguinte definição: "(…)scripts são "roteiros" seguidos por sistemas computacionais e trazem informações que são processadas e transformadas em ações efetuadas por um programa principal", cf. PEREIRA, André Luiz, "O que é script?", disponível em: http://www.tecmundo.com.br/programacao/1185-o-que-e-script-.htm, consultado a 29 de Julho de 2015.

ou a penetração em sistemas informáticos com o intuito de obter informações sobre corrupção, tráfico de pessoas, etc.[80]. Este é um fenómeno recente e ainda em mutação, mas as estatísticas apontam para um crescimento muito acentuado[81]. A título de curiosidade, diga-se que foram *hackers* portugueses e um espanhol, através de um *deface*[82], que terão sido os primeiros *hackers* a executar a primeira ação "hacktivista" da história, com o objetivo de apoiar o Estado de Timor-Leste[83].

Com o intuito de fornecer um entendimento mais claro destes conceitos, apresentamos a tabela n.º 1, considerando o tipo de *hacker*, o tipo de acesso e o tipo de intenção:

Tipo de Hacker	Tipo de Acesso	Tipo de intenção
Black Hat Hacker	Não Autorizado	Obter vantagens ou benefícios ilegítimos
White Hat Hacker	Autorizado (em regra)	Altruísta
Grey Hat Hacker	Não Autorizado (em regra)	Altruísta (em regra)
Blue Hat Hacker	Autorizado	Inócua
Script Kiddies	Não Autorizado (em regra)	Mera curiosidade (em regra)
Hacktivists	Não Autorizado (em regra)	Altruísta (em regra)

Tabela 1 - **Tipo de *hacker*, tipo de acesso e tipo de intenção**

5. A Diretiva 2013/40/UE

Para uma melhor compreensão do crime de acesso ilegítimo, e porventura em jeito de antecipação do seu tipo legal no futuro, é preciso trazer à colação a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12

[80] É o caso do movimento/ideia hacktivista *Anonymous*, *vide* COLEMAN, Gabriella, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, 1.ª ed., London; New York: Verso, 2014.

[81] Cf. PASSERI, Paolo, "April 2015 Cyber Attacks Statistics" disponível em: http://www.hackmageddon.com/2015/05/12/april-2015-cyber-attacks-statistics/, consultado a 25 de Julho de 2015 e cf. *Cyber Crime Statistics and Trends [Infographic]* disponível em: http://www.go-gulf.com/blog/cyber-crime/, consultado a 25 de Julho de 2015.

[82] Originalmente, a expressão significa na língua inglesa alterar a aparência ou a superfície de alguma coisa. *In casu,* será alterar a aparência ou o *layout* de um *website*.

[83] *Vide* FERRER, Mercè Molist, "Hackers portugueses y un catalán montaron la primera campaña hacktivista de la historia", disponível em: http://www.elmundo.es/tecnologia/2015/04/26/553d20bc22601d6c248b456d.html, consultado a 26 de Abril de 2015 e cf. FERRER, Mercè Molist, "La historia nunca contada del underground hacker en la Península Ibérica", disponível em: http://hackstory.es/, consultado a 22 de Outubro de 2015.

de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho[84]. Fundamentalmente, esta diretiva tem por base estabelecer regras mínimas relativas à definição das infrações penais e das sanções no domínio dos ataques contra os sistemas de informação. Ademais, tem também como objetivo facilitar a prevenção da prática de tais infrações e aperfeiçoar a cooperação nacional e internacional entre as autoridades judiciais e outras autoridades competentes.

No que diz respeito ao crime de acesso ilegítimo, encontramos a sua regulação no art.º 3.º da Diretiva. Este preceito, e ao contrário do previsto no art.º 2.º, n.º 2 da Decisão-Quadro 2005/222/JAI do Conselho, prevê que para haver lugar a responsabilidade criminal pelo acesso ilegítimo, necessariamente terá de existir concomitantemente a violação de medidas de segurança[85], o que antes seria apenas uma faculdade que cabia aos Estados-membros. No nosso entender, é uma evolução que certamente também não estará imune de críticas. Não é inteligível se é uma exortação a uma maior e efetiva segurança informática ou se será puro "desmazelo" por parte do Legislador europeu em entender a realidade pois, de facto, ainda se mantém na sociedade uma atitude despreocupada no que toca a regras de segurança nos dispositivos informáticos (*v.g.* utilizadores que não inserirem um código *PIN* nos seus telemóveis ou *passwords* nos seus computadores)[86].

No que toca a sanções, a Diretiva exorta ao endurecimento da punição dos delitos informáticos, e no art.º 7.º a uma punição mais severa pela disponibilização de instrumentos utilizados para cometer o acesso ilegítimo (entre outros ilícitos). Tal incriminação já estava prevista no art.º 6.º n.º 2 da Lei do Cibercrime, mas com uma moldura penal mais branda. Agora, segundo o n.º 2 do art.º 9.º da Diretiva[87], percebe-se que a pena máxima não deve ser inferior

[84] Cuja versão integral se encontra disponível em: http://www.dgpj.mj.pt/sections/informacao-e-eventos/2013/encontros-de-direito/downloadFile/attachedFile_f0/Diretiva_2013_40_UE_12AGO13.pdf?nocache=1400574470.82, consultada a 12 de Junho de 2015.

[85] Opção legislativa também presente na Lei 12.737/2012, que levou à nova redação do art.º 154-A do Código Penal Brasileiro (com a epígrafe "Invasão de dispositivo informático") e o qual, por sua vez, também contem um elemento tipificador subjetivo: "obter, adulterar ou destruir dados ou informações sem Autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita", disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm, consultado a 3 de Agosto de 2015.

[86] *Vide* FREITAS, Pedro Miguel F., & GONÇALVES, Nuno, "Illegal access to information systems and the Directive 2013/40/EU", *International Review of Law, Computers & Technology*, 2015.

[87] "Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 3.º a 7.º sejam puníveis com uma pena máxima de prisão não inferior a dois anos, pelo menos nos casos que se revistam de alguma gravidade."

a dois anos, pelo menos nos casos que se revistam de alguma gravidade, o que certamente importará modificações na atual redação do art.º 6.º e de outras normas da Lei do Cibercrime.

Por fim, importa atentar no considerando 17 da Diretiva, o qual refere que esta "(…) não imputa responsabilidade penal nos casos em que, embora estando preenchidos os critérios objetivos que configuram as infrações nela previstas, os atos sejam cometidos sem intenção criminosa, por exemplo caso uma pessoa ignore que o acesso não era autorizado ou caso o agente esteja mandatado para testar ou proteger sistemas de informação, nomeadamente quando é incumbido por uma empresa ou por um vendedor de testar a solidez do seu sistema de segurança [*v.g., pentests*] (…)". Resulta assim que a Diretiva poderá ainda ser útil para dirimir algumas críticas ou receios quanto à redação do n.º 1 do art.º 6.º da Lei do Cibercrime. Tal como demonstrado, na redação da norma terá sido suprimido o elemento subjetivo do tipo legal, *i.e.*, a norma deixou de atribuir relevância ao intuito do agente em obter benefícios ou vantagens ilegítimos - o que terá assim alargado o âmbito de aplicação da norma. No entanto, agora a Diretiva vem pugnar pela irresponsabilização nas situações em que mesmo estando preenchidos os elementos tipificadores objetivos do crime de acesso ilegítimo, quando este seja praticado sem "intenção criminosa", especificando a título de exemplo a situação do erro sobre as circunstâncias do facto (art.º 16.º n.º 1 do C.P.). Face a esta indicação, resta saber se o Legislador Português adaptará o texto da norma que regula o acesso ilegítimo num futuro próximo e, se a mesma será levada em conta na prática judiciária.

CAPÍTULO II – SEGURANÇA INFORMÁTICA

1. Breves Considerações sobre Segurança Informática (e Cibersegurança[88])

A chamada terceira revolução industrial (também conhecida como revolução da informação) trouxe consigo profundas evoluções no campo tecnológico, fruto do aumento significativo do conhecimento científico e do desenvolvimento no sector da produção industrial (em especial, da tecnologia de ponta), despoletando o aparecimento dos sistemas de informação[89]. Como bem refere a já analisada Diretiva 2013/40/EU no seu considerando n.º 2: "Os sistemas de informação são um elemento essencial para a interação política, social e económica na União. A sociedade está muito e cada vez mais dependente deste tipo de sistemas. O bom funcionamento e a segurança desses sistemas na União são vitais para o desenvolvimento do mercado interno e de uma economia competitiva e inovadora. Assegurar um nível adequado de proteção dos sistemas de informação deverá ser parte integrante de um quadro eficaz e exaustivo de medidas de prevenção que acompanhe as respostas do direito penal à cibercriminalidade". Ora, precisamente por os sistemas de informação (conectados ou não em-linha) assumirem a importância que assumem na sociedade contemporânea e simultaneamente, tendo em conta a proliferação da criminalidade informática, é imperativa a consciencialização sobre a temática da segurança informática e,

[88] Esta delimitação baseia-se na nossa consideração de que a cibersegurança é uma vertente da segurança informática, a qual retracta a segurança dos sistemas de informação no ciberespaço (em linha, portanto). A este propósito, recomendamos a leitura do caderno n.º 12 do Instituto de Defesa Nacional (IDN), o qual contem a Estratégia da Informação e Segurança no Ciberespaço, disponível em: http://www.idn.gov.pt/publicacoes/cadernos/idncaderno_12.pdf, consultado a 5 de Agosto de 2015.

[89] Podemos definir sistemas de informação como sistemas automatizados ou manuais, com o objetivo de reunir, processar, transmitir e disseminar dados que representam informação para um utilizador ou terceiro, ou seja, os sistemas de informação são compostos pelo conjunto dos dados, recursos físicos e pelos *softwares* aptos a armazená-los ou movimentá-los. Conforme assinala João Álvaro Carvalho, nesta matéria verifica-se uma "(…) inexistência de consenso, entre os estudiosos dos sistemas de informação, relativamente à natureza do objecto de estudo, a conceitos e, especialmente, relativamente à terminologia utilizada" e expõe ainda que "esta falta de consenso poderá explicar-se pelo facto de o domínio dos sistemas de informação, para além de ser relativamente recente, ser um domínio inter-disciplinar onde os contributos para o seu desenvolvimento têm origem em diferentes áreas do saber tais como: ciências da computação, engenharia de computadores, ciências da organização e gestão, economia, sociologia, psicologia". O mesmo Autor, adianta que um sistema de informação é "*um sistema de actividade humana que poderá ser suportado por computadores*" e também que "a visão mais restrita de sistema de informação será (…) designada por sistema informático." Assim, "Sistemas informáticos (ou aplicações informáticas) são assim sistemas (baseados em computador) que suportam a recolha, o armazenamento, o processamento e/ou a distribuição de informação numa organização" cf. CARVALHO, João Álvaro, "Desenvolvimento de Sistemas de Informação: Da Construção de Sistemas Informáticos à Reengenharia Organizacional", disponível em: http://www3.dsi.uminho.pt/jac/documentos/DSI.pdf, consultado a 14 de Outubro de 2015.

paralelamente, da chamada "cibersegurança". Impõe-se também a efetiva prossecução de uma verdadeira política de segurança[90] informática, tanto do domínio público, como do domínio privado. Naturalmente, importa que o Direito não fique indiferente ao fenómeno da cibercriminalidade e a esta dê respostas, em termos de prevenção e punição, mas, no nosso entender, tal não bastará. O agudizar da delinquência informática, fomentada pelo recurso exponencial às tecnologias da informação, comporta uma situação insustentável para todo o sector judiciário e em especial, para os tribunais – pois estes serão num futuro próximo incapazes de processar todas as causas informático-criminais que lhes sejam remetidas. Para mitigar esta situação, importa por um lado que os utilizadores (sejam eles pessoas coletivas[91] ou singulares, tenham estes interesses públicos ou privados) se consciencializem dos riscos associados à utilização das tecnologias informáticas, do dever de cuidado que devem possuir a todo o momento para não potenciar esses mesmos riscos[92] e, por outro lado, que utilizem - e mantenham atualizadas[93] - tecnologias que promovam a segurança informática (*v.g.*, mecanismos de segurança[94]).

Assim, importa, pois, responder à questão que evidentemente se coloca: o que é a segurança informática? E em que medida existe uma dicotomia entre segurança informática e cibersegurança?

Ora, também no tópico em apreço, surgem imprecisões terminológicas, quer pela rápida evolução das tecnologias da informação e comunicação, quer pelo jargão extremamente volátil que as circunda[95]. Assim, no que diz respeito a estes conceitos, certamente inexistem definições plenamente estanques[96],

[90] "As políticas de segurança definem o foco da segurança e o que deve garantir*"* – cf. ZÚQUETE, André*, op. cit*., p. 10.
[91] *Vide* PEREIRA, João Pedro, "Empresas desinvestiram na segurança informática", disponível em: http://www.publico.pt/sociedade/noticia/investimento-a-recuperar-1635648, consultado a 28 de Abril de 2014.
[92] Desde já se avança a distinção dos conceitos de Ataque, Risco/Ameaça e Defesa, em termos informáticos: "Um ataque é um conjunto de passos executados no âmbito da exploração de vulnerabilidades e que permitem concretizar uma acção ilícita. Um risco, ou ameaça, é o dano que pode resultar da execução bem-sucedida de um ataque. Finalmente, a defesa consiste no conjunto de políticas e mecanismos desenhados, concretizados e implantados para (i) diminuir a vulnerabilidades de um sistema, (ii) detectar e contrariar/anular ataques passados ou actuais e (iii) minimizar os riscos decorrentes de ataques bem sucedidos", cf. ZÚQUETE, André*, op. cit*., p. 6.
[93] *V.g.*, é importante verificar constantemente se os *softwares* utilizados contêm alguma vulnerabilidade conhecida e/ou que esteja a ser fortemente utilizada pelos ciberdelinquentes nesse dado momento e concomitantemente, substituir essas mesmas tecnologias ou utilizar outras que em si mesmas tenham por objectivo garantir um maior nível de segurança contra intrusões nos sistemas informáticos.
[94] "(…) mecanismos de segurança são a tecnologia que permite pôr em prática as políticas de segurança" cf. ZÚQUETE, André*, op .cit.,* p. 10.
[95] *V.g.,* segurança informática*,* segurança da informação*/data security,* ciberespaço*,* cibersegurança*,* etc.
[96] Como bem refere Myriam Dunn Cavelty, cujo entendimento seguimos de perto: "The vocabulary of clichés that inhabits the information-age debate, and the overall imprecision in terminology, obstruct meaningful analysis. There are three essential elements in the semantics of the information age: "information", "cyber", and "digital", all three of which are so important that they have become shorthand expressions for the age we live in. The information-age vocabulary is

mas para os fins da presente investigação, efetuaremos duas (breves) explanações conceptuais[97] para dar resposta às perguntas acima formuladas.

1.1 Segurança Informática

A segurança informática visa garantir que os recursos físicos ou digitais (*v.g.*, *software*) de uma dada organização sejam utilizados exclusivamente para o seu proposto fim. A segurança informática é essencialmente caracterizada como um conjunto de políticas e mecanismos que se propõem a garantir cinco objetivos fundamentais: a integridade (*i.e.*, garantir que os dados e sistemas são efetivamente aqueles que se crêem ser; a confidencialidade (*i.e.*, assegurar que só aqueles que estão autorizados conseguem visualizar os recursos físicos ou digitais, tornando a informação ininteligível para os restantes); a disponibilidade, (*i.e.,* garantir a manutenção do bom funcionamento dos sistemas de informação); o não-repúdio, (*i.e.,* permitir que exista uma garantia relativamente ao facto de que uma transação não poder ser negada e por fim, a autorização, (*i.e..,* assegurar que só pessoas autenticadas\autorizadas terão acesso aos recursos). Não raras vezes, segurança informática é também denominada como segurança da informação (especialmente nos países anglo-saxónicos, que raramente utilizam a expressão "informática"[98]), embora entendamos que este tipo de segurança está mais relacionada com a preservação da informação propriamente dita.

---

created by simply placing these prefixes before familiar words, thus creating a whole arsenal of new expressions. The nature of these terms is such that their meaning has never been precise – nowadays, however, they have been used so extensively that they can basically mean everything and nothing (…) The fuzziness of the terminology could be a problem in the context of developing a global culture of cybersecurity to the extent that it diminishes the ability of different stakeholders to reach agreement on elements of this culture. In particular, there is no generally accepted definition of cybersecurity, and several different terms are in use that have related meanings, such as information assurance, information or data security, or critical information infrastructure protection. Then again, because information technology continues to evolve rapidly, an overly rigid definition would likely lose its usefulness quickly, so that keeping the concept as flexible as possible may be beneficial" cf. CAVELTY, Myriam Dunn, "A Comparative Analysis of Cybersecurity Initiatives Worldwide", *WSIS Thematic Meeting on Cybersecurity*, Genebra, 28 de Junho a 1 de Julho de 2005, ITU, 2005, disponível em: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf, consultado a 4 de Agosto de 2015.

[97] *Vide* KISSEL, Richard, "Glossary of Key Information Security Terms", *National Institute of Standards and Technology,* 2013, disponível em: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, consultado a 5 de Agosto de 2015 e também: CAVELTY, Myriam Dunn, MAUER, Victor, (coords.) *The Routledge Handbook of Security Studies*, London, New York: Routledge, 2010.

[98] No inglês: *informatics*.

1.2 Cibersegurança[99]

É o termo vulgarmente utilizado para designar o uso de vários meios, tecnologias e processos de modo a proteger redes, sistemas informáticos/de informação e dados informáticos (inclusive programas/*software*) de acessos não autorizados, modificações (não consentidas), danos, etc. Entendemos que não andaremos longe da verdade ao considerar cibersegurança como a segurança informática e de informação aplicada no domínio do ciberespaço[100]. De resto, atendendo ao facto de que os sistemas informáticos dependem da disponibilidade dos sistemas (de informação) e redes para funcionar, são estes os principais alvos dos ataques informáticos e onde se encontram a maior parte das chamadas vulnerabilidades de segurança[101]. Entendemos também que a cibersegurança será uma vertente da segurança informática, pois o ciberespaço apenas existe porque existem sistemas informáticos[102].

---

[99] "Cybersecurity - Joining the two words together again, cybersecurity is concerned with making cyberspace safe from threats, namely cyber-threats. The notion of "cyber-threats" is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or as a tool by a wide range of malevolent actors. As commonly used, the term "cybersecurity" refers to three things: 1. A set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the national security; 2. The degree of protection resulting from the application of these activities and measures; 3. The associated field of professional endeavour, including research and analysis, aimed at implementing and those activities and improving their quality. Cybersecurity is thus more than just information security or data security, but is nevertheless closely related to those two fields, because information security lies at the heart of the matter. Information security refers to all aspects of protecting information. Most often, these aspects are classified in three categories: confidentiality, integrity, and availability of information. "Confidentiality" refers to the protection of the information from disclosure to unauthorized parties, while "integrity" refers to the protection of information from being changed by unauthorized parties. "Availability" means the information should be available to authorized parties when requested. Sometimes, "accountability", or the requirement that the actions of an entity be uniquely traceable to that entity, is added to the list." – cf. CAVELTY, Myriam Dunn*, op. cit.* Veja-se também a definição fornecida pela *International Telecommunication Union* (ITU): "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality, disponível em: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx, consultado a 23 de Outubro de 2015. Por fim, de um prisma ligeiramente diferente, Menny Barzilay refere: "Cybersecurity is the sum of efforts invested in addressing cyberrisk, much of which was, until recently, considered so improbable that it hardly required our attention. We must remember that the shift of the risk curve represents an ongoing trend. Very-high-impact risks will become increasingly frequent, forcing us to become better at protecting assets and devising creative solutions to mitigate risks. To understand the term cybersecurity we must first define the term cyberrisk", cf. BARZILAY, Menny, "A simple definition of cybersecurity", disponível em: http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296, consultado a 23 de Outubro de 2015.

[100] Consideramos o ciberespaço como um espaço virtual, onde ocorre a comunicação através dos meios tecnológicos. Para uma perspetiva mais alargada sobre o tópico: MONTEIRO, Silvana Drumond, "O ciberespaço: o termo, a definição e o conceito", *DataGramaZero: Revista de Ciência da Informação*, v. 8, n.º 3, p. 1-18, disponível em: http://www.dgz.org.br/jun07/Art_03.htm, consultado a 23 de Outubro de 2015 e RAJNOVIC, Damir, "Cyberspace – What is it?", disponível em: http://blogs.cisco.com/security/cyberspace-what-is-it, consultado a 23 de Outubro de 2015.

[101] "System vulnerability is defined to be the intersection of a system susceptibility or flaw, access to the flaw, and the capability to exploit the flaw", cf. "The Three Tenets of Cyber Security", disponível em: http://www.spi.dod.mil/tenets.htm, consultado a 5 de Agosto de 2015.

[102] Para uma melhor compreensão deste assunto, incentivamos a leitura do trabalho levado a cabo por SOLMS, Rossouw von e NIEKERK, Johan van, "From information security to cybersecurity", disponível em: http://www.sciencedirect.com/science/article/pii/S0167404813000801, consultado a 14 de Outubro de 2015.

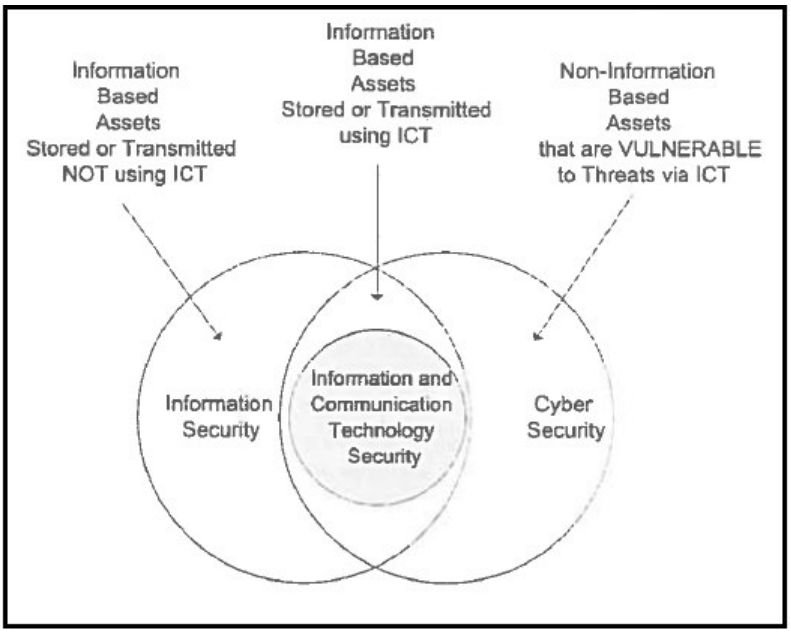

Imagem 1 - "A relação entre segurança da informação e comunicação, segurança da informação e cibersegurança"[103]

2. Sistemas de Proteção Ativa e Passiva

Os sistemas de proteção ativa e passiva podem ser definidos como a primeira linha de defesa dos sistemas informáticos, sendo verdadeiras partes integrantes da segurança informática (e cibersegurança). A diferença entre uns e outros estará na reatividade de cada um, *i.e.,* enquanto os sistemas de proteção passiva limitam-se a uma defesa "estática" (sem reação imediata), já os sistemas de proteção ativa sempre envolvem um certo tipo de reação (mas não de retaliação). Caracterizam-se por visarem (entre outros objetivos e de forma não-cumulativa) a defesa contra atividades não autorizadas, a defesa de perímetro[104] e a defesa em profundidade[105] ou, genericamente, a defesa contra

[103] Cf. SOLMS, Rossouw von e NIEKERK, Johan van*, op. cit.*, p. 101, fig. 4 (tradução nossa).
[104] "A defesa de perímetro, como o nome indica, consiste em definir um perímetro protegido englobando um conjunto de máquinas e redes e evitar interacções indesejáveis entre os dois lados desse perímetro. O perímetro divide o universo e máquinas e redes em dois: um é o lado onde estão os recursos a proteger, o outro é o lado onde estão os possíveis abusadores desses recursos. Mas a defesa em perímetro pode ir mais longe e considerar também o oposto, que no perímetro protegido podem estar potenciais abusadores de recurso exteriores ao mesmo. Neste caso a defesa de perímetro não serve apenas uma política de protecção egoísta, preocupando-se apenas com a segurança do perímetro protegido, mas também com a segurança que, na medida do possível, pode prestar a terceiros. Assim, a defesa de perímetro serve fundamentalmente para restringir as interacções entre domínios de segurança (…)*",* cf. ZÚQUETE, André*, op .cit.,* p. 10.
[105] "A defesa em profundidade segue uma aproximação mais complexa e quiçá mais eficaz, actuando em todos os níveis e não apenas em fronteiras entre domínios de segurança. A defesa em profundidade é particularmente útil para detectar problemas internos a domínios de segurança que foram originados internamente (logo, sem passar pelo perímetro de segurança) ou que, por alguma razão, foram originados externamente ao perímetro de segurança e conseguiram passar através do mesmo. Naturalmente, a defesa em profundidade é mais complexa de gerir, mas teoricamente mais eficaz do que a defesa de perímetro", cf. ZÚQUETE, André*, op. cit.,* p. 10.

vulnerabilidades, ataques e riscos/ameaças (e a adoção de certos tipos de mecanismos para cessar as mesmas). No fundo, os sistemas de proteção ativa e passiva caracterizam-se como sistemas integrados por um conjunto de mecanismos – eminentemente informáticos - que têm como objetivo reduzir a probabilidade de um ataque e/ou minimizar os seus efeitos, sem que haja necessariamente retaliação contra a entidade que perpetuou os ataques[106].

Sucede que, diversos Autores apontam críticas[107] a este tipo de sistemas de defesa (em especial aos sistemas de proteção passiva) dado que, *v.g.*, "o modelo de defesa de perímetro é perigosamente, até fatalmente, falível"[108] e proclamam a apologia de uma proteção verdadeiramente ativa[109], de forma a agir em antecipação para prevenir um ataque, opondo-se ao mesmo (gerando maiores dificuldades para os atacantes, *v.g.,* fornecendo desinformação) ou até mesmo contra-atacar (acedendo aos sistemas dos atacantes, danificado os mesmos, recolhendo provas e/ou informação, etc.[110]). No entanto (e como já referido), entendemos que sistemas de proteção ativa e passiva serão modalidades de uma defesa contra vulnerabilidades, ataques e riscos/ameaças. Assim, urge referir que embora os sistemas de proteção ativa possam ser seguidos de uma retaliação contra uma entidade que realizou um

[106] Tal como é o entendimento do Departamento de Defesa dos E.U.A: "measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative", cf. DEPARTMENT OF DEFENSE, *Dictionary of Military and Associated Terms*, Joint Publication 1-02 (April 12, 2001; as amended June 13, 2007)

[107] Neste sentido, "It is not adequate to rely on passive defenses that employ only after-the-fact detection and notification", cf. LYNN, III, William J. "Remarks on Cyber", RSA Conference, San Francisco, 15 de Fevereiro de 2011, disponível em: http://archive.defense.gov/speeches/speech.aspx?speechid=1535, consultado a 5 de Agosto de 2015; "Passive defenses are a necessary component of a well-designed cyber defense program, but they are no longer sufficient to address increasingly sophisticated threats", cf. LACHOW, Irving, "Active Cyber Defense - A Framework for Policymakers", CNAS, 2013, disponível em: http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf, consultado a 5 de Agosto de 2015; "Not all experts agree, but based on our experience over the past 30 years, we have concluded that a passive defense alone will not work. Effective cybersecurity must include some kind of active response—a threat or a cost higher than the attacker is willing to pay—to complement the passive defense. Developing an active defense will be difficult because identifying the source of an attack is difficult. The practical and legal implications of active defenses have not been determined, and the opportunities for mistakes are legion. The international implications are especially troublesome. It is difficult, usually impossible, to pinpoint the physical location of an attacker. If it is in another country, a countermeasure by a U.S. government computer might even be considered an act of war. Resolving this and related issues will require a thoughtful approach and careful international diplomacy. We desperately need long-term basic scholarship in this area", cf. WULF, Wm. A., JONES, Anita K., "Cybersecurity" in *The Bridge, National Academy of Engineering,* Vol. 32, N.º 1, *National Academy of Sciences,* 2002, p. 44, disponível em: https://www.nae.edu/Publications/Bridge/EngineeringandHomelandSecurity/Cybersecurity.aspx, consultado a 6 de Agosto de 2015 e "The problem of passive defense is that it is only as strong as its weakest part: a hacker needs to find only one exploitable vulnerability to gain access to a system", cf. HOLDAWAY, Eric J., "Active Computer Network Defense: An Assessment", Maxwell Air Force Base, Alabama, 2001, disponível em: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA407139, consultado a 7 de Agosto de 2015.

[108] Tradução nossa do texto original "The perimeter defense model is dangerously, even fatally, flawed", cf. WULF, Wm. A., JONES, Anita K., *op. cit.,* p. 43.

[109] Para uma compreensão mais aprofundada deste tópico, consideramos (absolutamente) indispensável a leitura da investigação efetuada por DEWAR, ROBERT S., "The "Triptych of Cyber Security": A Classification of Active Cyber Defence", in *2014 6th International Conference on Cyber Conflict,* NATO CCD COE Publications, Tallinn, 2014, disponível em: https://ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf, consultado a 6 de Agosto de 2015.

[110] Onde se inclui o denominado *hack back,* que analisaremos mais à frente.

dado ataque informático, entendemos que aí estaremos perante um contra-ataque e não propriamente perante uma proteção ativa. Doravante, caracterizaremos esse contra-ataque como *hack back.*

A verdade é que já nos primórdios da cultura de estratégia militar (*in casu,* século V, A.C.) SUN TZU defendia, na sua célebre obra *A arte da guerra*[111], a apologia da presciência[112], *i.e.*, a técnica da antecipação, da obtenção de informação prévia ou da análise do futuro como parte de uma estratégia vencedora dos estrategas militares – que a todo o momento devem manter um conhecimento claro da ameaça ativa e não se manter ignorante da condição do inimigo. Será aqui, pois, que o conceito da defesa ativa (ou proactiva) lança as suas raízes. Numa época bem mais recente, e com o surgimento da chamada "guerra da informação"[113], o Departamento de Defesa dos E.U.A. manifestou uma preocupação com esta matéria - e com o uso das tecnologias da informação e comunicação em geral - e tem definido como linha orientadora o uso por parte do Estado de sistemas de proteção ativa[114]. Neste sentido, PAUL ROSENZWEIG, seguindo o entendimento do Departamento de Defesa dos E.U.A. quanto à definição de defesa ativa, define sistemas de proteção ativa (os quais denomina de *active cyber defence*[115]) como "a capacidade sincronizada, em tempo real, de descobrir, detetar, analisar e mitigar ameaças"[116]. E prossegue ainda referindo que os sistemas de proteção

[111] TZU, Sun, *A Arte da Guerra,* Bertrand Editora, 2009.

[112] Pressentimento; Previsão. *in* Dicionário Priberam da Língua Portuguesa [em linha], 2008-2013, http://www.priberam.pt/dlpo/presci%C3%AAncia, consultado a 7 de Agosto de 2015. Presciência também se poderá definir como antecipação ou ciência do futuro. Etimologicamente, presciência advém do termo grego *prógnosis* [(de pro (antes) e gnósis (conhecimento)].

[113] Clarificando: "Information Warfare is an emergent reality that comes from a self organization process that has never seen before. The problem is that we talk about it using terms that have well known connotations. And it is difficult to talk about something completely new using words that bring with them specific understanding and expectancies. The early period of the automobile faced a similar situation. At one time it was called a "horseless carriage" as this was the only way to define its essential quality. As the negation of the only understood means of propulsion - the horse. The car is more than a carriage without a horse. This is the dilemma we face when we discuss Information Warfare. Old words do not explain something new. and the danger is that the use of familiar words misrepresent and mask the true extend of the revolution that will have to take place if we are to be able to retain a military capacity in a new physical, social and cognitive space", cf. GARIGUE, Robert, "Information Warfare - Developing a Conceptual Framework", 1995, disponível em: http://all.net/books/iw/iwframe/index.html, consultado a 6 de Agosto de 2015.

[114] "As malicious cyber activity continues to grow, DoD has employed active cyber defense to prevent intrusions and defeat adversary activities on DoD networks and systems. Active cyber defense is DoD's synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities. It builds on traditional approaches to defending DoD networks and systems, supplementing best practices with new operating concepts. It operates at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect DoD networks and systems. As intrusions may not always be stopped at the network boundary, DoD will continue to operate and improve upon its advanced sensors to detect, discover, map, and mitigate malicious activity on DoD networks", cf. DEPARTMENT OF DEFENSE, *Department of Defense Strategy for Operating in Cyberspace,* 2011, disponível em: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf, consultado a 7 de Agosto de 2015.

[115] Numa tradução nossa (literal): ciber defesa ativa.

[116] Tradução nossa do texto original: "the synchronized, real-time capability to discover, detect, analyze, and mitigate threats", cf. ROSENZWEIG, Paul, "International Law and Private Actor Active Cyber Defensive Measures", *Stanford*

ativa "operam à velocidade de rede utilizando sensores, *software* e serviços de informações para detetar e parar atividades maliciosas em especial antes de estas conseguirem afetar redes ou sistemas"[117].

3. *Hack Back*

A verdade é que os ataques informáticos, a cada momento, tornam-se mais complexos dado o grau de sofisticação dos mesmos (mas também dos seus agentes), bem como a sua organização e, ainda, a motivação dos atacantes (que na maior parte dos casos almejam a obtenção de vantagens patrimoniais) o que, consequentemente, gera uma taxa de sucesso consideravelmente alta de tais ataques (onde se inclui também o crime de acesso ilegítimo) e que potencia o abandono (pelo menos parcial) dos sistemas de proteção tradicionais. O sentimento cada vez mais generalizado é que a abordagem tradicional é insuficiente para anular as consequências do ataque informático. Ademais, em muitos casos, só ao fim de longos períodos de tempo os ataques são descobertos e as medidas tornam-se (ainda mais) ineficazes, o que importa situações verdadeiramente dramáticas para os lesados. Por vezes, estes mesmos lesados são repetidamente atacados, o que realmente exige no mínimo uma reflexão sobre as medidas informáticas utilizadas. Destarte, os Estados, os órgãos de polícia criminal e as empresas têm vindo a questionar a possibilidade de adotarem técnicas mais ofensivas de forma a mitigar as ameaças informáticas. Para esse efeito, pode ser já encontrado um vasto leque de medidas propostas pelos sistemas de proteção ativa, nomeadamente, os denominados *Honeypots*[118], que consistem na criação de falsas redes informáticas e na simulação de falhas de segurança de um sistema de forma a colher informações sobre os ataques e, eventualmente, sobre os atacantes e monitorizar a sua atividade (servindo como uma espécie de "engodo" para os

---

Journal of International Law, 47, 2013, disponível em: http://poseidon01.ssrn.com/delivery.php?ID=276073029008011087002126114094081120022037040029059051090103084007005093075065073077038055005012119033032068015095006079099123055081044083067126123021087101083026060017015031081104005104006124017117001123005090121107067102015099112120064064118029&EXT=pdf&TYPE=2, consultado a 7 de Agosto de 2015.

[117] Tradução nossa do texto original: "It operates at network speed using sensors, software and intelligence to detect and stop malicious activity ideally before it can affect networks and systems", cf. ROSENZWEIG, Paul*, op. cit.*

[118] Esta será sem dúvida uma medida que importa considerações jurídicas, não só por eventualmente levar à prática de um crime de interceção ilegítima mas também pela temática anexa das ações encobertas. Impõe-se pois a leitura de GONÇALVES, Nuno Filipe de Sousa, *O Recurso às Acções Encobertas no Âmbito da Lei do Cibercrime,* Dissertação de Mestrado em Direito da Informática, Escola de Direito, Universidade do Minho, 2014.

ciberdelinquentes); o recurso a documentos "armadilhados" que comprometem os atacantes quando abertos e ainda, de forma mais agressiva, utilizar *malware* para rastrear os intrusos; utilizar código malicioso para espalhar nos sistemas dos suspeitos dos ataques ou proceder ao *hack back* (contra-ataque informático), *i.e.,* aceder a um sistema informático ou intercetar dados informáticos do mesmo e ainda danificar ou destruir o sistema do atacante. Ademais, o *hack back* poderá consistir na elaboração de ataques informáticos de forma preventiva por um potencial lesado[119]. Assim, este fenómeno exige respostas (concretas) por parte do Legislador, da doutrina e da jurisprudência[120]. Da nossa parte, focar-nos-emos no acesso ao sistema informático do atacante (uma das modalidades[121] do *hack back*[122]*,* portanto), especificamente sobre a legitimidade do acesso em resposta a um ataque informático (deixando à margem as considerações políticas ou sobre a eficácia técnica deste tipo de medida bem como as possíveis consequências extrajurídicas do uso do *hack back*).

Nos E.U.A., a discussão sobre a admissibilidade do *hack back* tomou já proporções consideráveis e a conduta tanto encontra forte apoio como forte contestação[123]. Do ponto de vista jurídico, e em termos de Direito comparado, o

---

[119] Caso do vírus *stuxnet.*

[120] Pois "nem tudo o que é tecnicamente possível é legalmente admissível" – Autor desconhecido.

[121] No nosso entendimento, uma outra modalidade poderá ser, *v.g.,* a interceção ilegítima.

[122] Diversos Autores identificam o *hack back* como um termo coincidente com sistemas de proteção activa ou *active ciber defense*. Divergimos de tal entendimento, pois *hack back* extrapola o conceito de defesa, dado que se trata antes de um verdadeiro contra-ataque. Não se trata de impedir um ataque, fazer cessar o mesmo ou mitigar os seus efeitos, mas antes uma forma de retaliação. Em sentido diverso vai Dmitri Alperovitch: "Active Defense is NOT about 'hack-back,' retaliation, or vigilantism (…) we are fundamentally against these tactics and believe they can be counterproductive, as well as potentially illegal", cf. ALPEROVITCH, Dmitri, "Active Defense: Time for a New Security Strategy", disponível em: http://blog.crowdstrike.com/active-defense-time-new-security-strategy/, consultado a 10 de Agosto de 2015. Trazemos também à colação a definição fornecida pela Techopedia: "Back-hack is the process of identifying attacks on a system and, if possible, identifying the origin of the attacks. Back hacking can be thought of as a kind of reverse engineering of hacking efforts, where security consultants and other professionals try to anticipate attacks and work on adequate responses. (…) In some cases, back hacking can mean tracing an attack to an IP address; in other back hacking efforts, security teams can spot "electronic bread crumbs," or bits of information that an attacker leaves behind. Other efforts at back hacking may be largely pre-emptive, as when security consultants or even rogue coders discover vulnerabilities in a system", disponível em: http://www.techopedia.com/definition/23172/back-hack, consultado a 7 de Agosto de 2015; uma outra definição retrata o *hack back* como: "turning the tables on a cyberhacking assailant: thwarting or stopping the crime, or perhaps even trying to steal back what was taken", cf. RIOFRIO, Melissa, "Hacking Back: Digital Revenge Is Sweet but Risky", disponível em: http://www.pcworld.com/article/2038226/hacking-back-digitalrevenge-is-sweet-but-risky.html, consultado a 7 de Agosto de 2015.

[123] *Vide* VAAS, Lisa, "Counterterrorism expert wants to arm US companies with hack-back capabilities", diponível em: https://nakedsecurity.sophos.com/2015/08/05/counterterrorism-expert-wants-to-arm-us-companies-with-hack-back-capabilities/, consultado a 10 de Agosto de 2015; FIELD, Tom, "Legal Merits of 'Hack Back' Strategy", disponível em: http://www.bankinfosecurity.com/interviews/legal-merits-hack-back-strategy-i-1729/op-1#, consultado a 10 de Agosto de 2015; SORCHER, Sara, "Influencers: Companies should not be allowed to hack back", disponível em: http://passcode.csmonitor.com/influencers-hackback, consultado a 10 de Agosto de 2015; TIMBERG, Craig, NAKASHIMA, Ellen e DOUGLAS-GABRIEL, Danielle, "Cyberattacks trigger talk of 'hacking back", disponivel em http://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html, consultado a 10 de Agosto de 2015; WESTBY, Jody, "Caution: Active Response to Cyber Attacks Has High Risk", disponível em: http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/, consultado a 10 de Agosto de 2015; MCGEE, Shane, SABETT, Randy

ordenamento jurídico dos E.U.A. proíbe claramente a utilização deste tipo de reação, em especial, da reação na forma de acesso não autorizado a um sistema informático[124], nomeadamente no *Computer Fraud and Abuse Act*, no seu título 18, secção 1030[125]. Como refere ROBERT S. DEWAR, os sujeitos que empreguem *software* na sua defesa de forma a seguir o rasto de um atacante e envolverem-se e ações de retaliação na rede do atacante ficam sujeitos às mesmas sanções jurídicas como o atacante inicial[126]. No entanto, o Relatório da Comissão de Propriedade Intelectual dos E.U.A. de Maio de 2013, intitulado *The Report Of The Commission On The Theft Of American Intellectual Property,* "recomenda [como potenciais medidas futuras] que o Congresso e a administração autorizem ações informáticas agressivas contra os ladrões de propriedade intelectual"[127], o que demonstra a apologia do recurso ao *hack back.* Ademais, também o *Cyber Intelligence Sharing and Protection Act*[128]*,* (aprovado pela Câmara dos Representantes dos E.U.A. em Abril de 2013, mas não aprovado pelo Senado dos E.U.A., pois a Presidência dos E.U.A. entretanto anunciava que iria vetar a lei, pois não garantia a confidencialidade e respeito pelos direitos civis[129]) embora no geral proibisse o acesso não autorizado a sistemas informáticos, continha também disposições controversas[130], tais como qualquer empresa podia "(…) usar sistemas de cibersegurança para identificar e obter informações sobre ciberameaças para

V. e SHAH, Anand, "Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense", 8 J. Bus. & Tech. L. 1, 2013, disponível em: http://digitalcommons.law.umaryland.edu/jbtl/vol8/iss1/3, consultado a 7 de Agosto de 2015 e HARRINGTON, Sean L., "Cyber Security Active Defense: Playing with Fire or Sound Risk Management?", 20 RICH. J.L. & TECH. 12, 2014, disponível em: http://jolt.richmond.edu/v20i4/article12.pdf, consultado a 7 de Agosto de 2015.

[124] Seja esse acesso no âmbito do *hack back* ou um acesso ilegítimo "convencional".

[125] *Vide 18 U.S. Code § 1030 - Fraud and related activity in connection with computers,* disponível em: https://www.law.cornell.edu/uscode/text/18/1030, consultado a 10 de Agosto de 2015.

[126] Cf. DEWAR, Robert S., *op. cit.*

[127] Tradução nossa do texto original: "Recommend that Congress and the administration authorize aggressive cyber actions against cyber IP thieves", cf. THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY, "The Report Of The Commission On The Theft Of American Intellectual Property", The National Bureau of Asian Research, E.U.A., 2013, disponível em: http://ipcommission.org/report/IP_Commission_Report_052213.pdf, consultado a 10 de Agosto de 2015.

[128] *Vide Cyber Intelligence Sharing and Protection Act*, H.R. 624, 113th Cong., 2013, disponível em: https://www.congress.gov/bill/113th-congress/house-bill/624/text, consultado a 10 de Agosto de 2015.

[129] Cf. "Cyber-security bill Cispa passes US House", disponível em: http://www.bbc.com/news/world-us-canada-17864539, consultado a 10 de Agosto de 2015 e ALBANESIUS, Chloe, "White House Threatens to Veto CISPA", disponível em: http://www.pcmag.com/article2/0,2817,2403549,00.asp, consultado a 10 de Agosto de 2015.

[130] Importa atentar no entendimento perfilhado por William Jackson: "In the face of increasing cyber threats there is an understandable pent-up desire for an active response, but this response should not cross legal thresholds. In the end, we either have the rule of law or we don't. That others do not respect this rule does not excuse us from observing it. Admittedly this puts public- and private-sector organizations and individuals at a short-term disadvantage while correcting the situation, but it's a pill we will have to swallow." cf. JACKSON, William, "The hack-back vs. the rule of law: Who wins?", disponível em: http://gcn.com/blogs/cybereye/2013/05/hacking-back-vs-the-rule-of-law.aspx?admgarea=cybereye, consultado a 10 de Agosto de 2015.

proteger os direitos e propriedade (…)"[131] - da empresa - e depois partilhar a informação com terceiros, incluindo entidades governamentais[132], desde que fosse com "propósitos de cibersegurança"[133] (o que certamente importaria considerações mais profundas no âmbito da temática da privacidade e da proteção de dados pessoais). Apesar da existência de disposições[134] no ordenamento jurídico americano que impedem que as empresas partilhem informação privada, o *Cyber Intelligence Sharing and Protection Act* estatuía que as suas provisões seriam efetivas "não obstante qualquer outra lei"[135]. Acresce também que as empresas estariam imunes quanto a "decisões tomadas com base em informação sobre ciberameaças" o que podia dar aso a interpretações extensivas e possibilitar a estas o recurso a medidas de segurança ativa ilegais (mas *in casu* "desculpáveis"). A lei foi recentemente introduzida na Câmara dos Representantes em Janeiro de 2015[136] e está presentemente em fase de apreciação para averiguar se posteriormente poderá ser novamente votada[137]. Por fim, também o Departamento de Justiça dos E.U.A., no manual *Prosecuting Computer Crimes* caracteriza o *hack back* como ilegal[138]. Ademais, um dos principais parceiros estratégicos dos E.U.A. - o Reino Unido[139], no *Computer Misuse Act*[140] de 1990, criminaliza o acesso não autorizado a sistemas informáticos[141].

---

[131] Tradução nossa do texto original: "(…) use cybersecurity systems to identify and obtain cyber threat information to protect the rights and property (…)", cf. Sec. 1104 (b) (1) (A) (i) e (ii); (B) (1) e (2) do *Cyber Intelligence Sharing and Protection Act*.

[132] Quanto a este ponto, será de salientar que a colaboração com as autoridades judiciais para identificar os atacantes, não seria necessariamente algo de malicioso.

[133] Tradução nossa do texto original: "cybersecurity purposes", cf. Sec. 1104 (3) (A) (ii), do *Cyber Intelligence Sharing and Protection Act*.

[134] *V.g., Cable Communications Policy Act, Wiretap Act, Video Privacy Protection Act e o Electronic Communications Privacy Act.*

[135] Tradução nossa do texto original: "Notwithstanding any other provision of law", *Ibid.*

[136] Com o identificador H.R. 234.

[137] *Vide* KNIBBS, Kate, "The New CISPA Bill Is Literally Exactly the Same as the Last One", disponível em: *http://gizmodo.com/the-new-cispa-bill-is-literally-exactly-the-same-as-the-1679496808,* consultado a 10 de Agosto de 2015.

[138] "Do Not Hack into or Damage the Source Computer (…) Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as "hacking back" into the attacker's computer - even if such measures could in theory be characterized as "defensive." Doing so may be illegal, regardless of the motive", cf. COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION CRIMINAL DIVISION, *Prosecuting Computer Crimes*, 2.ª ed., *Office of Legal Education Executive Office for United States Attorneys* (sem data), p. 180, disponível em: http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf, consultado a 10 de Agosto de 2015.

[139] Que, juntamente com os E.U.A., com a Austrália, com o Canada e com a Nova Zelândia compõem os chamados *Five Eyes* – que basicamente se traduzem numa aliança entre esses mesmos países para recolha e troca de informações.

[140] *Computer Misuse Act 1990*, disponível em: http://www.legislation.gov.uk/ukpga/1990/18, consultado a 10 de Agosto de 2015.

[141] *Ibid,* n.ºs 1 ("Unauthorised access to computer material"), 2 ("Unauthorised access with intent to commit or facilitate commission of further offences") e 3 ("Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.").

A nível internacional, a Convenção sobre o Cibercrime – que também foi assinada e ratificada pelos E.U.A. – obriga os Estados-signatários a prever e punir quer o acesso ilegítimo quer a interceção ilegítima e bem ainda, a interferência em dados e, ainda, a interferência em sistemas nos seus arts. 2º, 3º, 4º e 5º, respetivamente. Ademais, a Convenção sobre o Cibercrime contém importantes disposições no que diz respeito à responsabilidade das pessoas coletivas[142]: os Estados-signatários obrigam-se a adotar medidas (legislativas e outras) que garantam a responsabilização pela prática de infrações penais previstas na Convenção (tais como a interceção e o acesso ilegítimo) sempre que tais infrações sejam cometidas, em benefício das pessoas coletivas e por qualquer pessoa singular agindo quer individualmente quer como membro de um órgão da pessoa coletiva, que exerça uma posição de direção, no seio das mesmas ou quando a ausência de supervisão ou de controlo por parte de uma das pessoas mencionada no n.º 1 da norma, tenha tornado viável a prática das infrações previstas na Convenção, em benefício da referida pessoa coletiva e agindo sob a autoridade desta. A responsabilidade das pessoas coletivas pode ser de natureza criminal, civil ou administrativa, sem prejuízo da responsabilidade criminal das pessoas singulares que cometeram a infração. Está bom de ver pois que a Convenção sobre o Cibercrime impede claramente as empresas de procederem ao *hack back* o que significa que caso essa reação fosse legitimada pelos E.U.A e, *v.g.*, as empresas recorressem a este tipo de medida para acederem ilegitimamente a sistemas de outros Estados-Signatários, estariam a praticar um ilícito previsto pela Convenção e dar aso eventualmente a uma crise diplomática.

O mesmo sucede no que concerne ao Direito da União Europeia, pois também as disposições comunitárias classificam o *hack back*, na forma de interceção ilegítima ou na forma de acesso não autorizado a sistemas, como

[142] Cf. art.º 12.º: "Responsabilidade das pessoas colectivas: 1. Cada Parte adoptará as medidas legislativas e outras que se mostrem necessárias para garantir a responsabilização das pessoas colectivas pela prática de infracções penais previstas na presente Convenção, sempre que tais infracções sejam cometidas, em seu benefício, por qualquer pessoa singular agindo quer individualmente quer como membro de um órgão da pessoa colectiva, que exerça, no seu seio, uma posição de direcção, com base em: a) Poder de representação da pessoa colectiva; b) Autoridade para tomar decisões em nome da pessoa colectiva; c) Autoridade para exercer controlo no seio da pessoa colectiva. 2. Para além dos casos já previstos no n.º 1 do presente artigo, cada Parte adoptará as medidas que se mostrem necessárias para garantir a responsabilização de uma pessoa colectiva quando a ausência de supervisão ou de controlo por parte de uma pessoa singular, mencionada no n.º 1 do presente artigo, tenha tornado viável a prática das infracções previstas na presente Convenção, em benefício da referida pessoa colectiva e agindo sob a autoridade desta. 3. De acordo com os princípios jurídicos da Parte, a responsabilidade de uma pessoa colectiva pode ser de natureza criminal, civil ou administrativa. 4. Tal responsabilidade é determinada sem prejuízo da responsabilidade criminal das pessoas singulares que cometeram a infracção".

uma medida ilícita. 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, contém disposições (análogas às disposições referidas da Convenção sobre o Cibercrime) que obrigam os Estados-membros a prever e punir acesso ilegal a sistemas de informação, a interferência ilegal no sistema, a interferência ilegal nos dados e a interceção ilegal (arts. 3.º, 4.º, 5.º e 6.º, respetivamente). Também a referida diretiva regula a matéria da responsabilidade das pessoas coletivas, no seu art.º 10.º, em moldes essencialmente idênticos aos do art.º 12.º da Convenção sobre o Cibercrime. No entanto, é preciso ainda referir que existe já uma proposta de lei[143] por parte do Governo Holandês que visa permitir o *hack back* por parte dos órgãos de polícia criminal, proposta essa que gerou bastante polémica e cuja votação (e desfecho) ainda se aguarda[144].

No que diz respeito ao ordenamento jurídico português, e como já observado[145], o acesso não autorizado a sistemas informáticos (acesso ilegítimo) é previsto e punido no art.º 6.º da Lei n.º 109/2009, de 15 de Setembro – Lei do Cibercrime. Também a interceção ilegítima é prevista e punida no art.º 7.º da referida lei e esta, no seu art.º 9.º, prevê a responsabilidade penal das pessoas coletivas e entidades equiparadas, às quais atribui responsabilidade penal por tais crimes e pelos restantes previstos no diploma, nos termos e limites do regime de responsabilização previsto no Código Penal[146]. Assim, por esta via, também o Legislador português prevê que as referidas medidas do *hack back* são consideradas ilícitas e como tal, puníveis, e imputa também ainda responsabilidade penal às pessoas coletivas que as pratiquem. Não se denotam diferenças substanciais portanto em relação à Convenção sobre o Cibercrime e à Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de agosto de 2013. Há que referir ainda, que nos termos da Lei do Cibercrime, os órgãos de polícia criminal poderão proceder ao *hack back*, *i.e.*, aceder a um sistema informático ou

[143] Disponível em: https://wetgevingskalender.overheid.nl/Regeling/WGK003539, consultado a 13 de Agosto de 2015.
[144] *Vide* PIETERS, Janene, "Dutch gov't to take on hackers in 2015 debate", disponível em: http://www.nltimes.nl/2014/10/20/dutch-govt-take-hackers-2015-debate/, consultado a 10 de Agosto de 2015 e EIJNDHOVEN, Don, "Dutch Police Hacking Back - A Privacy Violation Waiting to Happen", disponível em: http://www.securitycurrent.com/en/news/ac_news/dutch-police-hacking-back-a-privacy-violation-waiting-to-happen, consultado a 10 de Agosto de 2015.
[145] P. 15 e ss.
[146] Art.º 11.º do C.P.

efetuar uma interceção aos dados de um sistema, no âmbito de uma investigação criminal em curso, pela "permissão legal" conferida no art.º 6.º e no art.º 7.º da Lei do Cibercrime, permissão essa fundada nas disposições processuais contidas no seu Capítulo III[147] (e naturalmente, mediante autorização da autoridade judiciária competente para o efeito).

Assim, entendemos que o *hack back,* quer na sua modalidade de acesso não autorizado a sistemas informáticos, quer na modalidade de interceção ilegítima em tais sistemas, é um tema controverso, a vários níveis e que importa sempre uma reflexão não só jurídica, mas também técnica, política e até sociológica. Não é um tema cuja discussão esteja próxima do seu fim, porque, como já aludido, a sofisticação dos ataques e das ameaças exigem novas respostas e sem dúvida que *hack back* poderá ser uma das possíveis reações. Aliás, os meios militares, os serviços de informações e os órgãos de polícia criminal em geral clamam por tal solução (em alguns países, será até algo já admissível). No entanto, pelo menos para os particulares e empresas esta solução é (ainda) ilícita. Tendo por base esta consideração, propomo-nos a analisar se haverá lugar a alguma causa de exclusão da ilicitude ou da culpa no âmbito do *hack back*, especificamente através do acesso ilegítimo do sistema informático do atacante por parte de uma empresa ou de um particular. No entanto, antes de procedermos a essa análise afigura-se-nos premente, efetuar duas breves caracterizações, nomeadamente dos chamados *pentests* e ainda do *backtrack* pois, quer uns quer outros, têm a virtualidade de serem utilizados de forma benigna ou de forma maliciosa e estão intrinsecamente ligados à exploração de vulnerabilidades, ou seja, são aptos a serem utilizados no *hack back.*

4. *Pentests*

Também conhecidos como *penetration tests* ou "testes de penetração"[148], caracterizam-se como a "(…) simulação de um ataque a um

[147] *Vide* VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada*, Coimbra Editora, 2011.
[148] Para uma compreensão mais aprofundada dos *pentests*: NORTHCUTT, Stephen, SHENK, Jerry, SHACKLEFORD, Dave, ROSENBERG, Tim, SILES, Raul e MANCINI, Steve, "Penetration Testing: Assessing Your Overall Security Before Attackers Do", SANS Institute, 2006, disponível em: https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635, consultado a 11 de Agosto de 2015.

sistema, rede, equipamento ou outra instalação, com o objetivo de demonstrar o quão vulnerável um sistema ou "alvo" esteja perante um ataque real"[149]. Além disso, "um teste de penetração pode também determinar como um sistema reage a um ataque, se as defesas de um sistema poderão ser transpostas e que informações podem ser adquiridas do sistema"[150]. Como já referido[151], os *pentests* podem ser efetuados por *white* e *blue hat hackers* na prossecução de tarefas a si confiadas por um contratante para o efeito. Estão, portanto, autorizados a aceder a um sistema informático do qual não são seus titulares. Por regra, a generalidade dos *pentests* são precedidos por uma autorização do titular dos sistemas informáticos sujeitos a tais testes. Relembramos que o já referido considerando 17) da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de agosto de 2013, o qual refere claramente que esta "não imputa responsabilidade penal (…) quando o agente esteja mandatado para testar ou proteger sistemas de informação, nomeadamente quando é incumbido por uma empresa ou por um vendedor de testar a solidez do seu sistema de segurança". Ademais, o próprio art.º 6.º da Lei do Cibercrime exclui da sua previsão quem aceda a um sistema informático de forma autorizada pelo seu proprietário[152]. Por fim, cumpre referir que os *pentests* são efetuados *a priori* do ataque informático, e são utilizados de forma identificar vulnerabilidades, seja pelo titular do sistema informático (ou por pessoas por si contratadas) ou pelo potencial atacante desse sistema informático.

5. *BackTrack*

É um termo que originalmente no inglês é utilizado para caracterizar o processo de "voltar na mesma rota pela qual alguém veio"[153] ou "retraçar os passos de alguém"[154], etc.

[149] Tradução nossa do texto original: "Penetration testing is the simulation of an attack on a system, network, piece of equipment or other facility, with the objective of proving how vulnerable that system or "target" would be to a real attack", cf. HENRY, Kevin M., *Penetration Testing: Protecting Networks and Systems*, ITGP, 2012.
[150] Tradução nossa do texto original: "A penetration test can determine how a system reacts to an attack, whether or not a system's defenses can be breached, and what information can be acquired from the system", cf. KRUTZ, Ronald L. e VINES, Russell Dean, *The CISSP and CAP Prep Guide: Platinum Edition,* John Wiley & Sons, 2006.
[151] Pp. 27 - 28.
[152] "ou sem para tanto estar autorizado pelo proprietário"
[153] Tradução nossa do texto original: "to return by the same route by which one has come", cf. *Collins English Dictionary* [em linha], disponível em: *http://www.collinsdictionary.com/dictionary/english/backtrack,* consultado a 11 de Agosto de 2015.

No campo da segurança informática, *backtrack* (avançado desde já uma definição minimal), traduz-se num processo que conjuga testes de penetração e ciência forense digital (o que torna o *backtrack* mais complexo que os *pentests)*, visando reconstituir o caminho que um atacante percorreu, desde o alvo do ataque até à sua origem. Poder-se-á então caracterizar o *backtrack* como um dos mecanismos de segurança informática ativa e cuja conduta associada poderá ter implicações jurídico-criminais, mormente no caso da "reconstituição" do caminho traçado pelo atacante implicar em última análise um acesso não autorizado ao sistema informático do atacante (constituindo assim um contra-ataque/*hack back*).

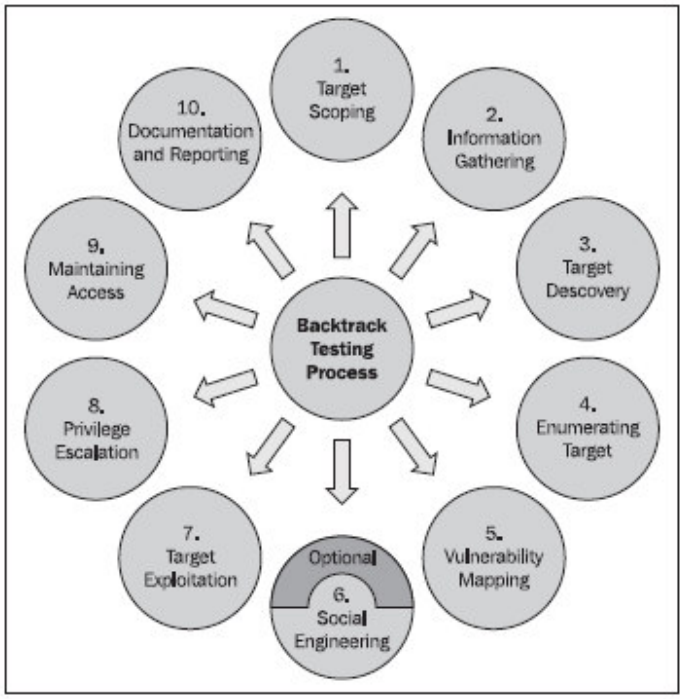

Imagem 2 - *BackTrack Testing Process*[155]

Por fim, diga-se ainda que ao invés dos *pentests,* que são efetuados *a priori* do ataque informático, o *backtrack*[156] é efetuado *a posteriori* do ataque informático. O método pode ser utilizado pelo potencial atacante desse sistema informático bem como pelo titular do sistema informático (ou por pessoas por si contratadas), quer para reconstituir o caminho efetuado pelo atacante, quer

[154] Tradução nossa do texto original: "Retrace one's steps", cf. *Oxford Dictionaries* [em linha], disponível em: http://www.oxforddictionaries.com/definition/english/backtrack, consultado a 11 de Agosto de 2015.
[155] Imagem disponível em: https://www.packtpub.com/books/content/backtrack-4-security-penetration-testing-methodology, consultado a 11 de Agosto de 2015.
[156] Importa salientar que *BackTrack* é também a designação do pretérito sistema operacional *BackTrack Linux* (que visava os mesmos propósitos), tendo sido o mesmo substituído pelo *Kali Linux*.

para posteriormente (entre outras virtualidades) aceder de forma não autorizada ao sistema informático do atacante, praticando assim o *hack back*. Assim, também quanto a esta factualidade, importa verificar da existência de algum tipo justificador ou de alguma causa de exculpação do agente.

CAPÍTULO III - ANÁLISE DE CASO(S) DE ESTUDO - COMPREENSÃO AO NÍVEL DA ILICITUDE E DA CULPA

Como ficou exposto, *hack back* é um novo comportamento da era digital e não só reveste as especificidades analisadas mas também suscita dúvidas no que concerne ao enquadramento típico de tal ação emergente no espaço digital. Destarte, e para os fins da presente investigação, debruçar-nos-emos sobre a prática do *hack back,* enquanto contra-ataque levado a cabo pelo visado de um ataque informático (seja por um particular, seja por Pessoas Coletivas[157]) contra o sistema informático envolvido no referido ataque. Neste sentido, parece-nos pois essencial analisar, se haverá algum tipo justificador ou algum motivo que anule a culpa do agente que acede a um sistema informático alheio sem autorização.

Assim, a questão primordial a que nos propomos dar resposta será se a prática do *hack back* por um agente será legalmente admissível e, em caso de não o ser, se lhe será aplicável alguma causa de exclusão da ilicitude ou da culpa. Por forma a demonstrar o nosso raciocínio, sugerimos então uma hipótese prática [ou um estudo de caso(s)], para condensar a questão suscitada, que passamos a analisar:

1. Hipótese Prática - *Hack the hackers*

Uma pessoa (seja singular ou coletiva), na sequência de um ataque informático em que é visada, contra-ataca e acede ao sistema informático do atacante[158], praticando assim o chamado *hack back*.

[157] Mormente, as Pessoas Coletivas de Direito Privado, *v.g.*, Sociedades Comerciais - atento o facto que serão estas o tipo de Pessoas Coletivas mais suscetíveis de recorrer ao *hack back*). Como tem sido amplamente noticiado, os prejuízos decorrentes dos ataques informáticos são extremamente avultados e as empresas têm-se mostrado recetivas ao uso das técnicas disponíveis associadas ao *hack back,* cf. COHN, Scott, "Companies Battle Cyberattacks Using 'Hack Back'", disponível em: http://www.cnbc.com/id/100788881, consultado a 7 de Agosto de 2015. A este propósito, recordamos que o art.º 9.º da Lei do Cibercrime prevê a responsabilidade penal das pessoas coletivas e entidades equiparadas, às quais atribui responsabilidade penal por tais crimes e pelos restantes previstos no diploma, nos termos e limites do regime de responsabilização previsto no C.P. (art.º 11.º deste diploma).

[158] Fora da hipótese ficam factos que podiam, em abstrato, dar lugar ao preenchimento das estruturas qualificadas do crime de acesso ilegítimo, tal deve-se ao nosso intuito de nos focarmos numa hipótese de análise e compreensão simples.

Quanto a esta hipótese, e para dar resposta à questão enunciada, cumpre desde já aferir se uma pessoa, que na sequência de um ataque informático, contra-ataca e acede ao sistema informático do atacante (corporizando o chamado *hack back*), comete, por essa via, um crime de acesso ilegítimo, previsto e punido pelo art.º 6.º da Lei n.º 109/2009, de 15 de Setembro.

Ora, quanto à definição de crime, segundo MANUEL SIMAS SANTOS e MANUEL LEAL-HENRIQUES, este será a "(…) conduta humana, voluntária e culposa que preencheu um dos modelos ou tipos onde a lei inscreveu bens jurídicos considerados dignos de protecção"[159], *i.e.*, trata-se pois de um comportamento humano (que será todo o comportamento humano dominado ou dominável pela vontade), que consiste numa ação penalmente relevante (ação essa que é típica, ilícita, culposa e punível). Analisemos[160] então quais são os elementos (ou pressupostos[161]) que constituem o crime[162]:

I. Conduta – Pode consistir numa ação (*i.e.*, fazer o que a lei expressamente proíbe) ou numa omissão (não cumprir um imperativo legal, *v.g.*, não atuar quando estava obrigado a tal). Por sua vez, a conduta sempre implica uma vontade, uma atividade (no caso da omissão, uma atividade negativa), um resultado e um nexo causal, gerando bem assim um facto;

II. Tipicidade - Trata-se do preenchimento de um tipo legal. Significa isto que terá que se verificar se estarão preenchidos os elementos objetivos e subjetivos de um tipo legal, *i.e.*, verificar se a concreta atuação humana se enquadra no tipo normativo, mormente, na previsão dos seus elementos objetivos e subjetivos;

---

[159] Cf. SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *Noções de Direito Penal*, Rei dos Livros, 4.ª Ed., 2011, p. 59.

[160] Na análise em apreço, seguimos de perto a esquematização e o entendimento de SANTOS, Manuel Simas e LEAL-HENRIQUES, *op. cit.,* p. 61 e ss.

[161] Estes pressupostos são denominados de categorias analíticas da punibilidade, que enformam a punibilidade em sentido amplo. No que diz respeito à punibilidade em sentido estrito (ou condições de punibilidade), estas dividem-se em condições positivas e em condições negativas de punibilidade. Autores como Figueiredo Dias advogam que a punibilidade deve ser uma categoria autónoma dentro dos pressupostos do crime mas concordamos com Taipa de Carvalho quando diz que esta nova categoria "(…) teria de ter consistência, autonomia e de ser comum a todo e qualquer crime. Pois, só na medida em que for comum a todo e qualquer crime é que se pode configurar como categoria da teoria *geral* do crime"*,* cf. CARVALHO, Américo Taipa de, *Direito Penal - Parte Geral - Questões Fundamentais – Teoria Geral do Crime,* Coimbra Editora, 2ª ed, 2014, p. 262.

[162] *Vide* GARCIA, M. Miguez, *O Risco de Comer uma Sopa e Outros Casos de Direito Penal. I - Elementos da Parte Geral*, 2.ª ed., Almedina, 2012, p. 105 e ss.

III. **Ilicitude –** Será a contrariedade à ordem jurídica na sua globalidade e, simultaneamente, a lesão de interesses juridicamente protegidos. Existe pois uma desconformidade com o direito o que significa que "(…) o acto é ilícito quando ofende ou põe em perigo um bem jurídico tutelado por lei"[163], registando-se pois a antijuridicidade ou ilegalidade do comportamento;

IV. **Culpa/Culpabilidade –** caracteriza-se como "(…) a vontade de infringir o dever de agir ou não agir, imposto por lei"[164] e significa que o facto típico é praticado culposamente ou será pelo menos "(…) a possibilidade de o comportamento assumido pelo agente vir a ser-lhe censurado por lhe ter dado causa"[165]. Estabelece-se pois uma "relação subjectiva entre o facto típico e o seu autor, que permite responsabilizar este pelo cometimento daquele"[166].

Ora, considerando estes elementos (ou pressupostos), e aplicando-os ao caso concreto em análise, verificamos que uma pessoa que aceda a um sistema informático, sem permissão legal ou sem estar autorizada pelo seu proprietário, pratica um facto que indicia o preenchimento de um tipo de ilícito. Clarifiquemos: o acesso por uma pessoa a um sistema informático alheio, de forma não autorizada, sempre implica uma vontade na prática de tal acesso, bem como uma atividade (*in casu,* uma ação que a lei proíbe, no art.º 6.º da Lei do Cibercrime), um resultado (o acesso propriamente dito ao sistema) e ainda um nexo causal (mormente, uma ação adequada a produzir o efeito desejado[167]); Além do mais, trata-se da conduta típica prevista no n.º 1 do art.º 6.º da Lei do Cibercrime: "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte

[163] Cf. SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *op. cit.,* p. 63.
[164] *Ibid,* p. 64.
[165] *Ibid.*
[166] *Ibid*, p. 61. Ademais, os referidos Autores também adiantam que "(…) a culpabilidade é o elemento subjectivo do delito e consiste na relação que se estabelece entre a vontade do agente em cometer o facto e a conduta que põe em prática essa vontade, conduzindo à realização desse mesmo facto", Cf. SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *op. cit.,* p. 64.
[167] Ação esta que poderá ser praticada através do recurso a *Backdoors*, *Trojans*, *Exploits* ou *Rootkits* (programas que são designados de *malware* ou *malicious software*, *i.e*., *software* malicioso cujo objetivo é a infiltração em sistemas informáticos alheios) seja para obter informação (que em regra será confidencial) seja para modificar ou apagar dados, bem como ainda causar danos no sistema.

dele, de qualquer modo aceder a um sistema informático (…)" pelo que também se encontra preenchido o pressuposto da tipicidade[168].

2. Causas de justificação

No entanto, para que possamos afirmar que tal agente verdadeiramente cometeu um crime, é ainda necessário a verificação do preenchimento dos pressupostos da ilicitude e da culpa. Quer isto dizer e, desde logo, no que ao pressuposto da ilicitude concerne (que será a referida desconformidade com o direito/lesão de interesses juridicamente protegidos) é ainda necessário verificar se existe a presença de algum dos tipos justificadores (*i.e.*, causas de justificação ou de exclusão da ilicitude) de forma a afirmarmos se estamos perante um crime de acesso ilegítimo. Isto porque, como bem menciona TAIPA DE CARVALHO, ao identificar a complementaridade material e funcional do tipo legal e das causas de justificação[169], "(…) o direito penal, como qualquer ramo do direito, existe para se aplicar às concretas situações da vida social. E estas situações ou casos concretos podem apresentar-se como relativamente simples ou como realmente complexas (…) quer isto significar que um facto que, em princípio, i. é, em abstrato, constitui um tipo de ilícito, pode, em concreto, por força das circunstâncias em que é praticado, transformar-se num facto justificado, aprovado pela ordem jurídica e, portanto, não ilícito"[170]. Destarte, para que um facto (formalmente típico, como é o caso da presente hipótese) seja punível, para além de ser necessariamente típico, ilícito e culposo (pressuposto que adiante merecerá a nossa reflexão), importa verificar se também não estamos perante a presença de um tipo justificador, ou como refere FIGUEIREDO DIAS, de um *"(contra)tipo"*[171].

---

[168] Para além do preenchimento do elemento tipificador objetivo ["(…) sem permissão legal ou sem para tanto estar autorizado pelo proprietário (…) de qualquer forma aceder"] importa verificar se o elemento subjetivo geral do tipo está preenchido (mormente o dolo, que essencialmente consiste na consciência e vontade de realizar os elementos objetivos do tipo), algo que também analisaremos posteriormente.

[169] Também neste sentido, ANDRADE, Costa, *Consentimento e acordo em Direito Penal: Contributo para a fundamentação de um paradigma dualista*, Coimbra Editora, 1991, p. 23 e p. 245; COSTA, José de Faria, *O Perigo em Direito Penal,* p. 431 e PALMA, Fernanda, *A Justificação por Legítima Defesa como Problema de Delimitação de Direitos, vol. II*, 1990, p. 704 e ss.

[170] CARVALHO, Américo Taipa de, *op. cit.,* pp. 256 - 257; Ademais, o mesmo Autor adianta que "Tal acontece, sempre que o facto formalmente típico seja praticado numa situação a que uma norma jurídica (penal ou não penal) atribua eficácia justificante.", Ibid.

[171] Segundo o entendimento do Autor, "(…) os tipos justificadores, ou *causas de justificação* (…) que, servindo igualmente a concretização do conteúdo ilícito da conduta, assumem o carácter de limitação ("negativa") dos tipos incriminadores. Também os tipos justificadores constituem, no seu *modus* particular, formas delimitadoras do conteúdo

Como apuramos, a ilicitude será a lesão de interesses juridicamente protegidos (existe pois uma desconformidade com o direito) o que significa que "(…) o acto é ilícito quando ofende ou põe em perigo um bem jurídico tutelado por lei"[172], assinalando-se pois a antijuridicidade/ilegalidade do comportamento. Na presente hipótese, o acesso a um sistema alheio de forma não autorizada origina uma lesão dos interesses juridicamente protegidos tais como a proteção da fiabilidade, integridade e disponibilidade dos sistemas e programas informáticos; o domicílio informático ou, como já exposto[173] e, de forma mais abrangente, sobre a inviolabilidade dos sistemas informáticos. Cumpre pois verificar se haverá algum tipo justificador que justifique essa lesão e, por essa via, afaste a ilicitude do acesso não autorizado a um sistema informático alheio.

Tendo em consideração a configuração do nosso ordenamento jurídico-penal, fornecemos um elenco dos motivos que excluem a ilicitude do facto, tradicionalmente referidos como causas de justificação ou de exclusão da ilicitude[174]:

- Causa genérica de exclusão (prevista no n.º 1 do art.º 31.º do C.P.):

- Ordem jurídica considerada na sua totalidade.

- Enumeração exemplificativa[175] (conforme n.º 2 do art.º 31.º do C.P.):

- Legítima Defesa;

- Exercício de um direito;

---

de ilícito (e, na verdade, formas que possuem os seus elementos constitutivos, os seus pressupostos, mesmo uma certa descrição fáctica e são assim, elas próprias, em suma, susceptíveis de tipificação (…) e podem por isso ser vistos como verdadeiros *(contra)tipos, funcionalmente complementares* dos tipos incriminadores", cf. DIAS, Jorge de Figueiredo, *Direito Penal – Parte Geral – Tomo I – Questões Fundamentais*; *A Doutrina Geral do Crime*, Coimbra Editora, 2012, p. 269.

[172] Cf. SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *op. cit.,* p. 63.

[173] P. 18.

[174] De forma a perceber as diversas tentativas de sistematização das causas de justificação: CARVALHO, Taipa de, *op. cit.,* p. 335 e ss. Cumpre também trazer à colação o entendimento de Figueiredo Dias, que refere que está "doutrinalmente afastada (…) a ideia segundo a qual os tipos justificadores operariam em pura objectividade (…)" adiantando que a "(…) razão por que se impôs a exigência de elementos subjectivos da justificação reside em que os elementos objectivos do tipo justificador só apresentam virtualidade para excluir o *desvalor do resultado*, enquanto os elementos subjectivos servem para caracterizar, por excelência, a falta do desvalor da acção (…)" pelo que "o conhecimento pelo agente dos elementos do tipo justificador há de constituir a exigência mínima indispensável à exclusão da ilicitude, o mínimo denominador comum de toda e qualquer causa justificativa", cf. DIAS, Jorge de Figueiredo , *op. cit.,* pp. 392 – 393. Por fim, damos nota ainda que, no elenco em apreço, seguimos grosso modo a esquematização e o entendimento de SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *op. cit.,* p. 93 e ss.

[175] *Vide* GONÇALVES, Manuel Lopes Maia, *Código Penal Português - Anotado e Comentado - Legislação Complementar*, 18.ª ed., Almedina, 2007, p. 164.

- Cumprimento de um dever imposto por lei ou ordem legítima da autoridade;

- Consentimento do lesado.

- Outras causas de justificação previstas no C.P.:

- Direito de necessidade;

- Conflito de deveres.

- Causa de justificação "supra-legal"[176]:

- Direito de necessidade defensivo[177] (ou estado de necessidade defensivo[178])

Tendo em mente a hipótese formulada, cumpre então debruçar-nos sobre cada um destes (*"contra")* tipos.

Em 1º lugar, **no que concerne à causa genérica de exclusão da ilicitude** (prevista no n.º 1 do art.º 31.º do C.P.), **esta assenta na consideração da ordem jurídica na sua totalidade.** Tal como refere FIGUEIREDO DIAS "as causas de justificação não têm de possuir carácter especificamente penal, antes podem provir da totalidade da ordem jurídica e constarem, por conseguinte, de um qualquer ramo de direito"[179]. Ora, tal como se pode extrair do art.º 18.º da C.R.P., o direito penal apenas deve intervir na regulação e resolução dos litígios emergentes na comunidade como ultima *ratio*

[176] Além das causas de justificação consagradas na lei, a doutrina defende ainda a existência de causas de justificação "supra-legais", *i.e.*, causas de justificação existentes que não estão diretamente consagradas na lei. Essencialmente, esse entendimento assenta na ideia de que a lei não pode esgotar todas as causas de justificação (do facto) no plano do ordenamento jurídico-penal. Uma das causas de exclusão "supra-legais" seria a que deriva da "teoria da defesa mais eficaz" (*theorie der wirksamsten abwehr*) avançada por SUPPERT, Hartmut, *Notwehr und "notwehrähnlichen lage"*, Röhrscheid, 1973, p. 371 e ss., também conhecida como "legítima defesa preventiva". Quanto a esta, expõe Paulo Pinto de Albuquerque que "Não é admissível a legítima defesa preventiva (…) isto é, aquela que tem lugar ainda antes da agressão iminente, porque a ameaça pode ser evitada por via da intervenção da força pública. Sendo impossível ou ineficaz a intervenção da força pública, pode eventualmente recorrer-se ao estado de necessidade" cf. ALBUQUERQUE, Paulo Pinto de, *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, Lisboa: Universidade Católica Editora, 2008, p. 146. Também neste sentido, CARVALHO, Américo Taipa de, *A Legítima Defesa*, Coimbra: Coimbra Editora, 1995, p. 276 e ss. e DIAS, Jorge de Figueiredo, *op. cit.,* p. 412. No entanto, por outra via, entendemos que o estado de necessidade defensivo (ou direito de necessidade defensivo) deve figurar no elenco fornecido, enquanto causa de justificação "supra-legal". De todo o modo, entendemos que as causas de exclusão da ilicitude "clássicas" deverão ser sempre convocadas em primeiro lugar, por maior certeza e pela sua consagração legal e só em última instância deverão ser convocadas as causas de exclusão da ilicitude "supra-legais".

[177] CARVALHO, Américo Taipa de, *Direito Penal - Parte Geral - Questões Fundamentais – Teoria Geral do Crime*, Coimbra Editora, 2ª ed, 2014, p. 361 e CARVALHO, Américo Taipa de, *A Legítima Defesa*, Coimbra: Coimbra Editora, 1995, p. 293 e ss.

[178] DIAS, Jorge de Figueiredo, *op. cit.,* p. 460 – 463.

[179] DIAS, Jorge de Figueiredo, *op. cit.,* p. 387.

(o chamado principio da mínima intervenção do direito penal), *i.e.*, quando a lesão de bens jurídicos assume uma gravidade tal que justifique a intervenção do direito. Neste sentido, ocorrendo uma conduta que outros ramos do direito considerem lícita, o direito penal, atendendo a este princípio, não a deverá considerar como ilícita[180].

Parece-nos pois que a **ação direta**, prevista no art.º 336.º do Código Civil[181], deve aqui ser convocada pois poderá ser apta a excluir a ilicitude do facto[182]. No nosso entendimento, apesar deste instituto visar a proteção interesses[183] jurídico-civilmente relevantes, também deve por maioria de razão (e perante a ordem jurídica considerada na sua totalidade), proteger interesses jurídico-penalmente relevantes, pela importância destes[184]. Enquadrada nas disposições sobre o exercício e tutela dos direitos no C.C., a ação direta caracteriza-se pela admissibilidade do recurso à força para proteger interesses jurídico-civilmente relevantes (e no nosso entender, além de excluir a responsabilidade civil[185], também poderá afastar a ilicitude do facto) desde que

[180] A este propósito, como bem aludem Manuel Simas Santos e Manuel Leal-Henriques: "É isso que se contém na economia do n.º 1 do art.º 31.º, ao consagrar-se o *princípio da unidade da ordem jurídica*, explicitando a regra de que o direito penal, em matéria de causas de exclusão da ilicitude, não assume carácter de exclusividade". Os Autores, neste sentido, referem os exemplos da ação directa (art.º 336.º do C.C.), do estado de necessidade (art.º 339.º do C.C.) e do direito de correção dos pais relativamente aos seus filhos (art.º 1878.º do C.C.), cf. SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *op. cit.,* p. 94.

[181] Nos seus precisos termos: "1. É lícito o recurso à força com o fim de realizar ou assegurar o próprio direito, quando a acção directa for indispensável, pela impossibilidade de recorrer em tempo útil aos meios coercivos normais, para evitar a inutilização prática desse direito, contanto que o agente não exceda o que for necessário para evitar o prejuízo. 2. A acção directa pode consistir na apropriação, destruição ou deterioração de uma coisa, na eliminação da resistência irregularmente oposta ao exercício do direito, ou noutro acto análogo. 3. A acção directa não é lícita, quando sacrifique interesses superiores aos que o agente visa realizar ou assegurar."

[182] Ainda a este propósito: CORREIA, Eduardo*, Direito Criminal II,* Coimbra, 1965, p. 113, PALMA, Fernanda*, op. cit*., p. 816 e ss. e ASCENSÃO, Oliveira – "A teoria finalista e o ilícito civil", in *Direito e Justiça*, vol. II, 1981-1986, p. 92 e ss. e GARCIA, M. Miguez, *op. cit.,* pp. 345 e 346.

[183] Para esclarecer alguma confusão que se possa gerar entre os conceitos de "interesse jurídico" e "bem jurídico" trazemos à colação o entendimento de Taipa de Carvalho que expõe que o bem jurídico "(…) é uma designação específica (…) do direito penal; ora como os bens susceptíveis de serem salvaguardados, com base no direito de necessidade, podem não ser bens jurídico penais, é razoável que o legislador tenha utilizado a designação genérica "interesse" jurídico, (que abrange tantos os interesses tutelados penalmente como os tutelados apenas pelo direito civil ou pelo direito de ordenação social) em vez de "bem jurídico"(…)" cf. CARVALHO, Taipa de, *op. cit.,* p. 407.

[184] Discordamos pois do entendimento de Taipa de Carvalho quando expõe que "(…) nem o teor literal, nem a função, nem a natureza dos direitos objecto de protecção pelo art.º 336.º do Código Civil permitem a sua aplicação analógica às situações de perigo actual de um agressão (ou repetição de agressão) ilícita." e que "(…) a acção directa pressupõe um direito relativo (direito de crédito)", cf. CARVALHO, Américo Taipa de, *A Legítima Defesa*, Coimbra Editora, 1995, pp. 290-291. Esta nossa posição resulta quer da interpretação literal quer da interpretação teleológica (e até sistemática) do art.º 336.º do C.C. pois, por um lado, não resulta da letra da lei que o recurso à força seja apenas lícito para o fim de realizar ou assegurar direitos de crédito mas antes para realizar ou assegurar "o próprio direito" (protegendo assim, *v.g.,* direitos absolutos como os direitos reais ou de personalidade) e por outro lado, a lei estatui que a ação direta não poderá sacrificar "interesses superiores aos que o agente visa realizar ou assegurar" – o que significa que estes interesses serão mais do que simples direitos de crédito pois, como próprio ilustre Autor anos mais tarde expõe, o bem jurídico "(…) é uma designação específica (…) do direito penal; ora como os bens susceptíveis de serem salvaguardados, com base no direito de necessidade, podem não ser bens jurídico penais, é razoável que o legislador tenha utilizado a designação genérica "interesse" jurídico, (que abrange tantos os interesses tutelados penalmente como os tutelados apenas pelo direito civil ou pelo direito de ordenação social) em vez de "bem jurídico"(…)", cf. CARVALHO, Américo Taipa de, *Direito Penal - Parte Geral - Questões Fundamentais – Teoria Geral do Crime,* Coimbra Editora, 2ª ed, 2014, p. 407 e cf. nota 183 da presente dissertação.

[185] Segundo Antunes Varela, a ação direta "trata-se de uma forma primária e grosseira de realização da justiça, que pode falhar contra os mais fortes e conduz a excessos, com grave dano da paz pública, contra os mais fracos; mas que

tal ação seja indispensável para evitar lesões irreversíveis num direito próprio, que seja impossível recorrer em tempo útil aos meios jurisdicionais, que a ação se limite ao estritamente necessário para evitar o prejuízo e ainda que a ação não sacrifique interesses superiores aos que o agente visa realizar ou assegurar[186].

A convocação da ação direta para o caso *sub judice* ganha ainda maior relevo se equacionarmos na nossa hipótese que o agente, alvo do ataque informático, vê registos fotográficos seus com conteúdo sexual presentes no seu sistema informático, serem-lhe subtraídos e, chegando ao seu conhecimento que tais registos iriam, com toda a certeza, ser publicados nas horas seguintes. Por forma a evitar a publicação de tais imagens, o agente acede, de forma não-autorizada, ao sistema informático do atacante (subtraindo as referidas imagens, destruindo-as, etc.).

Tendo esta realidade fáctica em mente, a ação direta poderá aqui tornar-se vital à exclusão da ilicitude, desde que o recurso à força[187] (*in casu,* do acesso ilegítimo) seja indispensável e que haja uma impossibilidade de recorrer aos meios coercivos normais para acautelar o seu direito. Parece-nos sensata a arguição no caso em apreço que dificilmente os meios jurisdicionais conseguiriam acautelar o direito do agente (em tempo útil), conquanto o agente se limite a retirar o referido conteúdo e que o facto não sacrifique interesses superiores aos que o agente visa realizar ou assegurar. Quanto a este último pressuposto, está bom de ver que estamos perante a temática do bem ou interesse jurídico preponderante, que cumpre explanar de forma breve. Conforme expõe FIGUEIREDO DIAS, "*o princípio geral mais relevante* de toda a justificação [é o de que] esta opera sempre em uma situação conflitual, em que se debatem interesses contrapostos e em que importa determinar a qual

---

pode-se tornar necessária, pela impossibilidade de os meios estaduais de tutela do Direito chegarem a tempo de evitar prejuízos irreparáveis", cf. VARELA, Antunes, *Das obrigações em geral,* 10.ª ed., revista e actualizada (5.ª Reimpressão da edição de 2000), 2008, p. 553.

[186] A ação direta distingue-se da legítima defesa pois visa evitar a inutilização de um direito, ao passo que a legítima defesa visa antes repelir uma agressão. Ademais, a ação direta contem em si já uma ponderação de interesses (dado que a ação não poderá sacrificar interesses superiores aos que ao gente visa realizar ou assegurar) medida em que o interesse inerente ao direito cuja inutilização o agente visa evitar tem de ser superior ao interesse lesado com a atuação do exercício da ação direta. Distingue-se também da legítima defesa na medida em que esta causa de justificação não exige já o requisito da atualidade, exigindo como qualificativo da agressão na legítima defesa.

[187] Entendemos que o uso da força terá sempre de ser o meio estritamente necessário a repelir a agressão pois existindo um outro meio de repelir a agressão (e que não implique o uso da força), aí o recurso à mesma deixará de ser admissível.

deles deve ser concedida prevalência[188]*".* O mesmo Autor, adianta ainda que "(…) teleológica e funcionalmente, a justificação resulte da preponderância jurídica, em situação, de um interesse perante o outro ou, como costuma dizer-se numa fórmula mais curta, da prevalência do interesse juridicamente preponderante. Por isso a situação de justificação implica sempre um "sopeso jurídico" dos interesses conflituantes. O que, de resto, está em plena consonância com a função primariamente preventiva do direito penal, conducente à maior preservação possível dos bens jurídicos"[189].

Assim, seguindo de perto o entendimento do referido Autor, entendemos que as causas de justificação são convocadas em situações de disputa entre interesses conflituantes, como sucede *in casu*, e sempre ter-se-á que proceder a uma ponderação dos interesses e aferir qual deles será o interesse preponderante. Tal ponderação deve partir da solução constante do n.º 2 do art.º 335.º do C.C.[190] (e não do n.º 1, pois não entendemos que no caso em apreço estejamos perante uma colisão de direitos iguais ou da mesma espécie), *i.e.,* sendo que os direitos (interesses) são desiguais, prevalece o que deva considerar-se superior (prevalência que sempre deve ser aferida casuisticamente e que sempre implica um *ratio* de proporcionalidade na respetiva ponderação). Diga-se aliás que esta ponderação de interesses é de certa forma idêntica à que é efetuada no âmbito do direito de necessidade (causa de justificação prevista no art.º 34.º do C.P., que adiante analisaremos[191]) pois, também nesta causa de justificação, terá de "haver sensível superioridade do interesse a salvaguardar relativamente ao interesse sacrificado(…)"[192]. De todo o modo[193], tanto numa causa de justificação como noutra, necessário é que se esteja perante uma colisão entre bens juridicamente tutelados e em que o sacrifício de um (de forma mais ou menos acentuada) será a salvaguarda do outro[194].

---

[188] Cf. DIAS, Jorge de Figueiredo, *op. cit.,* p. 391.
[189] *Ibid.*
[190] Nos seus precisos termos: "1. Havendo colisão de direitos iguais ou da mesma espécie, devem os titulares ceder na medida do necessário para que todos produzam igualmente o seu efeito, sem maior detrimento para qualquer das partes. 2. Se os direitos forem desiguais ou de espécie diferente, prevalece o que deva considerar-se superior."
[191] P. 64 e ss.
[192] Conforme al. b) do art.º 34.º do C.P.
[193] *Vide* DIAS, Jorge de Figueiredo, *op. cit.,* P. 505, §22.
[194] Sem prejuízo do que se disse, segundo o Acórdão do Tribunal da Relação de Coimbra, de 28-03-2012, processo 1133/10.0IDLRA.C1, será possível, no nosso entender, guiar-nos num caso e noutro por "índices para a determinação da sensível superioridade que tem de existir entre o interesse salvaguardado e o interesse sacrificado: · A medida das

Assim, tendo por base a referida solução, quando resulte que seja clara e inequívoca a superioridade de um dos interesses, entendemos que se registará justificação (cumpridos os restantes pressupostos da causa de justificação convocada)[195].

Ora, fazendo o confronto no caso em apreço entre o bem (jurídico-penal) *inviolabilidade dos sistemas* e os bens *direito à imagem, reserva da intimidade vida privada* e quiçá, *integridade pessoal* (bens protegidos pelo regime do art.º 18.º da C.R.P. e constitucionalmente consagrados nos arts. 25.º, n.º 1 e 26.º n.º 1, do mesmo diploma) parece-nos que o bem inviolabilidade dos sistemas deve soçobrar. Isto porque nos parece claro e inequívoco que, pesando a inviolabilidade dos sistemas informáticos (e a lesão que aí possa ocorrer) e o interesse do agente em recuperar material tão sensível e que indubitavelmente coloca em causa a sua privacidade, integridade moral, honra, (entre outros interesses fundamentais) entendemos estarem preenchidos os requisitos da ação direta na hipótese acima caracterizada. De todo o modo, esta ponderação deve ser feita no caso concreto, pois a solução poderá ser radicalmente diferente num outro caso[196], assumindo assim a questão da ponderação do bem/interesse jurídico um importante relevo em toda a nossa investigação.

---

sanções penais cominadas para a violação dos bens jurídicos em causa, por referência à axiologia constitucional; Deve atender-se também aos princípios ético-sociais vigentes na comunidade em determinado momento; À modalidade do facto; À reversibilidade ou irreversibilidade das lesões; Às medidas de culpa; À medida do sacrifício imposto ao próprio lesado" cf. Acórdão disponível em: http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/b1844b3afb0136f7802579ea0033c2b6?OpenDocument, consultado a 22 de Setembro de 2015.

[195] Neste sentido, vai também o Acórdão proferido pelo Tribunal da Relação de Coimbra, de 25-03-2009, no âmbito do processo 404/08.0PBTMR.C1, que embora não se debruce especificamente sobre a justificação pela convocação da ação direta (mas antes sobre o direito de necessidade e sobre o estado de necessidade desculpante) parece-nos de todo pertinente traze-lo aqui à colação: "(…) Como é sabido, o juízo de ilicitude sobre uma conduta concreta é o resultado da verificação do tipo legal e da inexistência de uma qualquer causa de justificação ou seja, a acção pode ser típica mas não ser ilícita. As causas de justificação são normas que, em situações de conflitos de interesses jurídicos, protegem o que, na concreta situação, é considerado o interesse mais valioso. (…) A exigência da *sensível superioridade do interesse a salvaguardar relativamente ao interesse sacrificado*, conduz-nos ao princípio do interesse preponderante e por isso, à análise dos valores dos interesses em conflito designadamente, dos bens jurídicos em oposição e do grau de perigo que os ameaça (…) Desta forma, a justificação ocorre *"apenas quando é clara, inequívoca, indubitável ou terminante a aludida superioridade à luz dos factores relevantes de ponderação*", cf. Acórdão disponível em: http://www.dgsi.pt/jtrc.nsf/0/23316c8255decd83802575980054865c?OpenDocument, consultado a 10 de Agosto de 2015.

[196] Parece-nos, *v.g.,* que a conclusão será outra no caso de uma empresa que, perante um ataque informático que consista numa subtração de dados sobre mero expediente da empresa e esta decide aceder de forma não autorizada ao sistema informático do atacante para os recuperar. A ação direta será de verificação mais difícil pois desde logo não nos parece que se cumpra o pressuposto referido no art.º 336.º n.º 2 do C.C., *i.e.*, que o acesso não autorizado não sacrifique interesses superiores aos que a empresa visa realizar ou assegurar, pois, no nosso entender tratam-se *in casu* de interesses não preponderantes e no nosso entender, serão estes que devem recuar perante o bem inviolabilidade dos sistemas informáticos, não só porque se trata de bens cuja proteção é menor face a este, mas também porque estar-se-ia a anuir uma situação de profunda instabilidade e insegurança no que diz respeito aos sistemas informáticos, criando um cenário de *hack back* desmesurado, como que vigorando uma espécie de *far west*, atento a frequência com que estes tipos de situações tendem a ocorrer no seio das empresas. De todo o modo e como já o referimos, é sempre essencial fazer a ponderação dos interesses no caso concreto e verificar quais serão os que devem prevalecer, tendo sempre por base o critério fornecido no art.º 335.º do C.C.

No que diz respeito à **legítima defesa**[197] enquanto causa de justificação, tem sido discutido com alguma intensidade a admissibilidade do recurso à mesma na eventualidade de um ataque informático. Discute-se aliás um novo conceito para caracterizar essa circunstância, nomeadamente o conceito de *self help*[198]. *Self-help, lato sensu,* pode ser retratada como uma ação apta a prevenir ou resolver um conflito/disputa/ameaça sem a intervenção jurisdicional ou de terceiros, através do recurso à força, de forma proporcional, pelo que haverá alguma coincidência com o conceito de legítima defesa. Mas em bom rigor, não se trata de legítima defesa, porque falha o pressuposto da necessidade do meio de defesa e do intuito defensivo (*animus deffendendi*) e contra este conceito levantam-se já vozes dissonantes[199]. Em suma, o conceito de *self-help* será a resposta proactiva (e até mesmo agressiva) a um ataque informático, sem recorrer aos meios coercivos normais. Trata-se pois, de certa forma, da transferência de alguns elementos que compõem a legítima defesa para o ciberespaço (criando um novo paradigma que implica medidas contempladas na aludida segurança informática ativa destinadas a reagir a ataques informáticos)[200].

---

[197] *Vide* MONTEIRO, Conde, *A Legitima Defesa: Um contributo para a sua fundamentação,* Dissertação de Mestrado em Ciências-Jurídico-Criminais, Universidade do Porto, 1994; PALMA, Fernanda, *op. cit.;* DIAS, Jorge de Figueiredo, *op. cit.,* p. 404 e ss.; GONÇALVES, Manuel Lopes Maia, *op. cit.,* p. 166 e ss.; BELEZA, Teresa, "Legítima defesa e género feminino" in *Revista Crítica de Ciências Sociais*, n.º 31, 1991 e BRITO, Teresa de, *O Direito de necessidade e a legítima defesa no Código Civil e no Código Penal,* Lex-Edições Jurídicas, 1994.

[198] Em português: auto-ajuda (tradução nossa).

[199] Desde logo, e como à frente explanado, a defesa não é a estritamente necessária ou apta a repelir a agressão, como também não há uma intenção defensiva mas antes, uma intenção ofensiva, como forma de retaliação pela agressão inicial. No plano legislativo e politico-criminal salientamos a crítica de Alice Tang contra a legalização de medidas de segurança informática ativa que estejam à margem dos pressupostos da legítima defesa (*self help*) : "Without clear restrictions, legalizing active defense would bring huge risks of "potentially dangerous misattribution or misunderstanding." The difficulties in differentiating aggressive back hacking from actual hacking actions would lead to serious legal issues. Although there exist different voices, most practitioners and scholars agree that back hacking is not a viable option for various reasons. However, in the contemporary era of information sharing, the private sector has greater demand for a secure cyber environment and advanced cyber protection technologies. Some commentators have urged that active defense "must be considered as a possible device in the cyber toolkit," based on the fact that private firms currently do not receive enough help from the government. As the government continues to fail to take action to protect private organizations and individuals from cyber attacks, the private sector must step in and resort to self help. However, these self-help strategies implemented by private organizations may or may not be appropriate in terms of legality. Without clear guidance from the government and law, such self-help actions could be risky and even dangerous", cf. TANG, Alice, "Hacking back against cyber attacks"*, Chicago Policy Review*, 2015, disponível em: http://chicagopolicyreview.org/2015/07/21/hacking-back-against-cyber-attacks/, consultado a 15 de Agosto de 2015.

[200] Segundo David Dittrich, "Some advocates of uncooperative, aggressive responses to computer attack, usually independent of law enforcement involvement (or instead of reporting to law enforcement at all) use the term *self-help* as a synonym for *self-defense*. *Self-help* implies that no other help (i.e., from law enforcement or other government agencies) is available and that the only option is to take matters into one's own hands. There are times when this may be true, but in such situations the responsibility to be able to clearly articulate justification of Necessity (at minimum) is raised. The term *self-help* may become meaningless when a third-party is engaged to act on a victim's behalf, in which case the word *self* loses its common meaning altogether. In most cases, *self-help* is a euphemism for acting outside of criminal legal process without the involvement of law enforcement (…)" cf. DITTRICH, David, "The Active Response Continuum: Ethical and Legal Issues of Aggressive Computer Network Defense", 2013, disponível em: https://staff.washington.edu/dittrich/arc/book/definitions.html, consultado a 15 de Agosto de 2015. Ainda a este respeito: "It might be thought that victims of an attack have a moral right to retaliate against or punish their attackers by inflicting a morally proportional harm on their attackers. If, for example, A hits B in the face and then turns and runs away in an obvious attempt to escape, it is ethically permissible, on this view, for B to catch A and then hit him back in the face. B's

Vejamos então quais os pressupostos da legítima defesa:

- Existência de uma **agressão** (**atual** e **ilícita**);
- A defesa tem de ser **necessária** e possuir **intenção defensiva** (*animus deffendendi)*

Assim, para a verificação deste tipo justificador, desde logo necessário é que exista uma agressão[201] a bens ou interesses jurídico-penalmente tutelados. Ademais, necessário é que a agressão seja atual ou iminente, que esteja a decorrer ou ainda perdure pelo que o uso da força só será admissível para repelir uma ameaça que ainda perdure, sob pena de se cometer o uso ilícito da força (por uso da mesma demasiado cedo – a agressão ainda não aconteceu - ou por uso da força tarde demais – a agressão já não existe). Naturalmente, a agressão terá ainda de ser ilícita, *i.e.,* contrária ao direito e à ordem jurídica na sua globalidade[202]. Perante a agressão, a defesa deve ser a estritamente necessária[203] *i.e.,* o meio empregue na defesa terá de ser o menos gravoso para o agressor e, simultaneamente, a defesa deve ser adequada a repelir a agressão[204]. O intuito defensivo (o chamado *animus deffendendi*) traduz-se na ideia que a defesa se deve reportar a um ato de pura defesa[205]. Pode ocorrer que este intuito presida até na vontade da defesa, mas a verdade é que caso o agente recorra a um meio excessivo, de forma a repelir a agressão, não se verifica necessidade na defesa mas antes um excesso de legítima defesa, previsto no art.º 33.º do C.P.

---

retaliatory act is justified because it gives A what A deserves and thereby restores the balance of justice that was disturbed by A's morally wrongful act. Applied to the present context, such an analysis would permit the victim of a digital attack to respond with force as a means of "evening the score." Nevertheless, it is generally accepted that, in any society with a morally legitimate government, it is ethically impermissible for citizens to punish or retaliate against wrongdoing. Mainstream political theorists are unanimous in holding that it is the province of government – and not the individual – in such societies to punish wrongdoers after they have been found guilty in a fair trial. Indeed, vigilantism is universally condemned as wrong: so long as the state is reasonably effective in prosecuting and punishing wrongdoing, citizens are morally prohibited from forceful self-help. As a general matter, it is wrong for private victims to even the score by retaliating or punishing attackers", cf. HIMMA, Kenneth Einar e DITTRICH, David, "Active Response to Computer Intrusions", 2005, disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=790585, consultado a 1 de Setembro de 2015.

[201] Tanto pode consistir numa lesão sobre bens ou interesses jurídico-penalmente tutelados como numa ameaça de lesão a esses mesmos bens ou interesses.

[202] *Vide* CARVALHO, Taipa de, *op. cit.,* p. 363.

[203] A respeito da necessidade, Manuel Simas Santos e Manuel Leal-Henriques indicam que a mesma "(…) deve aferir-se objectivamente, ou seja, segundo o exame das circunstâncias feito por um homem médio colocado na situação do agredido", cf. SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *op. cit.*, p. 97.

[204] Taipa de Carvalho identifica a agressão como "(…) toda a conduta humana dirigida contra interesses ou bens jurídicos", cf. CARVALHO, Taipa de, *op. cit.,* p. 360. Tal como na ação direta, entendemos que o uso da força na defesa terá de ser o meio estritamente necessário a repelir a agressão pois existindo um outro meio de repelir a agressão (e que não implique o uso da força), aí o recurso à mesma deixará de ser admissível.

[205] "facto praticado como meio necessário para repelir a agressão" – art.º 33.º do C.P.

Voltando à nossa hipótese prática, não nos parece que o caso do agente, que na sequência de um ataque informático, contra-ataca e acede ao sistema informático do atacante, seja um caso onde se registe a legítima defesa e esteja afastada a ilicitude de tal facto. Isto porque, desde logo, apesar de haver uma agressão ilícita (ataque informático) contra interesses do agente (inviolabilidade do sistema informático) a verdade é que o contra-ataque praticado de forma a aceder ao sistema informático do atacante poderá ocorrer quando o ataque informático já tenha cessado. Mas sobretudo, o contra-ataque que redunde num acesso ilegítimo nem sequer poderá ser considerado uma defesa porque, por um lado, o acesso ilegítimo não tem a virtualidade de suspender ou impedir a agressão (pelo que a defesa não é indispensável para proteger um interesse jurídico do agredido, o que implica que o meio não seja apto) e por outro, não há sequer vontade de defesa (*animus deffendendi*), mas antes a vontade de responder na mesma medida, *i.e.,* de fazer face ao acesso ilegítimo com outro acesso ilegítimo. Não sendo o acesso ilegítimo meio adequado a impedir a agressão[206], dado que o seu efeito útil é nulo (e pode até incentivar o atacante a prosseguir com novos ataques informáticos) entendemos que falha assim o elemento da necessidade da defesa[207] pois, tal como declara TAIPA DE CARVALHO: "tendo em conta que a função da legítima defesa é apenas a de impedir ou repelir a agressão, resulta que só pode ser considerada necessária a acção de defesa, quando o agredido utilizar o meio adequado para impedir a agressão(…)"[208]. Assim, a factualidade da hipótese em apreço não está justificada – o facto em geral é um facto ilícito – e o próprio *hack back,* por esta via, também não beneficia da legítima defesa enquanto causa de exclusão da ilicitude[209]. O que aliás vai de encontro à nossa opinião[210] quanto *hack back* extrapolar o conceito de defesa, pois este não se

[206] A este respeito: "A necessidade do meio afere-se objectivamente, com referência ao momento da agressão ilegal e com base no comportamento do homem médio nas circunstâncias concretas do caso, tendo como balizas a finalidade da causa e a justificação (…)", cf. Acórdão do Supremo Tribunal de Justiça, de 21-01-1998; BMJ, 473, 133.
[207] Aliás, como já visto, mesmo que houvesse o intuito defensivo mas por sua vez o meio não fosse o necessário, estaríamos já numa situação de excesso de legítima defesa.
[208] Cf. CARVALHO, Taipa de, *op. cit.* P. 371
[209] Fazemos no entanto referência à utilização de ataques de negação de serviço (*Distributed Denial of Service/ DDoS*) como uma outra medida do *hack -back*. Tais ataques, praticados pelos titulares dos sistemas informáticos atacados em 1º lugar, não são uma novidade no ciberespaço e colocam outro tipo de desafios, e nesta causa de justificação em específico, porque um ataque de negação de serviço praticado com intuito defensivo *quid sapit* poderá ser um meio adequado a parar\impedir uma agressão atual e ilícita contra o sistema atacado. Parece-nos pois que sai reforçada a ideia de que para aplicação das causas justificadoras da ilicitude é necessária uma reflexão sobre o caso concreto estamos perante situações que não são estanques, constituindo como que equações que exigem soluções concretas e não propriamente soluções universais abstratas.
[210] *Vide Hack back,* p. 40 e ss.

propõe a impedir um ataque, fazer cessar o mesmo ou mitigar os seus efeitos, mas antes a retaliar contra os responsáveis dos ataques informáticos, constituindo assim um verdadeiro contra-ataque.

Quanto à causa de exclusão da ilicitude prevista no art.º 31.º n.º 2, al. b) do C.P. - **exercício de um direito** - cumpre referir que, em bom rigor, estamos perante o direito de necessidade previsto no art.º 34.º do C.P.[211]. Como expõem MANUEL SIMAS SANTOS e MANUEL LEAL-HENRIQUES[212], o legislador português (optando pela teoria diferenciada), distingue o exercício de um direito em duas modalidades: pode existir como causa de exclusão da ilicitude (arts. 31º, n.º 2. Al. b) e 34º), ou pode existir como causa de exculpação (nomeadamente, através do estado de necessidade desculpante previsto no art.º 35.º C.P.)[213]. Vejamos pois em que consiste o exercício de um direito - **direito de necessidade** - como causa de exclusão da ilicitude.

Tal como expõe TAIPA DE CARVALHO, "a situação-base do estado de necessidade [que engloba as situações do direito de necessidade e o estado de necessidade desculpante] está descrita no corpo do artigo: existência de uma situação de perigo actual para determinado bem ou interesse jurídico de determinada pessoa, situação de perigo esta que só pode ser neutralizada mediante a lesão de um interesse ou bem jurídico de uma terceira pessoa alheia à criação da situação de perigo"[214]. Fundamentalmente, o direito de necessidade assenta numa lógica de ponderação de interesses entre o bem ou interesse jurídico ameaçado por um perigo (real e efetivo) e o bem ou interesse jurídico sacrificado para afastar esse perigo. Assim, tal como sucede no âmbito da ação direta (art.º 336.º do C.C.) como causa de justificação (genérica),

[211] Nos seus precisos termos: "Não é ilícito o facto praticado como meio adequado para afastar um perigo actual que ameace interesses juridicamente protegidos do agente ou de terceiro, quando se verificarem os seguintes requisitos: a) Não ter sido voluntariamente criada pelo agente a situação de perigo, salvo tratando-se de proteger o interesse de terceiro; b) Haver sensível superioridade do interesse a salvaguardar relativamente ao interesse sacrificado; e c) Ser razoável impor ao lesado o sacrifício do seu interesse em atenção à natureza ou ao valor do interesse ameaçado."

[212] Cf. SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel*, op. cit.,* pp. 98-99.

[213] Os mesmos Autores acrescentam ainda que "O exercício de um direito (aqui do direito de necessidade) é integrado pelo «complexo de actos que o titular do direito pratica para conseguir a satisfação do interesse que a lei tutela». Com efeito, todo o indivíduo é dotado pelo ordenamento jurídico de um conjunto de *direitos* ou faculdades, abstractamente enunciadas, cujo *exercício* permite a realização da sua personalidade como ser humano (o direito à vida, à integridade física, à honra, à propriedade privada, aos seus valores sociais e colectivos, etc). Daí que a lei proteja os cidadãos contra qualquer ofensa ilícita ou ameaça de ofensa à sua personalidade física e moral (cfr. art.º 70.º do C. Civil). Por isso, o exercício de tais direitos estará justificado – isto é, será legítimo e, portanto, não é ilícito – sempre que respeite os limites que lhe são postos quer internos (os que definem o próprio direito), quer externos (os que o condicionam e restringem perante direitos alheios)", cf. SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *op. cit*., p. 99.

[214] CARVALHO, Taipa de, *op. cit.,* p. 400. Ademais, o Autor refere que "esta situação básica é comum ao direito de necessidade (causa de justificação – art.º 34.º) e ao estado de necessidade desculpante (causa de exclusão da culpa – art.º 35.º)"*, Ibid.*

também no direito de necessidade se regista o princípio da prevalência do interesse jurídico, dado que este tipo justificador também tem na sua base a mesma exigência de ponderação de interesses[215].

Assim, além da necessidade de uma **sensível superioridade entre o interesse a salvaguardar relativamente ao interesse sacrificado** (princípio da prevalência do interesse jurídico)[216], o direito de necessidade tem como pressuposto adicional que **o perigo a afastar seja um perigo real e efetivo** (e não uma mera aparência de perigo), bem como **atual** (à semelhança da legítima defesa), que **a situação de perigo não tenha sido voluntariamente criada pelo agente, exceto para proteger um interesse de terceiro** (art.º 34.º al. a) e **que seja razoável impor ao lesado o sacrifício do seu interesse em atenção à natureza ou ao valor do interesse ameaçado** (art.º 34.º al. c). Há ainda também a necessidade de se verificar um elemento subjetivo, nomeadamente, que o agente conheça a situação de perigo, atuando de forma a evitar o perigo que importará uma lesão. Caso assim não seja, *i.e.,* caso o agente, nas mesmas circunstâncias, não conheça a situação de perigo, então não haverá a justificação do facto.

Tendo por base o exposto, cumpre então verificar se o direito de necessidade se aplica na hipótese vertida. Apesar do agente não criar a situação de perigo (perigo este proveniente do ataque informático e que pode até já ter cessado)[217], não nos parece que o contra-ataque seja o meio adequado a afastar o perigo. Aliás, no nosso entender, não só outros meios poderão ser mais eficazes a interromper o ataque[218] como também serão de legalidade menos discutível. Acresce também que não é manifesta a sensível superioridade do interesse a salvaguardar relativamente ao interesse

[215] Segundo M. Miguez Garcia, "O direito de necessidade é a forma justificante do estado de necessidade, configurando-se como outra das causas de exclusão da ilicitude. De acordo com o artigo 34º, não é ilícito o facto praticado como meio adequado para afastar um perigo actual que ameace interesses juridicamente protegidos de terceiro. Ponto é que se verifiquem os requisitos das três alíneas seguintes, destacando-se no pensamento legislativo a qualificação da superioridade do interesse (alínea c): "haver *sensível* superioridade do interesse a salvaguardar relativamente ao interesse sacrificado". Tem de ser um perigo não susceptível de ser conjurado de outro modo, colocando-se no âmbito do confronto ou colisão entre bens jurídicos, em que o sacrifício de um é a salvaguarda de outro. A "acção" do estado de necessidade, como única hipótese de afastar o perigo, deve ser objectivamente necessária e subjectivamente conduzida pela vontade de salvamento. Podem existir diferentes modos de afastar o perigo e se uma dessas modalidades produz menor dano, se é a menos gravosa, corresponderá então ao meio adequado. O facto de esse meio coactivo não ser substituível por outra medida menos gravosa torna-o *necessário*", cf. GARCIA, M. Miguez, *op. cit.,* pp. 342 e 343.

[216] Relembramos o conteúdo do Acórdão citado na nota 195, p. 60.

[217] Sem prejuízo de eventuais considerações sobre o dever de manutenção e zelo dos sistemas informáticos de que o agente seja titular (responsabilidade pelo risco).

[218] Entre os quais, alguns métodos não-evasivos já disponíveis nos sistemas de proteção ativa.

sacrificado. Se o interesse que o agente visa salvaguardar é o bem jurídico-penal *inviolabilidade dos sistemas informáticos*, então o sacrifício do mesmo bem não é o sacrifício de um interesse inferior, especialmente se considerarmos as consequências que a violação deste interesse\bem possa ter na sociedade. Assim, não nos parece que na nossa hipótese haja exclusão da ilicitude pela via do direito de necessidade.

No entanto, a solução poderá ser outra se equacionarmos novamente a hipótese em que o agente, alvo do ataque informático, vê registos fotográficos seus com conteúdo sexual presentes no seu sistema informático serem-lhe subtraídos e, chegando ao seu conhecimento que tais registos iriam, com toda a certeza, ser publicados nas horas seguintes e, por forma a evitar a publicação de tais imagens, o agente acede de forma não-autorizada ao sistema informático do atacante (subtraindo as referidas imagens, destruindo-as, etc.). Dado que inexistem outros meios, menos evasivos, e porque não é possível recorrer às autoridades judiciais em tempo útil, o acesso não autorizado poderá ser mesmo o único meio ao dispor do visado para afastar o perigo, mormente a divulgação de tais fotos (e não do ataque informático em si mesmo), desde que a ação seja o menos danosa possível (*in casu,* que se limite a subtrair as fotos referidas do sistema informático do atacante). Parece-nos evidente que a situação de perigo não é criada pelo agente e tal como na ação direta, existe uma sensível superioridade do interesse a salvaguardar (direito à imagem, reserva da intimidade vida privada e até integridade pessoal) relativamente ao interesse sacrificado (inviolabilidade dos sistemas informáticos)[219]. Por esta via, entendemos que é razoável impor ao atacante "primitivo" o sacrifício do seu interesse em atenção à natureza dos bens por si colocados em perigo, até porque sendo as referidas fotos difundidas constituiria uma lesão irreversível nos interesses do agente.

Relativamente ao **cumprimento de um dever imposto por lei ou por ordem legítima da autoridade**, não nos parece que este tipo justificador se aplique na hipótese avançada por razões compreensíveis. Salvo melhor

[219] Conforme aresto do RGSt citado por Faria Costa, "há situações da vida em que uma acção, que pelo seu recorte externo preenche a factualidade típica de um crime, constitui o único meio de defesa de um bem jurídico ou o cumprimento de um dever imposto ou reconhecido pelo direito. Em tais casos, a qualificação como conforme ao direito, não proibida ou ilícita, da mesma acção, terá de decidir-se a partir das relações de valor entre os bens jurídicos ou deveres em conflito, sancionados pelo direito vigente" cf. COSTA, José de Faria, *op. cit.,* p. 163.

entendimento, não vislumbramos em que sentido a Lei impõe ao lesado o dever de contra-atacar, após um ataque informático, ou a autoridade poderia dar uma ordem um particular ou a uma pessoa coletiva para, após um ataque informático, proceder ao contra-ataque e assim aceder a um sistema informático de forma não-autorizada.

No entanto, poderíamos equacionar, na nossa hipótese, que o *hack back* era ordenado pelos superiores hierárquicos do agente no exercício das suas funções. Acerca da **obediência hierárquica**[220]**,** refere TAIPA DE CARVALHO que "num *Estado de Direito Democrático*, tem de se considerar definitivamente ultrapassada a antiga tese da "obediência cega" às ordens e decisões das autoridades públicas"[221]. Da nossa parte, acrescentamos (e afirmamos) que não só deve a tese da "obediência cega" estar definitivamente ultrapassada quanto às ordens e decisões das autoridades públicas mas também das entidades privadas (particularmente quando os comandos das entidades patronais resultem em responsabilidade criminal). Ora, como já demonstrado[222], o art.º 9.º da Lei do Cibercrime rege os termos da responsabilidade penal das pessoas coletivas e entidades equiparadas, atribuindo responsabilidade penal às mesmas pela prática dos crimes previstos no mesmo diploma, nos termos e limites do regime de responsabilização previsto no Código Penal, nomeadamente no seu art.º 11.º. De forma similar ao estatuído no art.º 12.º da Convenção sobre o Cibercrime[223] e porque estamos perante um caso especialmente previsto na Lei[224] – do Cibercrime – o Código Penal determina que "as pessoas colectivas e entidades equiparadas (…) são responsáveis pelos crimes (…) quando cometidos: Em seu nome e no interesse colectivo por pessoas que nelas ocupem uma posição de liderança" [al. a)] ou "por quem aja sob a autoridade das pessoas referidas na alínea

[220] *Vide* BRANDÃO, Nuno, *Justificação e desculpa por obediência em direito penal*, Dissertação de Mestrado, FDUC, 2004.
[221] Cf. CARVALHO, Taipa de, *op. cit.,* p. 432.
[222] P. 45.
[223] A Convenção sobre o Cibercrime obriga os seus estados signatários a adotarem "(…) medidas legislativas e outras que se revelem necessárias para garantir que as pessoas colectivas possam ser consideradas responsáveis pelas infracções penais previstas na (…) Convenção, cometidas em seu benefício por qualquer pessoa singular, agindo individualmente ou enquanto membro de um órgão da pessoa colectiva, que nelas ocupem uma posição de liderança (…)" (n.º 1) e, simultaneamente, medidas "(…)que se revelem necessárias para garantir que uma pessoa colectiva possa ser considerada responsável sempre que a falta de vigilância ou controlo por parte de uma pessoa singular referida no n.º 1 possibilite a prática de uma das infracções previstas na presente Convenção em benefício da referida pessoa colectiva por uma pessoa singular que aja sob a sua autoridade." (n.º 2).
[224] N.º 1 do art.º 11.º do C.P.

anterior em virtude de uma violação dos deveres de vigilância ou controlo que lhes incumbem" [al. b)][225].

Perante a articulação dos diferentes normativos referidos, efetivamente resulta a responsabilização da pessoa coletiva pela prática do acesso ilegítimo, quando cometido em seu nome e no interesse coletivo (seja por pessoas que nelas ocupem uma posição de liderança, seja por quem atue sob a autoridade daquelas pessoas em virtude de uma violação dos deveres de vigilância ou controlo que lhes incumbem) exceto se "(…) o agente tiver atuado contra ordens ou instruções expressas de quem de direito" (n.º 6 do mesmo preceito). Assim, além da possível responsabilização da pessoa coletiva pelas instruções dadas que resultaram na prática do acesso ilegítimo, também o agente (subordinado) que tenha diligenciado o contra-ataque não está isento de responsabilidade criminal. Responsabilidade criminal que poderá ser exclusiva do mesmo, por atuar contra ordens ou instruções expressas de órgãos e representantes da pessoa coletiva com autoridade para exercer o controlo da sua atividade (cf. n.º 4 do mesmo art.º). Neste caso, por forma a aferir do pressuposto da ilicitude, defende TAIPA DE CARVALHO que "(…) há que distinguir, relativamente ao inferior hierárquico, entre ordens cuja ilicitude criminal é sindicável pelo inferior hierárquico (caso em que, se este cumpre a ordem, também comete um ilícito criminal) e ordens cuja ilicitude criminal é objectivamente insindicável pelo inferior hierárquico (caso em que este não pode deixar de cumprir a ordem e, consequentemente, o seu facto não é ilícito, pois está justificado, só havendo responsabilidade criminal do superior, que utiliza o inferior como mero instrumento)" [226]. *In casu,* porque a ilicitude criminal da ordem é sindicável pelo inferior hierárquico (o agente, subordinado, devia ter-se recusado a cumprir a ordem, o que aliás encontra suporte na letra da lei: "o dever de obediência hierárquica cessa quando conduzir à prática de um crime"[227]) afigura-se na hipótese avançada que caso o referido agente cumpra a ordem, também comete um ilícito criminal e assim sendo, deve sem mais

[225] A este respeito, salienta Pedro Dias Venâncio: "como o n.º 1 deste artigo 11.º do Código Penal continua a prever que «Salvo o disposto no número seguinte e nos casos especialmente previstos na lei, só as pessoas singulares são susceptíveis de responsabilidade criminal», continua a ser necessária a expressa previsão dessa responsabilidade para os crimes da LC, embora no mais aplicando-se o regime geral do Código Penal", cf. VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada*, Coimbra Editora, 2011, p. 84.
[226] Cf. CARVALHO, Taipa de, *op. cit.,* p. 440.
[227] Cf. art.º 36.º n.º 2, C.P.

recusar a ordem, sob pena de ele mesmo incorrer em responsabilidade criminal, pois não está justificada a ilicitude do facto[228]. Assim, importará verificar – em sede própria[229] - se haverá antes alguma causa de exculpação do agente (em especial, a obediência indevida desculpante) que se possa aplicar na hipótese em apreço.

Quanto à figura do **consentimento**[230], cumpre apenas referir que admitindo-se, como hipótese de raciocínio, que o *hack back* é consentido pelo atacante primitivo, *i.e.,* sendo consentida (*a priori)* a prática do acesso ao sistema informático do atacante, é excluída a ilicitude do facto. No entanto, não nos parece plausível que o atacante primitivo consinta no acesso ao seu sistema informático pelo ofendido, pelo que este tipo justificador não nos merece grandes explanações.

A última das causas de exclusão previstas no Código Penal é o **conflito de deveres**[231] (previsto no art.º 36.º do C.P.). Quanto a este tipo justificador, alude M. MIGUEZ GARCIA: "(…) em caso de conflito no cumprimento de deveres jurídicos não é ilícito o facto de quem satisfizer dever de valor igual ou superior ao do dever que sacrificar"[232]. FARIA COSTA acrescenta ainda que "o direito não pode exigir dos seus destinatários nada que seja de cumprimento impossível, pelo que, em estado de colisão inextrincável de deveres iguais, só pode ser exigido do agente que cumpra um deles, conferindo-lhe a ordem jurídica uma plena liberdade de escolha"[233].

Partindo deste entendimento e do texto legal, não se revela a presença do conflito de deveres na nossa hipótese prática, pois não impende sobre o agente um dever de ação, nomeadamente o dever de na sequência de um ataque informático, contra-atacar e aceder ao sistema informático do atacante "primitivo".

---

[228] A este respeito, refere ainda Taipa de Carvalho que "(…) sempre que, na situação concreta, uma ordem seja (apareça objectiva e necessariamente como) vinculativa para o funcionário, não poderá, sob pena de contradição normativa e de tratamento injusto do funcionário, considerar-se o seu comportamento de execução como ilícito.", Cf. CARVALHO, Taipa de, *op. cit.,* p. 440.

[229] P. 76.

[230] Torna-se essencial a leitura de ANDRADE, Costa, *op. cit*., mas também DIAS, Jorge de Figueiredo, *op. cit.,* p. 470 e ss. e CARVALHO, Taipa de, *op. cit.,* p. 443 e ss.

[231] *Vide* DIAS, Jorge de Figueiredo, *op. cit.,* p. 466; SILVA, Germano Marques, *Direito Penal Português, Parte Geral, II,* Verbo, 1998, p. 124; CARVALHO, Taipa de, *op. cit.,* p. 423; CORREIA, Eduardo, *op. cit*., p. 93 e ss. e GARCIA, M. Miguez, *op. cit.* p. *343.*

[232] Cf. GARCIA, M. Miguez, *op. cit*, p. 422.

[233] Cf. COSTA, José de Faria, "Formas do Crime" in *Jornadas de Direito Criminal,* CEJ, 1983, p. 63.

Por fim, no que diz respeito às causas de exclusão da ilicitude, cumpre ainda fazer referência a uma possível causa de justificação "supra-legal", nomeadamente o **direito de necessidade defensivo** (ou estado de necessidade defensivo[234]). Nas palavras de TAIPA DE CARVALHO, este "(…) visa preservar a intocabilidade do bem jurídico face a uma agressão ou perigo de agressão (ou de lesão)"[235]. Segundo FIGUEIREDO DIAS, os pressupostos deste tipo justificador "supra-legal" são os seguintes[236]:

- uma situação de defesa à qual falta um dos pressupostos indispensáveis para configurar uma situação de legítima defesa;

- impossibilidade para o agente de evitar o perigo;

- necessidade do facto para o repelir;

- o bem lesado pela defesa não seja muito superior ao bem defendido.

No fundo, o agente ao abrigo desta causa de exclusão da ilicitude (que carece de ser positivada) reage contra interesses do agressor, mas numa situação que em concreto não se verificam todos os pressupostos da legítima defesa (por exemplo, a atualidade da agressão). Imperioso é que se verifique a "inexistência, na situação concreta, de alternativa à reacção defensiva preventiva"[237] *i.e.*, que o agente não consiga evitar o perigo e que a reação seja a estritamente necessária para repelir o perigo\agressão.

Como já observado, na nossa hipótese não se verificou uma situação de legítima defesa por, grosso modo, não estar cumprido o pressuposto da atualidade da agressão (porque o ataque já poderia teria ocorrido) mas sobretudo por não estar cumprido o pressuposto da necessidade da defesa (porque o contra-ataque, que redunde num acesso ilegítimo não é propriamente uma defesa, nem tampouco existe vontade de defesa/*animus deffendendi*). Com efeito, o mesmo sucede quando examinamos se o direito de necessidade defensivo se verifica na hipótese prática sugerida. Embora no

[234] DIAS, Jorge de Figueiredo, *op. cit.,* pp. 460 – 463.
[235] Cf. CARVALHO, Américo Taipa de, *A Legítima Defesa*, Coimbra Editora, 1995, p. 292.
[236] Figueiredo Dias, *op. cit.,* p. 461.
[237] Cf. CARVALHO, Américo Taipa de, *op. cit*., p. 294.

caso do *hack back* se verifique a impossibilidade para o agente de evitar o perigo (pois o ataque informático irá com certeza ocorrer) e, independentemente do pressuposto da atualidade da agressão na situação de "defesa" estar verificado[238], a verdade é que falta ainda o cumprimento do indispensável pressuposto para verificação deste tipo justificador, a necessidade do facto para repelir o perigo/agressão, *i.e.,* o contra-ataque, na forma de acesso ilegítimo, não é estritamente necessário para repelir o perigo/agressão (ataque informático). Não nos parece portanto que esta causa de exclusão da ilicitude se verifique *in casu.*

No entanto, também aqui a solução poderia ser outra se equacionarmos que o agente, alvo do ataque informático, vê registos fotográficos seus com conteúdo sexual presentes no seu sistema informático serem-lhe subtraídos e, chegando ao seu conhecimento, que tais registos iriam com toda a certeza ser publicados nas horas seguintes e, por forma a evitar a publicação de tais imagens, o agente acede de forma não-autorizada ao sistema informático do atacante (subtraindo as referidas imagens, destruindo-as, etc.). De facto, existe uma situação de defesa à qual falta um dos pressupostos indispensáveis para configurar uma situação de legítima defesa (designadamente, a atualidade da agressão). Existe também uma impossibilidade para o agente de evitar o perigo (pois o ataque informático certamente irá acontecer) e existe ainda a necessidade do acesso ilegítimo para repelir o perigo (proceder ao acesso para impedir a divulgação das referidas fotos do agente). Ademais, também quanto ao último pressuposto do direito de necessidade defensivo, neste caso, o bem lesado pela defesa não ser muito superior ao bem defendido, estará verificado (pois o bem inviolabilidade dos sistemas informáticos não se afigura muito superior aos bens direito à imagem, à reserva da intimidade vida privada e à integridade pessoal). Por todos os pressupostos estarem verificados, parece-nos que a ilicitude presente na factualidade vertida nesta hipótese poderá ser afastada por via do direito de necessidade defensivo.

[238] Pois este estando verificado, sempre careceria de ser igualmente verificado o pressuposto da necessidade do meio. Embora um dos pressupostos do direito de necessidade defensivo seja a ausência de um pressupostos indispensáveis na situação de defesa para configurar uma situação de legítima defesa, (poderia ser a ausência do pressuposto da atualidade da agressão como a ausência do pressuposto da necessidade do meio) a verdade é que como já explanado não estamos sequer perante uma situação de defesa mas antes de contra-ataque pelo que sempre está por verificar – no caso concreto e quanto a este tipo justificador- o pressuposto da necessidade do facto (do contra-ataque) para repelir o perigo.

3. Causas de exculpação

Cumpre agora debruçarmo-nos sobre os motivos que anulam a culpa na produção do facto. Como já observamos anteriormente[239], a culpabilidade, enquanto elemento do crime, consiste na "vontade de infringir o dever de não agir, imposto por lei"[240] e que se traduz na "possibilidade de o comportamento assumido pelo agente vir a ser-lhe censurado por lhe ter dado causa"[241]. Aliás, como menciona TAIPA DE CARVALHO, "para que haja crime é necessário que a conduta, que constitui um tipo de ilícito (seja activo ou omissivo, doloso ou negligente) possa ser censurada, ético-pessoalmente, ao seu autor a título de culpa"[242]. Tal exigência portanto, não é mais do que a concretização do princípio *nulla poena sine culpa*[243]. A culpa, sendo um juízo de censura dirigido ao agente pelo cometimento do facto típico e ilícito, assenta na capacidade deste em avaliar a ilicitude no momento da prática do facto ou de se determinar de acordo com essa avaliação[244].

O mesmo Autor, muito doutamente realça que "tal como a questão da justificação do facto é uma questão que, nos planos lógico, metodológico e dogmático, é posterior à questão e afirmação da tipicidade do acto, também a questão da desculpação do agente pressupõe a afirmação prévia da ilicitude do facto, isto é, da inexistência de uma causa de justificação do facto típico"[245]. Assim, admitindo como hipótese de raciocínio que não se logrou verificar algum dos tipos justificadores na factualidade presente na nossa hipótese prática (pelo que a mesma será então ilícita), importa ora verificar se será aplicável *in*

[239] P. 53.
[240] Cf. SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *op. cit.,* p.64.
[241] *Ibid.*
[242] Cf. CARVALHO, Taipa de, *op. cit.,* p. 260.
[243] Para uma reflexão mais profunda acerca da culpa jurídico-penal, recomendamos a leitura de CARVALHO, Taipa de, *op. cit.,* p. 260 e ss. e DIAS, Jorge de Figueiredo, *op. cit.,* pp. 511 a 557.
[244] Cf. Art.º 20.º do C.P. De mais a mais, como menciona Taipa de Carvalho, "esta capacidade de avaliação da ilicitude do facto e de decisão constitui apenas o pressuposto do juízo de culpa jurídico-penal, e não o conteúdo material desta. O conteúdo material da culpa jurídico-penal e portanto, aquilo que se censura ao agente do facto típico-ilícito é a sua atitude ético-pessoal de oposição, indiferença ou de descuido perante o bem jurídico-penal lesado ou posto em perigo pela sua conduta", cf. CARVALHO, Taipa de, *op. cit.* p. 260.
[245] Cf. CARVALHO, Taipa de, *op. cit.* p. 489. Além disso, o Autor, relativamente à associação sistemática das causas de desculpação e das causas de justificação, expõe: "tal como as causas de justificação, também as causas de desculpação pressupõem situações de conflito de interesses. Assim, é razoável que o legislador tenha, no Código Penal, colocado lado a lado as causas de justificação e as causas de desculpação (…) Esta associação sistemática, que o Código Penal faz, das causas de desculpação às causas de justificação salienta que há um *denominador comum* a ambas, que é a existência de uma *situação de conflito de interesses*. Só que – e é este o *traço geral que distingue* estas duas categorias de causas – nas causas de desculpação não se verificam todos os pressupostos das causas de justificação; e, por isto, o facto praticado é ilícito, embora possa ser considerado não culposo", cf. CARVALHO, Taipa de, *op. cit.* p. 491

casu alguma das causas de exclusão da culpa[246] presentes no nosso ordenamento jurídico-criminal, as quais desde já elencamos[247]:

- **Inimputabilidade;**

- O excesso de legítima defesa asténico não censurável;

- O estado de necessidade desculpante;

- O conflito de deveres desculpante;

- A obediência indevida desculpante;

- **Erro sobre a ilicitude não censurável.**

No que diz respeito à **inimputabilidade**[248], esta pode ser em razão da idade (cf. art.º 19.º do C.P.) ou em razão de anomalia psíquica (art.º 20.º). Na nossa hipótese prática, partimos do pressuposto que o agente que procede ao *hack back* é maior de idade e que não padece de qualquer anomalia psíquica, pelo que a culpabilidade do mesmo não está afastada por esta via.

Quanto ao **excesso de legítima defesa asténico não censurável**, também não nos parece que esta causa de exculpação se verifique na nossa hipótese. Como já evidenciado[249], não se logrou demonstrar na mesma a existência da legítima defesa, não só porque não está verificado o pressuposto da necessidade do meio como também não estará verificado, eventualmente, o da atualidade da agressão (pois o ataque informático poderá já ter cessado). Ora, sobre o excesso de legítima defesa[250], refere TAIPA DE CARVALHO, que este "(…) caracteriza-se pela utilização de um meio de defesa desnecessário"[251] e adianta que "em geral, (…) consiste no facto de o defendente exercer uma *acção de defesa* que, embora adequada ou eficaz para impedir a agressão (ou a continuação desta), é todavia, *claramente mais intensa*, mais gravosa (…) que a necessária para realizar o objectivo de impedir

[246] *I.e., "circunstâncias que impedem que determinado acto considerado ilícito pela lei, seja atribuível de forma culposa ao seu autor"* cf. SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *op. cit.,* p. 113.
[247] Uma importante referência a efetuar desde já é a crítica da designação "não exigibilidade" avançada por Taipa de Carvalho, cf. CARVALHO, Taipa de, *op. cit.,* §476 e §871.
[248] Para mais esclarecimentos sobre a inimputabilidade: DIAS, Jorge de Figueiredo, *op. cit.,* pp. 560 – 596, CARVALHO, Taipa de, *op. cit.,* pp. 468 - 476 e GONÇALVES, Manuel Lopes Maia, *op. cit.,* pp. 122 - 128
[249] P. 61.
[250] *Vide* GARCIA, M. Miguez, *op. cit.,* pp. 459 – 467.
[251] Cf. CARVALHO, Taipa de, *op. cit*., p. 498

a agressão"[252]. Efetivamente, o meio de "defesa" não é meio necessário na hipótese vertida pois não é apto ou adequado a afastar a agressão. Mas em bom rigor, nem sequer existe intuito defensivo no acesso não autorizado mas antes, retaliação pelo ataque informático. Assim sendo, a ação de defesa não é adequada nem eficaz para impedir a agressão, pelo que nem sequer nos poderemos debruçar sobre o excesso de legítima defesa (nem tampouco se o excesso será asténico e não censurável).

Em relação ao **estado de necessidade desculpante**[253], estatui o n.º 1 do art.º 35.º do C.P. que "age sem culpa quem praticar um facto ilícito adequado a afastar um perigo actual, e não removível de outro modo, que ameace a vida, a integridade física, a honra ou a liberdade do agente ou de terceiro, quando não for razoável exigir-lhe, segundo as circunstâncias do caso, comportamento diferente". Em primeiro lugar, cumpre referenciar que o facto praticado é ilícito, *i.e.,* já foram avaliados os tipos justificadores da ilicitude e destes nenhum foi verificado, como o do direito de necessidade[254]. Depois - à semelhança do que sucede no direito de necessidade - no estado de necessidade desculpante é exigido a verificação da atualidade do perigo e que este não seja "removível de outro modo" (*i.e.,* que a conduta adotada pelo agente seja o único modo de remover o perigo, o que sempre implica um juízo sobre a adequação e indispensabilidade da ação salvadora[255]). De outro modo (e ao contrário do que sucede no direito de necessidade) esta causa de exculpação está associada tão-somente à defesa de bens jurídicos eminentemente pessoais (vida, integridade física, honra e liberdade)[256], do agente ou de terceiro[257]. Por fim, como indica TAIPA DE CARVALHO, "para

[252] *Ibid.*
[253] *Vide* GONÇALVES, Manuel Lopes Maia, *op. cit.,* p. 176 e ss. e GARCIA, M. Miguez, *op. cit.,* pp. 467 – 473.
[254] A este respeito, expõe Taipa de Carvalho: "o *estado de necessidade desculpante* pressupõe que a situação de conflito foi resolvida de modo ilícito, i. é, *pressupõe que o facto salvador praticado não respeitou as exigências ou pressupostos de que a lei (art. 34.º) faz depender a exclusão da ilicitude do facto típico praticado*. Pois que, se se tivessem verificado os pressupostos da justificação por direito de necessidade, não teria sentido levantar o problema da eventual desculpação", cf. CARVALHO, Taipa de, *op. cit.*, p. 512.
[255] *Vide* CARVALHO, Taipa de, *Ibid.*
[256] Nas situações em que esteja em causa um bem jurídico que não um bem jurídico de natureza eminentemente pessoal, estatui o n.º 2 do art.º 35.º C.P.: "Se o perigo ameaçar interesses jurídicos diferentes dos referidos no número anterior, e se verificarem os restantes pressupostos ali mencionados, pode a pena ser especialmente atenuada ou, excepcionalmente, o agente ser dispensado de pena", o que essencialmente significa que se a defesa se destinar ao salvamento de bens ou interesses jurídicos que não sejam eminentemente pessoais, não está excluída a culpa do agente, mesmo até que se verifiquem os requisitos exigidos pelo n.º1. No entanto, nessas circunstâncias, sempre pode a pena ser especialmente atenuada ou, excepcionalmente, o agente ser dispensado de pena.
[257] Como alude Figueiredo Dias, "uma vez que no estado de necessidade desculpante se não trata da vontade da ordem jurídica de preservação de bens jurídicos mais valiosos à custa de bens jurídicos de menor valor, mas de ser ou não exigível do agente, na concreta situação, um comportamento adequado ao direito, compreende-se que, segundo a lei positiva, a exclusão da culpa só possa ocorrer quando se trata de preservar determinados bens jurídicos individuais

haver a desculpação, é necessário que a motivação principal seja a de salvar o bem jurídico em perigo. Isto é, no estado de necessidade desculpante exige-se o elemento subjectivo específico do *animus salvandi*"[258]. Tendo estas considerações em mente, vejamos se o estado de necessidade desculpante se aplica na nossa hipótese.

Partindo do pressuposto que o *hack back* é ilícito (e não incide sobre o mesmo qualquer causa de justificação) e até admitindo que o ataque informático ainda perdura (registando-se o pressuposto da atualidade da agressão), ainda assim não se regista a adequação e indispensabilidade da ação salvadora. Uma vez mais, tal assenta no facto de que o acesso ao sistema informático do atacante pelo defensor não é o meio adequado para este afastar o perigo (ataque informático), que podia até ser removível de outro modo (através dos já mencionados ataques de negação de serviço). Além disso, na nossa hipótese, o agente contra-ataca para proteger bens que não são eminentemente pessoais, (aplicando-se assim o n.º 2 do art.º 35.º C.P.) e, concomitantemente, não existe o elemento subjetivo específico do *animus salvandi* pois a motivação principal do agente que procede ao *hack back* não se traduz propriamente no intuito de salvar um bem jurídico em perigo mas antes na pura retaliação. Destarte, não se verificam na nossa hipótese, pois, os requisitos do estado de necessidade desculpante, pelo que a culpa do agente também não estará afastada por esta via.

No entanto, se equacionarmos uma vez mais a situação em que o agente, alvo do ataque informático, vê registos fotográficos seus com conteúdo sexual presentes no seu sistema informático serem-lhe subtraídos e, chegando ao seu conhecimento que tais registos iriam, com toda a certeza, ser publicados nas horas seguintes e, por forma a evitar a publicação de tais imagens, o agente acede de forma não-autorizada ao sistema informático do atacante (subtraindo as referidas imagens, destruindo-as, etc.), a solução poderá ser outra. Admitindo também que por alguma razão não houve exclusão da ilicitude do facto por via dos tipos justificadores (o que não se concede, mas

elementares: concretamente, a vida, a integridade física, a honra ou a liberdade", cf. *op. cit.,* p. 613. Ainda sobre a expressão "quando não for razoável exigir-lhe comportamento diferente" importa verificar CARVALHO, Taipa de, *op. cit*., §903.

[258] Cf. CARVALHO, Taipa de, *op. cit*., p. 514.

se avança por mera hipótese de raciocínio), vejamos se estarão presentes os restantes pressupostos *in casu* do estado de necessidade desculpante. Entendemos que sim, pois não só se verificam os pressupostos da atualidade (perigo iminente da divulgação das referidas fotos) e da adequação e indispensabilidade da ação salvadora (pois o acesso ao sistema informático do atacante poderá ser a única forma de subtrair as fotos e impedir que as mesmas sejam divulgadas), mas também porque se regista o pressuposto da natureza dos bens ameaçados (que no caso em apreço são eminentemente pessoais – direito à honra[259]) e o elemento subjetivo específico do *animus salvandi,* pois a motivação principal do agente é salvar um bem jurídico em perigo – a sua honra (bem como a reserva da vida privada e até integridade moral).

Relativamente à situação do **conflito de deveres desculpante**, importa referir que, à semelhança do que acontece com o conflito de deveres (justificante), para que se registe tal causa de exculpação, necessário é que exista uma situação de conflito entre dois deveres de ação. Assim, como na nossa hipótese, mais uma vez, não se revela a presença do conflito de deveres, porque não impende sobre o agente um dever de ação, (nomeadamente o dever de na sequência de um ataque informático, contra-atacar e aceder ao sistema informático do atacante "primitivo"), não se verifica também esta causa de exculpação.

Voltemos à temática da obediência hierárquica, desta vez para analisar a eventual existência da **obediência indevida desculpante**[260], enquanto motivo que afasta a culpa do agente, que no exercício das suas funções e no cumprimento de uma ordem de um superior hierárquico, pratica o *hack back* na sua forma de acesso ilegítimo e acede ao sistema informático do atacante. Quando analisamos a obediência hierárquica em sede de causas de justificação, observamos que na nossa hipótese, porque a ilicitude criminal da

[259] A respeito da natureza dos bens jurídicos em perigo, Taipa de Carvalho avança que "(…) é muito discutível que se inclua a honra no círculo dos bens que podem estar na base da desculpação do agente", cf. CARVALHO, Taipa de, *op. cit*., p. 513. No nosso entender, não é descabido a honra constar no elenco dos bens presentes no art.º 35.º pois pode haver um perigo tal para a honra que constitua uma lesão incomportável no princípio da dignidade humana, tal como acontece no nosso caso. Defender que a honra deveria ser excluída do no referido elenco, teria consequências extremamente injustas e gravosas para o agente da hipótese em apreço.

[260] *Vide* GARCIA, M. Miguez, *op. cit.,* pp. 477 – 480 e BRANDÃO, Nuno, *op. cit.*

ordem é sindicável pelo inferior hierárquico[261], o referido agente ao cumprir a ordem (de proceder ao acesso ilegítimo ao sistema informático do atacante como forma de contra-ataque), também cometia um ilícito criminal e assim sendo, devia sem mais recusar a ordem, sob pena de ele mesmo incorrer em responsabilidade criminal, pois não está justificada a ilicitude do facto. Assim, importa agora verificar se haverá lugar à obediência indevida desculpante enquanto motivo que afasta a culpa do agente na prática de tal facto. Ora, em primeiro lugar, estatui o art.º do C.P. 37.º: "Age sem culpa o funcionário que cumpre uma ordem sem conhecer que ela conduz à prática de um crime, não sendo isso evidente no quadro das circunstâncias por ele representadas". Quer isto dizer que não sendo evidente a ilicitude criminal do acto ordenado, haverá então exclusão da culpa do inferior, mesmo tendo este cometido um ilícito[262]. Na nossa hipótese, parece-nos manifestamente evidente que tal factualidade típica e ilícita deveria ser apreendida pelo homem médio, colocado neste caso em concreto, que deveria conhecer que aceder a sistemas de informação sem estar autorizado, constitui um ilícito criminal, pelo que não está excluída a sua culpa.

De todo o modo, é importante assinalar que, tal como defende TAIPA DE CARVALHO, "(…) esta causa de exclusão da culpa (…) não é uma causa de desculpação em sentido estrito (…) mas sim uma hipótese de erro sobre a ilicitude não censurável"[263]. Assim, importa que nos ocupemos da temática do **erro sobre a ilicitude não censurável**[264], enquanto causa de exculpação.

Em termos jurídico-penais, o erro, como é consabido, é uma ausência ou falsa representação da realidade[265]. No que diz respeito ao erro sobre a ilicitude, previsto no art.º 17.º do C.P., este pode ser censurável ou não censurável, ou seja, a ausência ou deficiente consciência da ilicitude do facto

[261] O agente, subordinado, devia ter-se recusado a cumprir a ordem, o que aliás encontra suporte na letra da lei: "o dever de obediência hierárquica cessa quando conduzir à prática de um crime" (art.º 36.º n.º 2 do C.P.)
[262] *Vide* CARVALHO, Taipa de, *op. cit.*, §923.
[263] Cf. CARVALHO, Taipa de, *op. cit.,* pp. 521 – 522. O Ilustre Autor complementa aludindo que "(…) no caso da "obediência indevida desculpante", o que existe é verdadeira e exclusivamente um erro sobre a ilicitude do facto ordenado pelo superior e praticado pelo inferior. (…) Assim, a hipótese contemplada no art.º 37.º já estaria incluída no art.º 17.º - 1. A única vantagem prática da autonomização sistemática deste erro sobre a ilicitude não censurável foi a de tornar claro que este erro do inferior sobre a ilicitude é sempre não censurável." cf. CARVALHO, Taipa de, *Ibid.*
[264] Recomenda-se a leitura de DIAS, Jorge de Figueiredo, *O Problema da Consciência da Ilicitude em Direito Penal*, 6.ª ed., Coimbra Editora, 2009; DIAS, Augusto Silva, "Faz sentido punir o ritual do fanado?", RPCC 16, 2006 e SERRA, Teresa, *Problemática do Erro Sobre a Ilicitude*, Almedina, 1991.
[265] *Vide* PINTO, Frederico de Lacerda da Costa, "Erro de tipo e erro de proibição", Faculdade de Direito da Universidade Nova de Lisboa, 2007, disponível em: fd.unl.pt/docentes_docs/ma/tpb_MA_4894.doc, consultado a 1 de Junho de 2015.

por parte do agente eventualmente dará lugar a um juízo de censura sobre o mesmo. Tal ausência ou falsa consciência da ilicitude, sendo censurável, significa que o agente é punido pelo facto a título de dolo mas pode a pena ser especialmente atenuada (art.º 17.º, n.º 2 C.P.). Não sendo censurável, exclui a culpa do agente (conforme o disposto no n.º 1 do art.º 17.º C.P. e ao contrário das modalidades de erro previstas no art.º 16.º C.P., que excluem a imputação dolosa do facto ao agente) pelo que este não poderá ser punido, mesmo tendo cometido um ilícito. Uma importante nota a efetuar é a de que nos crimes cuja punição é conhecida pela sociedade em geral, o erro sobre a ilicitude sempre se enquadrará no art.º 17.º do C.P., ao passo que nos crimes cuja punibilidade ainda não está bem consolidada na consciência comunitária e como tal não é conhecida por todos os cidadãos, o erro será o previsto no art.º 16.º do C.P.[266], com as consequências que daí advêm. O Legislador não concretizou no art.º 17.º como é apurada a censurabilidade do erro, pelo que nos socorremos do entendimento perfilhado por TAIPA DE CARVALHO, que expõe que o erro não será censurável "(…) quando a falta de consciência da ilicitude do facto praticado não for reveladora de uma atitude ético-pessoal de indiferença perante o dever-ser jurídico-penal, tal falta ou erro tem o efeito de uma causa de exclusão da culpa"[267] ou, de outra maneira, será censurável quando "(…) for revelador de uma personalidade ou atitude ético-pessoal de indiferença perante o bem jurídico lesado ou posto em perigo, então *há culpa* (culpa dolosa) e o agente é punível pelo respectivo crime doloso"[268].

Munidos destas considerações, voltemos uma última vez à nossa hipótese prática. É nosso entendimento que o agente que contra-ataca e acede ao sistema informático do atacante atua com uma plena indiferença perante o bem jurídico-penal inviolabilidade dos sistemas informáticos. Na verdade, o agente, ao proceder ao *hack back,* na forma de acesso ilegítimo, pretende

[266] Neste sentido: "O erro sobre a ilicitude ou sobre a punibilidade que exclui o dolo (artº 16º1 CP) apenas se deve e pode referenciar aos crimes cuja punibilidade não se pode presumir conhecida de todos os cidadãos. (…) Aos crimes cuja punibilidade se pode presumir que seja conhecida por todos os cidadãos, o eventual erro sobre a ilicitude só pode ser subsumível ao artº 17º CP, em caso em que a culpa só é afastada se a falta de consciência da ilicitude do facto decorre de erro não censurável. (…) A censurabilidade só é de afastar se e quando se trate de proibições de condutas cuja ilicitude material não esteja devidamente sedimentada na consciência ético social", cf. Acórdão do Tribunal da Relação do Porto, de 25-02-2015, Processo n.º 120/08.3GCBGC-A.G1.P1, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/890e919fcf20bd4d80257e0300579e86?OpenDocument, consultado a 22 de Setembro de 2015. Sobre a relação entre o erro sobre a proibição legal (art.º 16.º, n.º1 C.P.) e o erro sobre a ilicitude (art.º 17º C.P.), remetemos para CARVALHO, Taipa de, *op. cit*., § 864.

[267] Cf. CARVALHO, Taipa de, *op. cit*., p. 486.

[268] *Ibid.*

puramente retaliar contra o atacante primitivo, mostrando-se o bem em questão irrelevante para o agente[269]. Assim, não nos parece que na nossa hipótese se registe erro sobre a ilicitude não censurável.

Assim, e já em jeito de conclusão, entendemos que podemos responder à questão avançada, mormente, se a prática do *hack back* por um agente será legalmente admissível. Entendemos que (em regra) não o é. Esta conduta é típica e culposa e a consequência será inevitavelmente a punição do agente em questão pela prática de um crime de acesso ilegítimo, previsto e punido pelo art.º 6.º da Lei do Cibercrime. Destarte, não nos parece que o *hack back,* enquanto contra-ataque informático, deva ser uma medida a figurar lado a lado com os mecanismos fornecidos pelos já analisados sistemas de segurança ativa. No entanto, também observarmos que em situações excecionais (*v.g.* quando os bens jurídicos que se visam proteger pela via do *hack back* são sensivelmente superiores aos do atacante e tal contra-ataque constituir o único meio e meio necessário a salvar os mesmos, evitando a sua lesão irreversível) registam-se motivos que afastam a ilicitude do facto ou a culpa do agente.

.

[269] Interessante seria averiguar se não existiria um erro sobre pressupostos das causas de justificação ou um erro sobre pressupostos das causas de desculpação (art.º 16.º, n.º 2 do C.P.) quando, admitindo por hipótese de raciocínio, que não se tinha registado qualquer causa de justificação ou de exculpação na hipótese em que o agente, alvo do ataque informático, vê registos fotográficos seus com conteúdo sexual presentes no seu sistema informático serem-lhe subtraídos e chegando ao seu conhecimento que tais registos iriam com toda a certeza ser publicados nas horas seguintes e, por forma a evitar a publicação de tais imagens, o agente acede de forma não-autorizada ao sistema informático do atacante (subtraindo as referidas imagens, destruindo-as, etc.), julgando que o faz ao abrigo de uma causa de exclusão da ilicitude ou da culpa.

CONCLUSÕES

A nossa investigação permitiu-nos compreender o crime informático de acesso ilegítimo, quanto à sua génese e evolução e ainda quanto às suas dimensões na atualidade, dos pontos de vista técnico, jurídico e até social.

Percebemos, pois, que o crime de acesso ilegítimo foi um dos primeiros crimes informáticos a surgir no panorama informático-penal, motivado pelo uso exponencial da Internet e das tecnologias de informação e comunicação e é ainda um dos ilícitos mais ocorrentes nesse plano, com consequências cada vez mais imprevisíveis.

Observamos que a nível europeu, atendendo ao forte crescimento da criminalidade informática em geral, do seu carácter transfronteiriço e com vista a dar uma resposta efetiva à mesma, foi elaborada a Recomendação 9/89, a qual tinha como objetivo promover a harmonização do direito interno comunitário e a cooperação judiciária nesta matéria, recomendando os Estados-Membros a legislar de forma a combater a criminalidade informática, seguindo o relatório sobre criminalidade informática elaborado pelo Comité Europeu para os Problemas Criminais do Conselho da Europa. Constatamos que neste relatório surgia então o crime de "acesso não autorizado", sugerindo a incriminação do "acesso ilícito a um sistema informático ou rede através da violação de medidas de segurança".

Examinamos que entre nós, e após a Recomendação 9/89 do Conselho Europeu, o crime de acesso ilegítimo foi originalmente previsto e punido através da Lei n.º 109/1991, de 17 de Julho (Lei da Criminalidade Informática), a qual no seu art.º 6.º referia que "Quem, não estando para tanto autorizado e com a intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos, de qualquer modo aceder a um sistema ou rede informáticos será punido com pena de prisão até 1 ano ou com pena de multa até 120 dias*"*. Constatamos que era assim exigido o preenchimento de um elemento tipificador objetivo (aceder de forma não autorizada a um sistema ou rede informática) e de um elemento tipificador subjetivo (pretender alcançar para si ou para terceiro, um beneficio ou uma vantagem ilegítima).

Verificamos também que mais tarde, viria a tomar lugar a Convenção sobre o Cibercrime, a qual foi o primeiro tratado internacional em termos de previsão, combate e sancionamento da criminalidade informática a nível mundial. Constatamos, também, que no seu Capítulo II, Secção 1, Título I, art.º 2.º esta refere que: "Cada Parte deverá adoptar as medidas legislativas e outras que se revelem necessárias para classificar como infracção penal nos termos do seu direito interno, quando praticado intencionalmente, o acesso ilícito a um sistema informático no seu todo ou a parte dele. Para que se verifique a infracção penal, qualquer uma das Partes pode exigir que ela seja cometida por meio da violação das medidas de segurança com intenção de obter dados informáticos ou com qualquer outra intenção, ou ainda que esteja relacionada com um sistema informático conectado a outro sistema informático".

Observamos igualmente que na sequência da Convenção sobre o Cibercrime, o Conselho da União Europeia viria também a emitir a Decisão-Quadro 2005/222/JAI do Conselho de 24 de Fevereiro de 2005, relativa a ataques contra os sistemas de informação e que no seu art.º 2.º, sob a epígrafe "Acesso ilegal aos sistemas de informação" estipulava que "Os Estados-Membros devem tomar as medidas necessárias para assegurar que o acesso intencional, não autorizado, à totalidade ou a parte de um sistema de informação seja punível como infracção penal, pelo menos nos casos que não sejam de menor gravidade" e que "Os Estados-Membros podem decidir que os comportamentos referidos no n.o 1 são puníveis apenas quando a infracção tiver sido cometida em violação de uma medida de segurança".

Verificamos ainda que em 2009, por força da Convenção sobre o Cibercrime e da Decisão-Quadro 2005/222/JAI, o Legislador Português viria a elaborar a Lei n.º 109/2009, de 15 de Setembro para prever e punir a criminalidade informática, intitulada Lei do Cibercrime, que revogou expressamente a Lei n.º 109/91, de 17 de Agosto (Lei da Criminalidade Informática) e diploma esse que ainda hoje regula a matéria da criminalidade informática no ordenamento jurídico português.

Constatamos que a nova redação do tipo legal respeitante ao crime de acesso ilegítimo prescindiu do elemento tipificador subjetivo. Assim, segundo o art.º 6.º da Lei n.º 109/2009, de 15 de Setembro para haver lugar à punição pela prática por este ilícito basta que "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 (…)". Assim, constatamos que o âmbito de aplicação da norma foi extremamente alargado, abarcando todo o acesso não autorizado a um sistema informático (seja o acesso a parte ou a todo o sistema), pelo que não se tem em consideração a intenção do agente – assim, para efeitos de caracterização da conduta típica punível, esta traduz-se no simples ato de aceder sem permissão legal ou autorização a um sistema informático. Entendemos que apesar de tal alteração facilitar bastante a persecução e punição deste ilícito, esta não deixa de estar isenta de críticas. Relativamente ao bem jurídico protegido pelo tipo legal do acesso ilegítimo, seguindo o entendimento de PEDRO FREITAS, percebemos que aquilo que é protegido pela norma é a inviolabilidade dos sistemas informáticos.

Ademais, para além da análise dogmática, procedemos também a uma análise etimológica dos conceitos de *Hack*, *Hacker* e *Hacking*. Tal análise permitiu-nos perceber que estes conceitos não são estanques e são inclusivamente associados a diferentes circunstancialismos. Para os fins da nossa investigação, identificamos *hack* com o ato de aceder a um sistema, seja de forma lícita ou ilícita, *hacker* como o indivíduo que usa *hacks* para aceder a um sistema informático e identificamos ainda o *hacking* como a própria conduta de aceder (seja de forma legitima ou ilegítima) a um sistema informático, o que significa que *hacking* é uma atividade (mais ampla) que se pode subdividir em duas grandes atividades, no acesso legítimo (ou *ethical hacking*) e no acesso ilegítimo. Propusemos ainda uma taxonomia dos *hackers*, tendo por base o tipo de acesso (legitimo ou ilegítimo) por estes praticado e as suas intenções (benignas ou malignas).

Em jeito de antecipação do futuro do tipo legal do acesso ilegítimo, analisamos também 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. Segundo a mesma, percebemos que para haver lugar a responsabilidade criminal pelo acesso ilegítimo, necessariamente terá de existir, concomitantemente, a violação de medidas de segurança. A Diretiva propõe também a exclusão da responsabilidade penal nas situações em que, mesmo estando preenchidos os elementos tipificadores objetivos do crime de acesso ilegítimo, este é praticado sem "intenção criminosa", especificando a título de exemplo a situação do erro sobre as circunstâncias do facto.

A nossa investigação permitiu-nos também perceber a temática da segurança informática (e da cibersegurança) e importância que a mesma assume numa sociedade tão dependente de tecnologias de informação e comunicação como a nossa. Observamos que a segurança informática visa essencialmente garantir que os recursos físicos ou digitais (*v.g. software*) de uma dada organização sejam utilizados exclusivamente para o seu proposto fim. Analisamos igualmente os sistemas de proteção ativa e passiva e das funcionalidades a que estes se propõem. Vimos que uns e outros sistemas não estão imunes de críticas e como tal, é já propagada a apologia por alguns Autores e instituições do chamado *hack back.* A nossa investigação, leva-nos a crer que *hack back* é a expressão utilizada para caracterizar o contra-ataque informático, *i.e.,* aceder ao sistema informático do atacante, intercetar os seus dados informáticos e ainda danificar ou destruir o sistema do atacante. Mas o *hack back* poderá ainda consistir na elaboração de ataques informáticos de forma preventiva por um potencial lesado. A nossa investigação permitiu-nos ainda caracterizar os conceitos de *pentests* e *backtrack,* que são ferramentas informáticas que permitem prática do *hack back* (mas não só).

O nosso trabalho permitiu-nos também perceber que o *hack back*, quer na sua modalidade de acesso não autorizado a sistemas informáticos, quer na modalidade de interceção ilegítima em tais sistemas, é um tema controverso, a vários níveis e que importa sempre uma reflexão não só jurídica, mas também técnica, política e até sociológica. Juridicamente, e com base nas disposições legais nacionais e internacionais, afirmamos que este fenómeno é ilícito e configura, na sua modalidade de acesso informático, um crime de acesso ilegítimo, pelo que se torna absolutamente essencial averiguar se haverá lugar

a alguma causa de exclusão da ilicitude ou da culpa no âmbito do *hack back*, especificamente através do acesso ilegítimo do sistema informático do atacante por parte de uma empresa ou de um particular. Para tanto, e perante a agregação de todas as referidas análises, procedemos ao confronto de uma situação de *hack back* com as causas de exclusão da ilicitude e da culpa no ordenamento jurídico português. Tal confronto operou através da condensação de uma hipótese prática: o caso de uma pessoa (seja singular ou coletiva), que na sequência de um ataque informático em que é visada, contra-ataca e acede ao sistema informático do atacante, (praticando assim o *hack back*).

Assim analisamos numa primeira fase os elementos que constituem o crime (conduta, tipicidade, ilicitude e culpa) e, posteriormente, analisamos as causas de justificação (causas que excluem a ilicitude do facto e as causas de exculpação (motivos que anulam a culpa do agente na produção do facto). Esta análise permitiu-nos proceder à compreensão do *hack back* ao nível da ilicitude e da culpa.

Quanto a este fenómeno, observamos que, em regra, o acesso não autorizado a um sistema informático alheio, mesmo na sequência de um ataque informático, não é justificado por uma das causas de exclusão da ilicitude (exceto no caso de se registar consentimento prévio para tanto, o que dificilmente acontecerá). De igual modo, inexistem motivos que levem ao agente em causa a ser desculpado (exceto no caso de inimputabilidade do agente, hipótese que registando-se, sempre levará à exclusão da culpa do agente).

No entanto, mesmo esta é uma conclusão permeável, pois há que ter em consideração, a todo o momento, o caso concreto.

Com efeito, vimos que no caso de um agente, alvo de um ataque informático no qual vê registos fotográficos seus com conteúdo sexual presentes no seu sistema informático serem-lhe subtraídos e, havendo certeza absoluta que tais registos irão ser publicados nas horas seguintes, por forma a evitar a publicação de tais imagens, o agente acede de forma não-autorizada ao sistema informático do atacante (subtraindo as referidas imagens,

destruindo-as, etc.) a conclusão quando à admissibilidade do recurso às causas de exclusão da ilicitude ou da culpa poderá ser radicalmente diferente.

Assim, perante esta "sub-hipótese" (que sugerimos como hipótese de raciocínio), observamos que a **ação direta** prevista no art.º 336.º do C.C., o **direito de necessidade** (ou estado de necessidade justificante) e o **direito de necessidade defensivo** (ou estado de necessidade defensivo) são causas que afastam a ilicitude da factualidade em apreço. Ademais, verificamos que o **estado de necessidade desculpante** afasta a culpa do agente que pratica tal factualidade.

Posto isto, chegamos também à conclusão que a prática do *hack back* por uma pessoa (singular ou coletiva) não é legalmente admissível. A conduta em si mesma é típica e culposa e a consequência será inevitavelmente a punição do agente em questão pela prática de um crime de acesso ilegítimo, previsto e punido pelo art.º 6.º da Lei do Cibercrime.

Assim, entendemos que o *hack back*, enquanto contra-ataque informático, não deverá ser uma medida a figurar lado a lado com os mecanismos fornecidos pelos já analisados sistemas de segurança ativa. No entanto, verificamos que em situações excecionais (mormente, quando os bens jurídicos que se visam proteger pela via do *hack back* são sensivelmente superiores aos do atacante, e tal contra-ataque constituir o único meio e meio necessário a salvar os mesmos, evitando a sua lesão irreversível) registam-se causas que afastam a ilicitude do facto ou a culpa do agente.

Assim, é sempre fundamental que se proceda a uma profunda análise do caso concreto, bem como uma ponderação dos interesses jurídicos em questão e uma verificação plena de todos os pressupostos (das causas de exclusão da ilicitude ou da culpa) para que a justificação ou a exculpação opere.

Da nossa parte, deixamos ao dispor da comunidade jurídica este contributo, saudando aqueles que nele vislumbrarem alguma pertinência para investigações futuras.

BIBLIOGRAFIA

AKHGAR, Babak, STANIFORTH e Andrew, BOSCO, Francesca (eds.), *Cyber Crime And Cyber Terrorism Investigator's Handbook*, Elsevier Science, 2014.

ALBANESIUS, Chloe, "White House Threatens to Veto CISPA", disponível em: http://www.pcmag.com/article2/0,2817,2403549,00.asp, consultado a 10 de Agosto de 2015.

ALBUQUERQUE, Paulo Pinto de, *Comentário do Código Penal à luz da Constituição da República Portuguesa e da Convenção Europeia dos Direitos do Homem*, Lisboa: Universidade Católica Editora, 2008.

ALBUQUERQUE, Paulo Pinto de e BRANCO, José, *Comentário das Leis Penais Extravagantes – Volume I,* Universidade Católica Editora, 2010.

ALBUQUERQUE, Paulo Pinto de e BRANCO, José, *Comentário das Leis Penais Extravagantes – Volume II,* Universidade Católica Editora, 2011.

ALPEROVITCH, Dmitri, "Active Defense: Time for a New Security Strategy", disponível em: http://blog.crowdstrike.com/active-defense-time-new-security-strategy/, consultado a 10 de Agosto de 2015.

ANDERSON, Kent, "Intelligence-based Threat Assessments for Information Networks and Infrastructures", Network Risk Management, LLC, 2005, disponível em: http://www.aracnet.com/~kea/Papers/threat_white_paper.pdf, consultado a 1 de Agosto de 2015.

ANDRADE, Costa, *Consentimento e acordo em Direito Penal: Contributo para a fundamentação de um paradigma dualista*, Coimbra Editora, 1991.

ANDRADE, Manuel da Costa e NEVES, Rita Castanheira, *Direito Penal Hoje - Novos desafios e novas respostas*, Coimbra Editora, 2009.

ANDRADE, José Carlos Vieira de, *Os Direitos Fundamentais na Constituição Portuguesa de 1976,* Almedina, 2012.

ANTUNES, Maria João, *Consequências jurídicas do crime*, 1.ª ed., Coimbra Editora, 2013.

ASCENSÃO, José de Oliveira – "A teoria finalista e o ilícito civil", in *Direito e Justiça*, vol. II, 1981-1986, p. 92 e ss.

ASCENÇÃO, José de Oliveira, "Criminalidade Informática", in *Direito da Sociedade da Informação*, vol. II, Coimbra Editora, 2001.

ASCENÇÃO, José de Oliveira, *Estudos sobre Direito da Internet e da Sociedade da Informação,* Almedina, 2001.

ATKINSON, Sean, "Psychology and the hacker – Psychological Incident Handling", SANS Institute, 2015, disponível em: http://www.sans.org/reading-room/whitepapers/incident/psychology-hacker-psychological-incident-handling-36077, consultado a 29 de Julho de 2015.

BARZILAY, Menny, "A simple definition of cybersecurity", disponível em: http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296, consultado a 23 de Outubro de 2015.

BEBBINGTON, Shaun "What is computer programming?", disponível em: http://yearofcodes.tumblr.com/what-is-programming, consultado a 2 de Julho de 2015.

BELEZA, Teresa, "Legítima defesa e género feminino", in *Revista Crítica de Ciências Sociais*, n.º 31, 1991.

BLANKENSHIP, Loyd, "The Conscience of a Hacker", disponível em: http://phrack.org/issues/7/3.html, consultado a 15 de Março de 2015.

BOWKER, Art, *"*Hackers, Crackers, Tramps and Thieves*",* disponível em: http://www.corrections.com/news/article/28572-hackers-crackers-tramps-and-thieves, consultado a 10 de Março de 2014.

BRADBURY, Danny, "Should we hack the hackers?", disponível em: http://www.theguardian.com/technology/2015/mar/09/cybercrime-should-we-hack-the-hackers?CMP=share_btn_fb, consultado a 20 de Setembro de 2014.

BRANDÃO, Nuno, *Justificação e desculpa por obediência em direito penal*, Dissertação de Mestrado, FDUC, 2004.

BRAVO, Rogério, "O Crime de acesso ilegítimo na Lei da Criminalidade Informática e na Ciberconvenção", in *Direito na Rede n.º 1* [*on-line*], Ordem dos Advogados, Lisboa, 2004, disponível em: http://www.academia.edu/2039178/O_Crime_de_Acesso_Ilegi_timo_na_Lei_da_Criminalidade_Informa_tica_e_na_CiberConvenc_a_o, consultado a 15 de Março de 2014.

BRITO, Teresa de, *O Direito de necessidade e a legítima defesa no Código Civil e no Código Penal*, Lex-Edições Jurídicas, 1994.

CAEIRO, Pedro, *Fundamento, Conteúdo e Limites da Jurisdição Penal do Estado*, Coimbra Editora, 2010.

CALKINS, Mary M., 2000–2001. "They Shoot Trojan Horses, Don't They - An Economic Analysis of Anti-Hacking Regulatory Models." *Georgetown Law Journal* 89, 2000. pp. 171–224.

CARVALHO, Américo Taipa de, *A Legítima Defesa*, Coimbra: Coimbra Editora, 1995.

CARVALHO, Américo Taipa de, *Direito Penal - Parte Geral - Questões Fundamentais – Teoria Geral do Crime,* Coimbra Editora, 2ª ed, 2014.

CARVALHO, João Álvaro, "Desenvolvimento de Sistemas de Informação: Da Construção de Sistemas Informáticos à Reengenharia Organizacional"

disponível em: http://www3.dsi.uminho.pt/jac/documentos/DSI.pdf, consultado a 14 de Outubro de 2015.

CASABONA, Carlos Romeo, "De los Delitos Informáticos al Cibercrimen. Una Aproximación Conceptual y Político-Criminal", in «*El Cibercrimen: Nuevos Retos Jurídico-Penales, Nuevas Respuestas Político-Criminales*», Editorial Comares, 2006.

CASTELLS, Manuel, "Hackers, crackers, seguridad y libertad" - *Lección inaugural del curso académico 2001-2002 de la UOC*, UOC, 2001, disponível em: http://www.uoc.edu/inaugural01/esp/hackers.html, consultado a 17 de Junho de 2015.

CASTELLS, Manuel, *La Galaxia Internet. Reflexiones sobre Internet, empresa y sociedad*, Madrid: Areté, 2001.

CAVELTY, Myriam Dunn, "A Comparative Analysis of Cybersecurity Initiatives Worldwide", *WSIS Thematic Meeting on Cybersecurity*, Genebra, 28 de Junho a 1 de Julho de 2005, ITU, 2005, disponível em: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf, consultado a 4 de Agosto de 2015.

CAVELTY, Myriam Dunn, *Cyber-Security and Threat Politics*, London, New York: Routledge, 2008.

CAVELTY, Myriam Dunn e MAUER, Victor, (eds) *The Routledge Handbook of Security Studies*, London, New York: Routledge, 2010.

CHOO, Kim-Kwang Raymond e SMITH, Russell G., "Criminal Exploitation of Online Systems by Organized Crime Groups", *Asian Journal of Criminology*, 1 (2008), pp. 37-59.

CLIFFORD, Ralph D., *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime*, 3.ª ed., Carolina Academic Press, 2011.

CLOUGH, Jonathan, “Data Theft? Cybercrime and the Increasing Criminalization of Access to Data”, *Criminal Law Forum,* 22 (1), 2011, pp. 145-170.

CLOUGH, Jonathan, “The Council of Europe Convention on Cybercrime: Defining ‘Crime’ in a Digital World”, *Criminal Law Forum,* 23 (4) (2012), pp. 363-391.

CLOUGH, Jonathan, *Principles of Cybercrime*, 1.ª ed., Cambridge University Press, 2010.

COHN, Scott, “Companies Battle Cyberattacks Using 'Hack Back'*”,* disponível em: http://www.cnbc.com/id/100788881, consultado a 7 de Agosto de 2015.

COLAÇO, Bernardo, “O crime informático na legislação portuguesa”, in RMP, ano 15, n.º 57, pp. 125-128.

COLEMAN, Gabriella, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous,* 1.ª ed., London; New York, Verso, 2014.

COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION CRIMINAL DIVISION, *Prosecuting Computer Crimes*, 2.ª ed., *Office of Legal Education Executive Office for United States Attorneys* (sem data), p. 180, disponível em: http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf, consultado a 10 de Agosto de 2015.

CORREIA, Eduardo, *Direito Criminal II,* Coimbra, 1965.

CORREIA, Miguel Pupo e SOUSA, Paulo Jorge, *Segurança no Software*, Lisboa: FCA–Editora de informática, 2010.

COSTA, José de Faria, *Direito Penal da Comunicação - Alguns escritos*, Coimbra Editora, 1998.

COSTA, José de Faria, “Formas do Crime” in *Jornadas de Direito Criminal*, CEJ, 1983

COSTA, José de Faria, *Noções Fundamentais de Direito Penal* (*Fragmenta Iuris Poenalis*), Coimbra, 2.ª ed., reimpressão, 2010.

COSTA, José de Faria, *O Perigo em Direito Penal*, Coimbra Editora, 1992

DAINTITH, John e WRIGHT, Edmund (eds), *A Dictionary of Computing*, 6.ª ed., 2010.

DELIO, Michelle, "The Greatest Hacks of All Time", disponível em: http://archive.wired.com/science/discoveries/news/2001/02/41630?currentPage=all, consultado a 1 de Julho de 2015.

DEPARTMENT OF DEFENSE, *Department of Defense Strategy for Operating in Cyberspace*, 2011, disponível em: http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf, consultado a 7 de Agosto de 2015.

DEPARTMENT OF DEFENSE, *Dictionary of Military and Associated Terms*, Joint Publication 1-02 (April 12, 2001; as amended June 13, 2007).

DEWAR, ROBERT S., "The "Triptych of Cyber Security: A Classification of Active Cyber Defence", in *2014 6th International Conference on Cyber Conflict,* NATO CCD COE Publications, Tallinn, 2014*,* disponível em: https://ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf, consultado a 6 de Agosto de 2015.

DIAS, Augusto Silva, *Ramos Emergentes do Direito Penal Relacionados com a Protecção do Futuro (Ambiente, Consumo e Genética Humana),* Coimbra Editora, 2008.

DIAS, Augusto Silva, "Faz sentido punir o ritual do fanado?", RPCC 16, 2006.

DIAS, Jorge de Figueiredo *et al, Comentário Conimbricense do Código Penal – Tomo I,* Coimbra Editora, 2012.

DIAS, Jorge de Figueiredo *et al, Comentário Conimbricense do Código Penal – Tomo II,* Coimbra Editora, 1999.

DIAS, Jorge de Figueiredo *et al, Comentário Conimbricense do Código Penal – Tomo III,* Coimbra Editora, 2012.

DIAS, Jorge de Figueiredo, *Direito Penal – Parte Geral – Tomo I – Questões Fundamentais; A Doutrina Geral do Crime,* Coimbra Editora, 2012.

DIAS, Jorge de Figueiredo, *O Problema da Consciência da Ilicitude em Direito Penal,* 6.ª ed., Coimbra Editora, 2009.

DINNISS, Heather Harrison, "Cyber Warfare and the Laws of War", *Cambridge Studies in International and Comparative Law*, n.º 92, Cambridge University Press, 2014.

DITTRICH, David "The Active Response Continuum: Ethical and Legal Issues of Aggressive Computer Network Defense", 2013, disponível em: https://staff.washington.edu/dittrich/arc/book/definitions.html, consultado a 15 de Agosto de 2015.

EIJNDHOVEN, Don, "Dutch Police Hacking Back - A Privacy Violation Waiting to Happen", disponível em: http://www.securitycurrent.com/en/news/ac_news/dutch-police-hacking-back-a-privacy-violation-waiting-to-happen, consultado a 10 de Agosto de 2015.

ERICKSON, Jon, *Hacking: The Art of Exploitation*, 2.ª ed., San Francisco, CA: No Starch Press, 2008.

EUROPEAN COMMITTEE ON CRIME PROBLEMS AND COUNCIL OF EUROPE, *Computer-related Crime: Recommendation No. R. (89) 9 on Computer-related Crime and Final Report of the European Committee on Crime Problems,* Council of Europe, Pub., 1990, disponível em: http://www.oas.org/juridico/english/89-9&final%20Report.pdf, consultado a 15 de Setembro de 2014.

FERRER, Mercè Molist, "Hackers portugueses y un catalán montaron la primera campaña hacktivista de la historia", disponível em:

http://www.elmundo.es/tecnologia/2015/04/26/553d20bc22601d6c248b456d.html, consultado a 26 de Abril de 2015

FERRER, Mercè Molist, "La historia nunca contada del underground hacker en la Península Ibérica", disponível em: http://hackstory.es/, consultado a 22 de Outubro de 2015.

FIELD, Tom, *"*Legal Merits of 'Hack Back' Strategy*"*, disponível em: http://www.bankinfosecurity.com/interviews/legal-merits-hack-back-strategy-i-1729/op-1#, consultado a 10 de Agosto de 2015

FREITAS, Pedro, "Breves nótulas sobre o crime de acesso ilegítimo previsto na Lei do Cibercrime*"*, artigo apresentado no IV Simpósio de Segurança Informática e Cibercrime, Instituto Politécnico de Beja, 2013.

FREITAS, Pedro e GONÇALVES, Nuno, "Illegal access to information systems and the Directive 2013/40/EU*"*, *International Review of Law, Computers & Technology*, 2015.

FRIZELL, Sam, "Here's How Sony Is Hacking Back to Defend Itself", disponível em: http://time.com/3629768/sony-hack-hackers/, consultado a 11 de Agosto de 2015.

GARCIA, M. Miguez, *O Risco de Comer uma Sopa e Outros Casos de Direito Penal. I - Elementos da Parte Geral,* 2.ª ed., Almedina, 2012

GARIGUE, Robert, "Information Warfare - Developing a Conceptual Framework*"*, disponível em: http://all.net/books/iw/iwframe/index.html, consultado a 6 de Agosto de 2015.

GONÇALVES, Manuel Lopes Maia*, Código Penal Português - Anotado e Comentado - Legislação Complementar,* 18.ª ed., Almedina, 2007.

GONÇALVES, Nuno Filipe de Sousa, *O Recurso às Acções Encobertas no Âmbito da Lei do Cibercrime,* Dissertação de Mestrado em Direito da Informática, Escola de Direito, Universidade do Minho, 2014.

GRABOSKY, P., "Virtual Criminality: Old Wine in New Bottles?", SLS, n.º 10, 2001, pp. 243

HAFELE, David M., "Three Different Shades of Ethical Hacking: Black, White and Gray", SANS Institute, 2004

HAFFNER, K., MARKOFF, J., *Cyberpunks: outlaws and hackers in the computer frontier,* New York: Touchstone Books, 1995.

HARRINGTON, Sean L., "Cyber Security Active Defense: Playing with Fire or Sound Risk Management?", 20 Rich. J.L. & Tech. 12, 2014, disponível em: http://jolt.richmond.edu/v20i4/article12.pdf, consultado a 4 de Agosto de 2015.

HEITOR, Pedro Oliveira e CANGUEIRO, Roberto, "La Sancíon de la prática de hacking en el ordenamiento jurídico portugués", artigo apresentado no âmbito do *IV Forum de expertos y jóvenes investigadores en Derecho y nuevas tecnologias*, Salamanca, Março de 2015.

HENRY, Kevin M., *Penetration Testing: Protecting Networks and Systems*, ITGP, 2012.

HERMIDA, Alvaro Redondo "El nuevo delito de acceso ilegal a sistemas de información en el proyecto de reforma del Código Penal" in *La ley penal: revista de derecho penal, procesal y penitenciário*, N.º 46, 2008, pp. 74-77.

HESS, Ken, "BackTrack Linux: The Ultimate Hacker's Arsenal" disponível em: http://www.admin-magazine.com/Articles/BackTrack-Linux-The-Ultimate-Hacker-s-Arsenal, consultado a 11 de Agosto de 2015.

HIMANEN, Pekka, *The Hacker Ethic and the Spirit of the Information Age*, Nova York, Random House, 2001.

HIMMA, Kenneth Einar e DITTRICH, David, "Active Response to Computer Intrusions", 2005, disponível em:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=790585, consultado a 1 de Setembro de 2015.

HIMMA, Kenneth Einar, “Ethical issues involving computer security: hacking, hacktivism, and counterhacking”, in *The handbook of information and computer ethics*, John Wiley & Sons, 2008, pp. 191-217.

HOLDAWAY, Eric J., “Active Computer Network Defense: An Assessment”, Maxwell Air Force Base, Alabama, 2001, disponível em: www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA407139, consultado a 7 de Agosto de 2015.

HUANG, Shane, “Proposing a Self-Help Privilege for Victims of Cyber Attacks”, *The George Washington Law Review*, Vol. 82 N.º 4, 2014, disponível em: http://www.gwlr.org/wp-content/uploads/2014/10/Huang_82_4.pdf, consultado a 7 de Agosto de 2015.

IHERING, Rudolf von, *A luta pelo direito*, 17.ª ed., Editora Forense, Rio de Janeiro 1999.

JACKSON, William, “The hack-back vs. the rule of law: Who wins?”, disponível em: http://gcn.com/blogs/cybereye/2013/05/hacking-back-vs-the-rule-of-law.aspx?admgarea=cybereye, consultado a 10 de Agosto de 2015.

JAYCOX, Mark, OPSAH, Kurt, “CISPA is Back: FAQ on What it is and Why it's Still Dangerous”, disponível em: https://www.eff.org/cybersecurity-bill-faq#hack, consultado a 10 de Agosto de 2015.

JOHNSON, Josh, “Implementing Active Defense Systems on Private Networks”, Sans Institute, 2015, disponível em: http://www.sans.org/reading-room/whitepapers/detection/implementing-active-defense-systems-private-networks-34312, consultado a 30 de Julho de 2015.

JORDAN, Tim e TAYLOR, Paul, *Hacktivism and Cyberwars: Rebels with a Cause?,* Routledge, 2004.

KEVELSON, Morton, "Isepic", in *Ahoy!*, n.º 22, 1985, pp. 71–73. disponível em: https://archive.org/stream/Ahoy_Issue_22_1985-10_Ion_International_US#page/n71/mode/2up, consultado a 20 de Junho de 2015.

KISSEL, Richard, "Glossary of Key Information Security Terms", *National Institute of Standards and Technology*, 2013, disponível em: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, consultado a 5 de Agosto de 2015.

KNIBBS, Kate*, "*The New CISPA Bill Is Literally Exactly the Same as the Last One*",* disponível em: *http://gizmodo.com/the-new-cispa-bill-is-literally-exactly-the-same-as-the-1679496808,* consultado a 10 de Agosto de 2015.

KNITTEL, John e SOTO, Michael, *Everything You Need to Know about the Dangers of Computer Hacking*, The Rosen Publishing Group, 2003.

KRUTZ, Ronald L. e VINES*,* Russell Dean, *The CISSP and CAP Prep Guide: Platinum Edition,* John Wiley & Sons*,* 2006.

LACHOW, Irving, "Active Cyber Defense - A Framework for Policymakers", CNAS, 2013, disponível em: http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf, consultado a 5 de Agosto de 2015.

LEIGH, David e HARDING, Luke, "Julian Assange: the teen hacker who became insurgent in information war", disponível em: http://www.theguardian.com/media/2011/jan/30/julian-assange-wikileaks-profile, consultado a 10 de Junho de 2015.

LEUKFELDT, Rutger e STOL, Wouter, *Cyber Safety: An Introduction*, The Hague, The Netherlands, Eleven International Publishing, 2012.

LEVY, Steven, *Hackers: heroes of the computer revolution,* O'Reilly Media, 2010.

LIU, Lily, "When Hacking Is Actually a Good Thing: The Civic Hacking Movement", disponível em: http://www.huffingtonpost.com/lily-liu/when-hacking-is-actually-_b_3697642.html, consultado a 23 de Fevereiro de 2015.

LYNN, III, William J., "Remarks on Cyber", RSA Conference, San Francisco, 15 de Fevereiro de 2011, disponível em: http://archive.defense.gov/speeches/speech.aspx?speechid=1535, consultado a 5 de Agosto de 2015.

MACEDO, João Carlos Cruz Barbosa de, "Algumas considerações acerca dos crimes informáticos em Portugal", in ANDRADE, Costa e NEVES, Rita Castanheira (orgs.), *Direito Penal hoje: novos desafios e novas respostas*, Coimbra Editora, 2009, pp. 221-262.

MARQUES, Garcia e MARTINS, Lourenço, "*Direito da Informática"*, Almedina, 2006.

MARTÍN, Ricardo M. Mata y, "Problemas fundamentales de la criminalidad informática*"*, disponível em: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2868, consultado a 1 de Agosto de 2015.

MARTINS, A. G. Lourenço, MARQUES, J. A. Garcia e DIAS, Pedro Simões, *Cyberlaw em Portugal - O Direito das Tecnologias da Informação e Comunicação*, Centro Atlântico, 2004.

MATOS, José António Alves de, *Dicionário de Informática e Novas Tecnologias*, FCA - Editora de Informática, Lisboa, 2009.

MAURUSHAT, Alana, “Types of Disclosure”, *in Disclosure of Security Vulnerabilities Legal and Ethical Issues,* SpringerBriefs in Cybersecurity*,* 2013, pp. 9-19.

MCGEE, Shane, SABETT, Randy V. e SHAH, Anand, “Adequate Attribution: A Framework for Developing a National Policy for Private Sector Use of Active Defense*”*, 8 J. Bus. & Tech. L. 1, 2013, disponível em: http://digitalcommons.law.umaryland.edu/jbtl/vol8/iss1/3/, consultado a 7 de Agosto de 2015.

MCQUADE, Samuel, *Encyclopedia of cybercrime*, Greenwood Press, 2009.

MIZRACH, Steven, “Is there a Hacker Ethic for 90s Hackers”, disponível em: http://www2.fiu.edu/~mizrachs/hackethic.html, consultado em 10 de Março de 2015.

MOLIST, Mercè, “La ética de los crackers”, disponível em: http://www.elmundo.es/tecnologia/2015/07/18/55a98327ca474107048b457d.html, consultado a 25 de Junho de 2015.

MONTA, Maria Elena, “Illegal but ethical”, disponível em: https://maryellenmontagenethics.wordpress.com/2015/07/28/illegal-but-ethical/, consultado a 28 de Julho de 2015.

MONTEIRO, Conde, *A Legitima Defesa: Um contributo para a sua fundamentação*, Dissertação de Mestrado em Ciências-Jurídico-Criminais, Universidade do Porto, 1994.

MONTEIRO, Silvana Drumond, “O ciberespaço: o termo, a definição e o conceito”, *DataGramaZero: Revista de Ciência da Informação*, v. 8, n.º 3, p. 1-18, disponível em: http://www.dgz.org.br/jun07/Art_03.htm, consultado a 23 de Outubro de 2015.

MOORE, Robert, *Cybercrime: Investigating High-Technology Computer Crime*, 1.ª ed., Cincinnati, Ohio: Anderson Publishing, 2006.

MOREIRA, Vital e CANOTILHO, José Joaquim Gomes, *Constituição da República Portuguesa – Anotada – Volume I – Artigos 1º a 107º,* Coimbra Editora, 2007.

MOREIRA, Vital e CANOTILHO, José Joaquim Gomes, *Constituição da República Portuguesa – Anotada – Volume II – Artigos 108º a 296º,* Coimbra Editora, 2010.

MUSA, Sam, "Cybersecurity: Understanding the Online Threat*",* disponível em: http://evolllution.com/opinions/cybersecurity-understanding-online-threat/, consultado a 6 de Agosto de 2015.

NORTHCUTT, Stephen, SHENK, Jerry, SHACKLEFORD, Dave, ROSENBERG, Tim, SILES, Raul e MANCINI, Steve, "Penetration Testing: Assessing Your Overall Security Before Attackers Do", SANS Institute, 2006, disponível em: https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635, consultado a 11 de Agosto de 2015.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, "Computer-related Crime: Analysis of Legal Policy", 10, OECD Publications, 1986.

PAGANINI, Pierluigi, "The Offensive Approach to Cyber Security in Government and Private Industry*",* INFOSEC Institute, 2013, disponível em*:* http://resources.infosecinstitute.com/the-offensive-approach-to-cyber-security-in-government-and-private-industry/, consultado a 5 de Agosto de 2015.

PALMA, Fernanda, *A Justificação por Legítima Defesa como Problema de Delimitação de Direitos, vol. II*, 1990.

PASSERI, Paolo, “April 2015 Cyber Attacks Statistics”, disponível em: http://www.hackmageddon.com/2015/05/12/april-2015-cyber-attacks-statistics/, consultado a 25 de Julho de 2015

PEREIRA, André Luiz, “O que é script?”, disponível em: http://www.tecmundo.com.br/programacao/1185-o-que-e-script-.htm, consultado a 29 de Julho de 2015.

PEREIRA, João Pedro, “Empresas desinvestiram na segurança informática”, disponível em: http://www.publico.pt/sociedade/noticia/investimento-a-recuperar-1635648, consultado a 28 de Abril de 2014.

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

PEREIRA, Joel Timóteo Ramos, *Direito da Internet e Comércio electrónico*, Quid Juris, 2001.

PETERSON, T., "Hack, hacker, hacking; Hacking ethics" in *Nightwork: a history of hacks and pranks at MIT*, Massachusetts Institute of Technology, 2011.

PIETERS, Janene, *“*Dutch gov’t to take on hackers in 2015 debate*”,* disponível *em:* http://www.nltimes.nl/2014/10/20/dutch-govt-take-hackers-2015-debate/*,* consultado a 10 de Agosto de 2015.

PINTO, Frederico de Lacerda da Costa, “Erro de tipo e erro de proibição*”,* Faculdade de Direito da Universidade Nova de Lisboa, 2007, disponível em: fd.unl.pt/docentes_docs/ma/tpb_MA_4894.doc, consultado a 1 de Junho de 2015.

POPPI, Ricardo, “Internet e sua normatividade no contexto da cultura hacker”, disponível em: http://www.arcos.org.br/artigos/internet-e-sua-normatividade-no-contexto-da-cultura-hacker/, consultado a 10 de Junho de 2015.

PRADA, Ignacio Flores, *Criminalidad Informática. Aspectos Sustantivos Y Procesales,* Tirant Lo Blanc, 2012.

RAJNOVIC, Damir, "Cyberspace – What is it?", disponível em: http://blogs.cisco.com/security/cyberspace-what-is-it, consultado a 23 de Outubro de 2015.

RAYMOND Eric S., "How To Become A Hacker", disponível em: http://www.catb.org/esr/faqs/hacker-howto.html, consultado a 30 de Julho de 2015.

RAYMOND, Eric *et al.* "The Meaning of 'Hack'", disponível em: http://www.catb.org/jargon/html/meaning-of-hack.html, consultado a 31 de Maio de 2015

RAYMOND, Eric S., "The New Hacker's Dictionary", disponível em: http://www.proselex.net/Documents/The%20New%20Hacker's%20Dictionary.pdf, consultado a 30 de Julho de 2015.

RIOFRIO, Melissa, "Hacking Back: Digital Revenge Is Sweet but Risky", disponível em: http://www.pcworld.com/article/2038226/hacking-back-digitalrevenge-is-sweet-but-risky.html, consultado a 7 de Agosto de 2015.

ROCHA, Manuel Lopes, "A lei da criminalidade informática", in *Legislação. Cadernos de Ciência da* Legislação, n.º 8, Outubro/Dezembro 1993, pp. 65-81.

ROCHA, Manuel Lopes, *Direito da Informática nos Tribunais Portugueses*, Centro Atlântico, 1999.

RODRIGUES, Benjamim Silva, *Da Prova Penal*, *Tomo IV, (Da Prova – Electrónico-Digital e da Criminalidade Informático-Digital)*, Lisboa: Rei dos Livros, 2011.

RODRIGUES, Benjamim Silva, *Direito Penal - Parte Especial - Tomo I - Direito Penal Informático-Digital,* Coimbra Editora, 2009.

ROSENZWEIG, Paul, "International Law and Private Actor Active Cyber Defensive Measures," in *Stanford Journal of International Law* 47, 2013, disponível em: http://poseidon01.ssrn.com/delivery.php?ID=276073029008011087002126114094081120022037040029059051090103084007005093075065073077038055005012119033032068015095006079099123055081044083067126123021087101083026060017015031081104005104006124017117001123005090121107067102015099112120064064118029&EXT=pdf&TYPE=2, consultado a 7 de Agosto de 2015.

SANTOS, Manuel Simas e LEAL-HENRIQUES, Manuel, *Noções de Direito Penal,* Rei dos Livros, 4.ª Ed., 2011.

SANTOS, Paulo, BESSA, Ricardo e PIMENTEL, Carlos, *Cyberwar – O Fenómeno, as Tecnologias e os Actores,* FCA – Editora de Informática, 2008.

SCHJOLBERG, Stein, *The History of Cybercrime 1976-2014,* Vol. 09, BoD – Books on Demand, 2014.

SCHJOLBERG, Stein e HUBBARD, Amanda M., "*Harmonizing National Legal Approaches on Cybercrime*", *WSIS Thematic Meeting on Cybersecurity*, Genebra, 28 de Junho a 1 de Julho de 2005, ITU, 2005, disponível em: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf, consultado a 25 de Março de 2015.

SCOTT, Brett, "The hacker hacked", disponível em: http://aeon.co/magazine/technology/how-yuppies-hacked-the-original-hacker-ethos/, consultado a 24 de Outubro de 2015.

SERRA, Teresa, *Problemática do Erro Sobre a Ilicitude*, Almedina, 1991.

SILVA, Germano Marques, *Direito Penal Português, Parte Geral, II*, Verbo, 1998.

SIMÕES, Pedro Dias, "O "*hacking*" enquanto crime de acesso ilegítimo. Das suas consequências à utilização das mesmas para a fundamentação de um novo direito", in *Direito da sociedade da informação*, vol. VIII, Coimbra Editora, 2009, pp. 229-261.

SOLMS, Rossouw von e NIEKERK, Johan van, "From information security to cybersecurity", disponível em: http://www.sciencedirect.com/science/article/pii/S0167404813000801, consultado a 14 de Outubro de 2015.

SORCHER, Sara, "Influencers: Companies should not be allowed to hack back", disponível em: http://passcode.csmonitor.com/influencers-hackback, consultado a 10 de Agosto de 2015.

STAMATELLOS, Giannis, *Computer Ethics: A Global Perspective*, Jones and Bartlett Publishers, 2007.

STROSSEN, Nadine, "Cybercrimes vs. Cyberliberties", in *Internet Policy and Economics*, *Challenges and Perspectives,* 2009, 111–138.

SUPPERT, Hartmut, *Notwehr und "notwehrähnlichen lage"*, Röhrscheid, 1973.

TANG, Alice, "Hacking back against cyber attacks*", Chicago Policy Review,* 2015, disponível em: http://chicagopolicyreview.org/2015/07/21/hacking-back-against-cyber-attacks/, consultado a 15 de Agosto de 2015.

THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY, "The Report Of The Commission On The Theft Of American Intellectual Property", The National Bureau of Asian Research., E.U.A., 2013, disponível em: http://ipcommission.org/report/IP_Commission_Report_052213.pdf, consultado a 10 de Agosto de 2015.

THOMAS, Douglas, *Hacker Culture*, Univ. of Minnesota Press, 2002.

THOMPSON, Ken, "Reflections on Trusting Trust", disponível em: https://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf, consultado a 28 de Julho de 2015.

TIMBERG, Craig, NAKASHIMA, Ellen e DOUGLAS-GABRIEL, Danielle, "Cyberattacks trigger talk of 'hacking back'", disponível em: http://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html, consultado a 10 de Agosto de 2015.

TOWNSEND, Kevin, "Hacking back – should it be a legal right for those under cyberattack?" disponível em: http://itsecurity.co.uk/2014/11/hacking-back-legal-right-cyberattack/, consultado a 1 de Agosto de 2015.

TRIGAUX, Robert, "A history of hacking", disponível em: http://www.sptimes.com/Hackers/history.hacking.html, consultado a 10 de Junho de 2015.

TZU, Sun, *A Arte da Guerra,* (Edição em Português) Bertrand Editora, 2009.

VAAS, Lisa, "Counterterrorism expert wants to arm US companies with hack-back capabilities", diponível em: https://nakedsecurity.sophos.com/2015/08/05/counterterrorism-expert-wants-to-arm-us-companies-with-hack-back-capabilities/, consultado a 10 de Agosto de 2015.

VARELA, Antunes, *Das obrigações em geral*, 10.ª ed., revista e actualizada (5.ª Reimpressão da edição de 2000), 2008, p. 553.

VENÂNCIO, Pedro Dias, *Lei do Cibercrime – Anotada e Comentada,* Coimbra Editora, 2011.

VENÂNCIO, Pedro Dias, "O Crime de Acesso Ilegítimo", JusJornal, N.º 1179, 18 de Fevereiro de 2011, Coimbra Editora, grupo Wolters Kluwer, disponível em: http://jusjornal.wolterskluwer.pt/Content/Document.aspx?params=H4sIAAAAAAAEAO29B2AcSZYlJi9tynt_SvVK1-

B0oQiAYBMk2JBAEOzBiM3mkuwdaUcjKasqgcplVmVdZhZAzO2dvPfee--999577733ujudTif33_8_XGZkAWz2zkrayZ4hgKrIHz9-fB8_lorZ7LOnb3bk2Xtw8Asv87opquVnezu7OzsP9x7gg-L8-mk1fXO9yj87z8om_38A82aBqjUAAAA%3DWKE, consultado a 30 de Outubro de 2014.

VERDELHO, Pedro, "A nova Lei do Cibercrime", in *Scientia Iuridica*, Tomo LVIII, n.º 320, Outubro/Dezembro, 2009, pp. 717-749.

VERDELHO, Pedro, "Anotação ao artigo 6.º da Lei n.º 109/2009, de 15 de Setembro", in Albuquerque, Paulo Pinto de e Branco, José (coords.), *Comentário das penais extravagantes*, vol. I, Universidade Católica Editora, 2010, pp. 515-517.

VERDELHO, Pedro, "Cibercrime", in *Direito da Sociedade da Informação* (org. José de Oliveira Ascensão), Vol. IV, Coimbra Editora (sem data), pp. 347-373.

VV.AA*, Temas de Direito da Informática e da Internet,* Coimbra Editora, 2004.

WEBER, Rolf H. e HEINRICH, Ulrike I., *Anonymization,* SpringerBriefs in Cybersecurity*,* 2012.

WESTBY, Jody, "Caution: Active Response to Cyber Attacks Has High Risk", disponível em: http://www.forbes.com/sites/jodywestby/2012/11/29/caution-active-response-to-cyber-attacks-has-high-risk/, consultado a 10 de Agosto de 2015

WILHELM, Douglas, *Professional Penetration Testing*, Syngress Press, 2010.

WULF, Wm. A., JONES, Anita K., "Cybersecurity" in *The Bridge, National Academy of Engineering,* Vol. 32, N. 1, *National Academy of Sciences,* 2002, pp. 41 a 45, disponível em: https://www.nae.edu/Publications/Bridge/EngineeringandHomelandSecurity/Cybersecurity.aspx, consultado a 6 de Agosto de 2015.

YAR, Majid, *Cybercrime and Society,* SAGE Publications, 2013.

ZICCARDI, Giovanni, *Resistance, Liberation Technology and Human Rights in the Digital Age,* Springer, 2013.

ZULUAGA, Camila, "En busca de cura para los delitos informáticos", disponível em: http://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170, consultado a 5 de Agosto de 2015.

ZÚQUETE, André, *Segurança em Redes Informáticas,* 3.ª ed., Lisboa: FCA - Editora de Informática, 2010.

Jurisprudência:

Acórdão do Supremo Tribunal de Justiça, de 21-01-1998; BMJ, 473, 133.

Acórdão do Tribunal da Relação de Coimbra, de 25-03-2009, processo 404/08.0PBTMR.C1, disponível em: http://www.dgsi.pt/jtrc.nsf/0/23316c8255decd83802575980054865c?OpenDocument, consultado a 10 de Agosto de 2015.

Acórdão do Supremo Tribunal de Justiça, de 14-05-2009, processo 389/06.8GAACN.C1.S1, disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/250e8e7b2272fe3b802575e1005155bb?OpenDocument, consultado a 11 de Agosto de 2015.

Acórdão do Tribunal da Relação de Coimbra, de 28-03-2012, processo 1133/10.0IDLRA.C1, disponível em: http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/b1844b3afb0136f7802579ea0033c2b6?OpenDocument, consultado a 22 de Setembro de 2015.

Acórdão do Tribunal da Relação de Guimarães, de 04-02-2013, processo 285/11.7IDBRG.G1, disponível em:

http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/c7b11687bdc7fe0f80257b1f00534ba2?OpenDocument, consultado a 22 de Setembro de 2015.

Acórdão do Tribunal da Relação do Porto, de 08-01-2014, Processo n.º 1170/09.8JAPRT.P2, disponível em: http://www.dgsi.pt/jtrp.nsf/d1d5ce625d24df5380257583004ee7d7/b54faf2d4330b8d480257c6e004ff2df?OpenDocument, consultado a 15 de Junho de 2015

Acórdão do Tribunal da Relação do Porto, de 25-02-2015, Processo n.º 120/08.3GCBGC-A.G1.P1, disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/890e919fcf20bd4d80257e0300579e86?OpenDocument, consultado a 22 de Setembro de 2015.