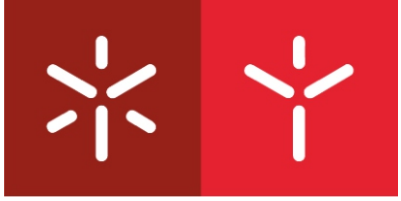
Universidade do Minho
Escola de Direito

Abrantes Malaquias Belo Caiúve

A problemática da regulação dos crimes informáticos no Anteprojeto de Código Penal angolano e a sua conformidade com a Convenção de Budapeste sobre o cibercrime

setembro de 2020

Uminho | 2019 Abrantes Malaquias Belo Caiúve **A problemática da regulação dos crimes informáticos no Anteprojeto de Código Penal angolano e a sua conformidade com a Convenção de Budapeste sobre o cibercrime**



Universidade do Minho
Escola de Direito

Abrantes Malaquias Belo Caiúve

A problemática da regulação dos crimes informáticos no Anteprojeto de Código Penal angolano e a sua conformidade com a Convenção de Budapeste sobre o cibercrime

Dissertação de Mestrado
Mestrado em Direito e Informática

Trabalho efetuado sob a orientação dos
Prof. Doutor Pedro Miguel Dias Venâncio
Prof. Doutor Joaquim Melo Henriques Macedo

setembro de 2020

Declaração

Nome: Abrantes Malaquias Belo Caiúve

Endereço eletrónico: abrantesmalaquiasbc@gmail.com

Telemóvel: +244 924 299 174

Número do Passaporte: N1747990

Título dissertação: A problemática da regulação dos crimes informáticos na proposta de lei do Código Penal angolano e a sua conformidade com a Convenção de Budapeste sobre o cibercrime

Orientadores: Professor Doutor Pedro Miguel Dias Venâncio e Professor Doutor Joaquim Melo Henriques Macedo

Ano de conclusão: 2020

Designação do Mestrado: Mestrado em Direito e Informática

Universidade do Minho, Setembro de 2020

Assinatura: _____

DEDICATÓRIA

Ao meu país Angola, como uma forma modesta de contribuir para a melhoria da reforma de toda a legislação penal que está em curso.

AGRADECIMENTOS

Ao Eurico Cambanda Belo Caiúve pela revisão linguística.

Ao Cardoso Muhongo e ao João Buaio pelo forte incentivo.

Ao Salvador Bonifácio Domingos Tito por ter sido o meu guia em Braga.

A Dona Ana Maria Igreja Magalhães Ferreira pela eficiência e prontidão laborais.

Aos meus orientadores pelo empenho, dedicação e disponibilidade demonstradas.

Ao Moisés Alfredo da Cunha Ferreira, "O MAF", Mestre Informático, pela parceria jurídico-tecnológica.

Ao pessoal da Procuradoria-Geral da República junto da Sala Criminal do Tribunal da Comarca de Benguela pela cooperação.

Aos meus colegas do 8º Curso do Mestrado em Direito e Informática, pela amizade e pelos esclarecimentos adicionais que me prestaram.

Aos meus familiares que, apesar de terem sofrido com as minhas constantes ausências, tudo fizeram para que eu fosse bem-sucedido.

A todos os companheiros que conviveram comigo na Camarata 2 da Residência Santa Tecla, em especial o Francisco Manuel Gina e o Botelho Isalino Jimbi, pela camaradagem.

PENSAMENTO

"A lei foi ultrapassada pela evolução das tecnologias e da capacidade inventiva de novas atuações ilícitas".

Pedro Verdelho.

RESUMO

A informática é o ramo da tecnologia que se ocupa do estudo do tratamento automático da informação. Desenvolveu-se rapidamente a partir da segunda metade do século XX com o surgimento da *Internet.*

O uso das tecnologias de informação e comunicação produziram mudanças no modo de vida de todas as sociedades, criando uma dependência de tal envergadura que tornou as pessoas praticamente incapacitadas de viver sem elas.

De forma dupla, este avanço da tecnologia informática teve um forte impacto no Direito Penal. Por um lado, veio facilitar o cometimento de certos crimes tradicionais. Por outro lado, os ataques cibernéticos e as técnicas de engenharia social possibilitaram o surgimento de diversas novas atividades que devem ser consideradas ilícitas por atentarem contra bens jurídicos indispensáveis à própria conservação e progresso da sociedade.

Em Angola, até ao ano de 2018, os crimes informáticos ainda não se encontravam legalmente previstos, o que de certa forma embaraçava o poder punitivo do Estado. Porém, no dia 23 de Janeiro de 2019 foi aprovado o Anteprojeto de Lei do Código Penal que prevê pela primeira vez o tratamento da criminalidade informática e o faz mediante a introdução de novos tipos criminais.

Dentre os crimes informáticos previstos neste anteprojeto temos os cometidos contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos (devassa por meio de informática, violação de telecomunicações e dano informático), os que atentam contra os computadores (falsidade informática e burla informática e nas telecomunicações) e os relacionados com os conteúdos (pornografia infantil).

A Convenção de Budapeste sobre o Cibercrime de 23 de Novembro de 2001 é o mais revelante tratado internacional sobre esta temática, por isso a generalidade das legislações têm acompanhado o seu espírito e sentido.

A nível da União Africana existe uma convenção que aborda a cibersegurança e, pela pertinência da matéria que acolhe, no dia 3 de Março de 2020 Angola a aprovou para ratificação.

Neste trabalho pretendemos analisar como é que o anteprojeto angolano trata os crimes informáticos, examinar se este tratamento está ou não em consonância com a Convenção de Budapeste, estudar os aspetos relevantes da convenção da união africana sobre a cibersegurança e proteção de dados pessoais e, por fim, investigar a implementação das TICs e a verificação de ataques cibernéticos no contexto angolano.

Palavras-chave: Crimes informáticos; Anteprojecto de Código Penal Angolano; Convenção de Budapeste sobre o Cibercrime; Convenção da União Africana sobre a Cibersegurança e Proteção de Dados Pessoais; Ataques Cibernéticos; Engenharia Social.

ABSTRACT

Computer science is the branch of technology that deals with the study of automatic processing of information. It developed rapidly from the second half of the twentieth century with the emergence of the Internet.

The use of information and communication technologies produces changes in the lifestyle of all societies, creating a dependency on such a scale that they have become almost incapable of living without them.

Doubly, this advancement of computer technology has had a strong impact on criminal law. On the one hand, it facilitated the commission of certain traditional crimes. On the other hand, cyberattacks and social engineering techniques made possible the emergence of several new activities that should be considered illicit because they undermine legal assets indispensable to the very conservation and progress of society.

In Angola, until 2018, cybercrimes were not yet legally foreseen, which somewhat embarrassed the punitive power of the state. However, on January 23, 2019, the Penal Code Bill was approved, providing for the first time the treatment of cybercrime and doing so by introducing new criminal types.

Among the cyber offences contained in this bill we have those against the confidentiality, integrity and availability of computer data and systems (intrusion through information system, breach of telecommunications and computer damage), computer-related offences (computer-related forgery and computer and telecommunications fraud) and content-related offences (child pornography).

The Budapest Convention on Cybercrime of 23 November 2001 is the most revealing international treaty on cybercrime, so the majority of laws have followed its mood and feeling.

In African Union there is a convention that deals with cybersecurity, due to the pertinence of the matter, on March 3, 2020 Angola approved it for ratification.

So, in this dissertation we intend to analyze how the Angolan Penal Code Bill deals with cybercrime, to examine whether or not this bill is in accordance with the Budapest Convention, to study the relevant aspects of the African Union Convention on cybersecurity and personal data

protection and, finally, to investigate the implementation of ICTs and the verification of cybercriminal attacks in the Angolan's reality.

Key-words: Cybercrimes; Angolan Penal Code Bill; Budapest Convention on Cybercrime; Africa Union Convention on Cyber Security and Personal Data Protection; Cyberattack; Social Engineering.

ÍNDICE

ACRÓNIMOS

AAPSI	Associação Angolana de Provedores de Serviços de Internet
ACT	Anteprojeto de Código Penal
AIDP	Associação Internacional de Direito Penal
AISI	African Information Society Initiative
Al.	Alínea
ANAC	Agência Nacional das Comunicações de Cabo Verde
ANPD	Agência Nacional de Protecção de Dados de Angola
APARKE	African Regional Action Plan on the Knowledge Economy
APWG	Anti-Phishing Working Group
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
Art.º	Artigo
AUC	African Union Commission
BICI	Brigada de Investigação de Criminalidade Informática de Portugal
CA	Conselho de Administração
CB	Convenção de Budapeste
CDADC	Código dos Direitos de Autor e dos Direitos Conexos
CDPC	European Committee on Crime Problems
CE	Conselho Europeu
CEDAO	Comunidade Económica dos Estados da África Ocidental
CERT	Computer Emergency Response Team

CM	Convenção de Malabo
CMJPLOP	Conferência de Ministros da Justiça dos Países de Língua Oficial Portuguesa
CNTI	Centro Nacional das Tecnologias de Informação de Angola
CPCA	Código de Processo Civil de Angola
CPS	Child Protection System
CRA	Constituição da República de Angola
CSIRTS	Computer Security Incident Response Team
DDoS	Distributed Denial-of-Service
DNS	Domain Name System
DoS	Denial-of-Service
ECA	Economic Comission for Africa
ECA	Estatuto da Criança e do Adolescente
EFCC	Economic and Financial Crimes Commission
ENISA	European Union Agency for Cybersecurity
FTP	File Transfer Protocol
GB	Gigabytes
GTGI	Grupo de Trabalho sobre o Governo na Internet
HTTPS	Hyper Text Transfer Protocol Secure
ICANN	Internet Corporation for Assigned Names and Numbers
ICI	Infraestruturas Críticas de Informação
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity

IMSI International Mobile Subcriber Identity

INACOM Instituto Nacional das Comunicações de Angola

INFOSI Instituto Nacional de Fomento da Sociedade de Informação de Angola

IP Internet Protocol

ISC Internet Systems Consortium

ISIA Iniciativa da Sociedade de Informação Africana

ISP Internet Service Provider

ITU The International Telecommunication Union

Kbps Kilobits por segundo

Kz Kwanza

LAN Local Area Network

LDACA Lei dos Direitos do Autor e Conexos de Angola

LGPD Lei Geral de Proteção de Dados

LPRSI Lei da Protecção das Redes e Sistemas Informáticos

LPWA Lucent Personalized Web Assistant

MAC Media Access Control

MB Megabytes

Mbps Megabits por segundo

MCT Ministério dos Correios e Telecomunicações de Angola

MININT Ministério do Interior de Angola

MITM Man-In-The-Middle Attack

MSN Microsoft Network

MTTI Ministério das Telecomunicações e Tecnologias de Informação de Angola

NEFF Nigerian Electronic Fraud Forum

NFIU Nigerian Financial Intelligence Unit

Nº Número

OCDE Organização para a Cooperação e Desenvolvimento Económico

OMPI Organização Mundial da Propriedade Intelectual

ONU Organização das Nações Unidas

PACB Protocolo Adicional à Convenção sobre Crimes Cibernéticos

PAGE Plano Estratégico da Sociedade de Informação

PALOP Países Africanos de Língua Oficial Portuguesa

PAREC Plano de Ação Regional Africano para a Economia do Conhecimento

PCA Presidente do Conselho de Administração

PEC Plataformas das Entidades Reguladoras das Comunicações Social dos Países de Língua Portuguesa

PGR Procuradoria-Geral da República

PNSI Plano Nacional da Sociedade de Informação

PoC Points of Contact

POP Post Office Protocol

QKD Quantum Key Distribution

RAT Remote Acess Trojan

RTSI Regulamento das Tecnologias e dos Serviços da Sociedade da Informação

SABRIC South African Banking Risk Information Centre

SADC Southern African Development Community (Comunidade de Desenvolvimento da África Austral)

SEPE Portal dos Serviços Públicos Eletrócnicos de Angola

SFTP	Secure File Transfer Protocol
SIC	Serviço de Investigação Criminal de Angola
SONANGOL	Sociedade Nacional de Combustíveis de Angola
SSH	Secure Shell
SSL	Secure Sockets Layer
STJ	Supremo Tribunal de Justiça
TCA	Trusted Credentials Area
TCP/IP	Transmission Control Protocol/Internet Protocol
TIC	Tecnologia de Informação e Comunicação
TR	Tribunal da Relação
TLS	Transport Layer Security
UA	União Africana
UE	União Europeia
UNODC	United Nations Office on Drugs and Crime
URL	Uniform Resource Locator
VPN	Virtual Private Network
WSIS	World Summiton the Information Society
WWW	World Wide Web

INTRODUÇÃO

A massificação do uso das novas tecnologias de comunicação e informação (doravante TIC) é uma realidade incontornável em todos os lugares do planeta terra e Angola não foge à regra.

A sua importância e o seu caráter quase indispensável são unanimidades globais, por isso, alguns países reconhecem o acesso à Internet como um direito fundamental[1].

Todavia, é bom que nos lembremos de que nem sempre as pessoas que fazem o uso dela são movidas pelas melhores razões. Devido ao seu potencial lesivo e a possibilidade de anonimização, muitos aproveitam-se dessas características para cometer transgressões. Daí legisladores de diversos países se dedicarem visando à tipificação e regulação dessas infrações perpetradas pelos *cibercriminosos*[2].

Nos seus 39 anos de existência como nação independente, Angola nunca teve uma lei que tivesse como objeto a criminalidade informática.

Em 2011 a Assembleia Nacional tinha elaborado o "Ante-Projecto de Lei de Combate à Criminalidade no Domínio das Tecnologias de Informação e Comunicação e dos Serviços da Sociedade da Informação"[3]. Infelizmente esta pretensão nunca teve efetivação.

Constata-se, por um lado, que os crimes informáticos ditos puros ou próprios[4] têm encontrado lacunas na lei. Por outro lado, os crimes impróprios, que têm apenas a informática como meio para a sua prática, por vezes têm tido um enquadramento forçado e dúbio, sendo solucionados por analogia, fazendo recurso ao – mais do que provecto – Código Penal, diploma

---

[1] Por exemplo, Portugal fá-lo no nº 6 do art.º 35º da Constituição. Na Constituição da República de Cabo Verde está previsto no nº 6 do art.º 44.º. O acesso à Internet também está estabelecido como um direito fundamental na Estónia, França, Finlândia e na Grécia. Disponível em https://pt.wikipedia.org/wiki/Acesso_à_Internet (Acedido aos 28-07-2019).

[2] Segundo o Dicionário do Infopédia (disponível em https://www.infopedia.pt/dicionarios/lingua-portuguesa/cibercriminoso e acedido aos 28-07-2019), o **cibercriminoso** é a pessoa que recorre à sistemas eletrónicos e às novas tecnologias de informação para cometer crime(s).

[3] Disponível em http://www.mtti.gov.ao/VerLegislacao.aspx?id=456 (Acedido aos 28-07-2019).

[4] São aqueles cujo único meio de prática é através da informática, ou seja, sem o computador é impossível o cometimento desta espécie de crime. Estes crimes surgiram com a evolução da tecnologia da informática e neles o bem jurídico protegido é a própria informática. (*Vide* **CASTRO**, Carla Rodrigues Araújo de. Crimes de informática e seus aspectos processuais. 2. ed. Rio de Janeiro: LumenJuris, 2003, p. 230).

que entrou em vigor no longínquo ano de 1886[5], altura em que o país ainda fazia parte do então Reino de Portugal.

Essas constatações agudizaram as nossas preocupações já que, por norma, "em sede de interpretação jurídico-penal está excluído o recurso à analogia"[6], admitindo-se somente em casos excecionais a interpretação extensiva[7].

Para a nossa satisfação, no dia 23 de Janeiro de 2019 foi aprovado na Assembleia Nacional, um anteprojeto[8] de Código Penal[9] e aguarda-se pela sua promulgação legal, para que entre em vigor.

Nesse futuro normativo[10] denota-se a previsão dos crimes informáticos, propriamente nos art.ºs 184º, 212º, 214º, 235º, 399º e 407º, compreendendo um total de seis. O primeiro apresenta a Pornografia infantil; o segundo, a Devassa por meio da informática; os demais tratam sucessivamente da Violação de telecomunicações, da Falsidade informática, do Dano informático e da Burla informática e nas telecomunicações.

A Convenção de Budapeste (doravante CB) sobre o cibercrime de 23 de Novembro de 2001 é o mais significativo e abrangente tratado internacional em matéria da criminalidade digital, sendo ratificado por vários países não pertencentes ao Conselho Europeu, dentre os quais alguns africanos. Ademais, a generalidade das legislações nacionais que versam sobre essa temática têm seguido o espírito e a configuração desse tratado, o que reconhece seu pioneirismo legislativo.

Sendo assim, a nossa preocupação é analisar profundamente este novo anteprojeto legislativo angolano, no sentido de verificarmos se o tratamento que faz acerca dos crimes informáticos está, ou não, em consonância com a CB. Faremos um breve exame à Lei nº 15/14

---

[5] Em termos cronológicos, já vai no terceiro século de existência. A sua versão original está disponível em https://www.fd.unl.pt/Anexos/Investigacao/1274.pdf (Acedido aos 19-07-2020).

[6] Acórdão do Tribunal de Lisboa, Proc. 4882/2008-9, em que é relator Rui Rangel. Disponível em http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/8cac11c0fbb3ec6a80257491003da99f?OpenDocument (Acedido aos 06-10-2019).

[7] Ainda no acórdão supracitado o relator adverte o seguinte: "é necessário ter cuidado ao interpretar a lei penal, na medida em que, como sabemos, não se pode admitir a criação de um novo ilícito por via judicial, sendo este o critério distintivo entre analogia e interpretação extensiva".

[8] O Grupo Técnico para acompanhar a discussão e aprovação deste anteprojeto foi criado pelo Despacho 489/11 de 28 de Julho de 2011 – I Série nº 143.

[9] Notícia constante no Jornal de Angola do dia 28 de Janeiro de 2019, escrita pelo jornalista Eduardo Magalhães, disponível em http://jornaldeangola.sapo.ao/opiniao/artigos/o_novo_codigo_penal_angolano (Acedido aos 06-09-2019). Também encontra-se em https://www.dw.com/pt-002/angola-poderá-o-novo-código-penal-travar-a-criminalidade/a-47199914 (acedido aos 06-09-2019). Na sua aprovação teve 155 votos a favor, 1 contra e 7 abstenções.

[10] Disponível em https://www.wipo.int/edocs/lexdocs/laws/pt/ao/ao026pt.pdf (Acedido aos 06-10-2019).

de 31 de Julho – Lei dos direitos do autor e conexos de Angola (doravante LDACA) – para verificarmos se faz alguma abordagem acerca da tutela penal digital.

Traremos ainda à colação a Convenção da União Africana sobre o Cibercrime e a Proteção de Dados de 2014[11] para observarmos se a legislação de Angola cumpre esta convenção e, num enjeito de direito comparado, estudaremos a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de Agosto de 2013.

Por último, estudaremos as mais relevantes vulnerabilidades, bem como as principais técnicas e metodologias ligadas à engenharia social usadas pelos criminosos digitais na perpetração das suas ilicitudes, tais como *hijacking*[12], *phishing*[13], spoofing[14] e denial of service (DoS)[15]. Usaremos como caso de estudo o ataque de negação de serviço que a empresa angolana SONANGOL – Sociedade Nacional de Combustíveis de Angola – sofreu recentemente (Junho de 2019), tendo paralisado todo o seu aparato informático[16], de forma a demonstrar a pertinência e a adequação (ou não) das previsões do novo projeto de Código Penal.

Ataque similar já havia acontecido contra diversos departamentos ministeriais e governos provinciais do estado angolano em 2016 e, de acordo estudos feitos, foram efetuados por *hackers* portugueses por alegada contestação à detenção de quinze ativistas políticos, dentre os quais um luso-angolano (Henrique Luaty da Silva Beirão)[17].

Um ataque de negação de serviço é de elevadíssima gravidade por afetar diretamente um dos principais pilares da segurança da informação, propriamente a disponibilidade, causando perturbação ao funcionamento regular dos sistemas informáticos e podendo desta forma preencher o ilícito penal de sabotagem informática.

---

[11] Aprovada para ratificação pela Resolução nº 33/19 de 9 de Julho no Diário da República – Iª Série nº 91. Disponível em https://angolaforex.com/2019/07/18/diario-da-republica-i-a-serie-n-o-91-de-9-de-julho-de-2019/ (Acedido aos 01-09-2020).
Foi ratificada pela República de Angola por intermédio da Carta de Ratificação nº 1/20 que é parte integrante do Diário da República – Iª Série n.º 23 de 3 de Março de 2020, cujo sumário pode ler-se "Aprova, para Ratificação, pela República de Angola, a Convenção da União Africana sobre a Cibersegurança e Protecção de Dados". Disponível em https://angolaforex.com/2020/03/10/diario-da-republica-i-a-serie-n-o-23-de-3-de-marco-de-2020/ (Acedido aos 06-04-2020). Moçambique ratificou um ano antes por via da Resolução nº 5/2019 de 20 de Junho. Disponível em https://lexlink.eu/conteudo/geral/ia-serie/3925437/resolucao-no-52019/20525/por-tipo-de-documentolegal (Acedido aos 08-05-2020).

[12] **GOODRICH**, Michael & **TAMISSA**, Roberto. Introduction to computer security. Pearson New International Edition, 2014, p. 253.

[13] **AMIRI**, I. S; **AKANBI**. O. A & **FAZELDEHKORDI**, E. A Machine-Learning Approach to Phishing Detection and Defense. Syngress. 2014, p. 9.

[14] **YANG**, Jie; **CHEN**, Yingying; **TRAPPE**, Wade & **CHENG**, Jerry. Pervasive Wireless Environments: Detecting and Localizing User Spoofing. Springer, 1st ed. 2014, p. 5.

[15] **YU**, Shui. Distributed Denial of Service Attack and Defense. Springer-Verlag New York, 2014, p. 1.

[16] Disponível em https://www.plenglish.com/index.php?o=rn&id=42936&SEO=angolan-oil-company-suffers-attempted-cyber-attack e em https://www.menosfios.com/en/sonangol-suffered-cyber-attack/ S (Acedido aos 08-05-2020).

[17] SPAMfighter News, disponível em http://www.spamfighter.com/News-20202-Anonymous-Attacks-Government-of-Angola-due-to-Jail-Sentence-for-17-Activists.htm (Acedido aos 09-09-2019).

Portanto, no nosso modesto entender, foram essas as constatações relevantes que justificaram a escolha do tema, bastando-nos agora arregaçarmos as mangas e calcorrearmos as trilhas investigativas no sentido de sermos bem-sucedidos nesta pretensão.

Capítulo I – APRESENTAÇÃO DO TEMA

1.1. Antecedentes históricos

A Internet, aglutinação da expressão inglesa ***inter****connected* ***net****work*, isto é, rede interconectada, é o sistema universal de redes de computadores interligados que utilizam o protocolo TCP/IP para conectar dispositivos em todo o globo. É uma rede de redes que consiste em redes privadas, públicas, académicas, comerciais e governamentais – de âmbito local a global – ligadas por uma ampla variedade de tecnologias de redes eletrónicas, sem fio e óticas. Possui amplos recursos e serviços de informações.

Suas origens remontam à pesquisas encomendadas pelo Governo Federal dos Estados Unidos de América na década de 60 do século passado para criar uma comunicação robusta e tolerante a falhas com as redes de computadores. A rede precursora primária, a ARPANET[18] (Advanced Research Projects Agency Network)[19], serviu inicialmente como espinha dorsal da interconexão de redes académicas e militares regionais nos anos 80. O financiamento da National Science Foundation Network para uma espinha dorsal de rede na década de 80, bem como o financiamento privado para outras extensões comerciais, levou à participação mundial no desenvolvimento de novas tecnologias de rede e na fusão de muitas redes.

A ligação de redes e empresas comerciais no início dos anos 90 marcou o início da transição para a Internet moderna e gerou um crescimento exponencial sustentado à medida que gerações de computadores institucionais, pessoais e móveis foram conectados à rede[20].

A maioria dos meios de comunicação tradicionais foi remodelada dando origem a novos serviços. As publicações de jornais, livros e outras publicações impressas estão-se adaptar à tecnologia do *site* ou são remodeladas em *blogs, feeds* da *Web* e agregadores de notícias *online*.

A Internet ativou e acelerou novas formas de interações pessoais por meio de mensagens instantâneas, fóruns da Internet e redes sociais. As compras *online* cresceram exponencialmente, tanto para grandes retalhistas quanto para pequenas empresas e empreendedores.

---

[18] Teve como precursora a ARPA, criada em 1956 com a finalidade de recuperar a liderança tecnológica dos Estados Unidos de América que se sentia abalada pelos sucessos espaciais que os soviéticos tiveram na época. (*Vide* **RODRIGUES**, Benjamim Silva. Direito Penal Parte Especial. Tomo I. Direito Penal Informático-Digital. Coimbra, 2009, p. 54).

[19] Traduz-se por Rede da Agência para Projetos de Pesquisa Avançada.

[20] Disponível em https://en.wikipedia.org/wiki/Internet#cite_note-5 (Acedido aos 08-10-2019).

A Internet não possui comando único[21] na implementação tecnológica ou nas políticas de acesso e uso; cada rede constituinte define suas próprias políticas. As definições de alcance excessivo dos dois principais espaços de nomes na Internet, o espaço de endereço de Protocolo da Internet (endereço IP) e o DNS (Domain Name System)[22], são mantidos e dirigidos pela ICANN (Internet Corporation for Assigned Names and Numbers)[23]. O suporte técnico e a padronização dos principais protocolos são uma atividade da IETF (Internet Engineering Task Force).

Os serviços "específicos"[24] disponibilizados aos internautas são os seguintes:

- World Wide Web (WWW);
- Webcasting ("WEBCAST");
- Transferência de Ficheiros, [File TransferProtocol – (FTP)];
- TELNET – Terminal Virtual. Rlogin;
- O correio eletrónico – E-MAIL ou MAIL;
- Grupos de discussão – NEWSGROUPS, USENET;
- Motores de pesquisa na Internet – ARCHIE, GPHER e WAIS;
- Difusão na Internet – Listas de distribuição, áudio, vídeo;
- A oferta de mundos virtuais; e
- Navegadores.

A Internet possibilitou a migração do analógico para o mundo digital, alterando drasticamente a realidade física então vivenciada e possibilitando a existência de uma nova realidade – a realidade virtual.

Com ela emergiram vários novos conceitos, tais como o de "aldeia global"[25], o de "ciberespaço"[26] e o de "cibercidadão"[27], inaugurando-se uma nova era – a "era digital" que infelizmente está a ser ameaçada pelo crescimento da criminalidade informática.

---

[21] Em https://en.wikipedia.org/wiki/Internet_governance (Acedido aos 08-10-2019) pode ler-se o seguinte *"No one person, company, organization or government runs the Internet".*

[22] Traduz-se por Sistema de Nomes de Domínio.

[23] Corporação da Internet para Nomes e Números Atribuídos.

[24] Seguimos os serviços enunciados em **RODRIGUES**, Benjamim Silva. Idem, p. 53-65.

[25] Termo criado pelo filósofo canadiano **Herbert Marshall McLuhan** visando indicar que as novas tecnologias eletrónicas tendem a encurtar distâncias e o progresso tecnológico tende a reduzir todo o planeta à mesma situação que ocorre em uma aldeia: um mundo em que todos estariam, de certa forma, interligados. *In* https://pt.wikipedia.org/wiki/Aldeia_Global (Acedido aos 02-11-2019).

[26] O escritor estadunidense e canadiano **William Ford Gibson** massificou este termo na sua obra *Neuromancer* de 1984 (*in* https://pt.wikipedia.org/wiki/William_Gibson Acedido aos 02-11-2019), porém apareceu pela primeira vez no contexto das artes visuais no final

1.2. Introdução ao conceito jurídico de criminalidade informática

Antes de entrarmos para as questões jurídicas faremos uma breve resenha histórica sobre o surgimento dos crimes informáticos.

O registo dos primeiros casos remonta os meados da década de 60 e eram quase todos relacionados a crimes de imprensa ou económicos. Duas décadas depois começou a registar-se um aumento deste tipo de criminalidade que passou a envolver "manipulações de caixas bancários, abusos de telecomunicações, pirataria de programas e pornografia infantil"[28].

O desenvolvimento do comércio eletrónico possibilitou o surgimento de *sites* fraudulentos e de muitas burlas decorrentes do processo de compra e venda.

Deste modo, ficou evidenciado as vulnerabilidades que os sistemas então apresentavam, o que fomentou o surgimento das primeiras doutrinas sobre essa matéria[29] e confirmou-se que a evolução tecnológica potenciou a evolução da criminalidade[30].

Apesar dessas constatações delituosas, a palavra "cibercrime" surge apenas no final dos anos 90 em Lyon, França, no decorrer de uma reunião de um subgrupo do G8 que estudava e discutia os problemas que surgiam pelo uso das redes de telecomunicações, numa altura em que se expandia a utilização da Internet, principalmente nos países do norte da América[31][32].

Em 23 de Novembro de 2001, esse termo foi incorporado no primeiro instrumento internacional sobre a temática, a *Convenção sobre o Cibercrime* adotada em Budapeste, na Hungria, pelo Conselho da Europa.

Feita essa resenha histórica, começamos por frisar que os crimes informáticos, em alguns aspetos, assemelham-se aos crimes tradicionais, representando tão-somente "versões

---

dos anos 1960, quando a artista dinamarquesa Susanne Ussing e seu arquiteto parceiro Carsten Hoff se constituíram como Atelier Cyberspace (*in* https://en.wikipedia.org/wiki/Cyberspace Acedido aos 02-11-2019).

[27] **PATROCÍNIO**, José Tomás Vargues. (2004). *Tornar-se pessoa e cidadão digital – Formar-se dentro e fora da escola na sociedade tecnológica globalizada* (dissertação de doutoramento). Universidade Nova de Lisboa, Lisboa. Disponível em http://run.unl.pt/handle/10362/1294 (Acedido aos 02-11-2019), p. 182. Diferentemente da palavra cidadão que "sugere uma definição geográfica ou nacional de pertença social", o termo cibercidadão "reflete a nova pertença social baseada numa perspectiva não-geográfica".
Com o mesmo valor semântico o ilustre autor fala de e-cidadã(o), ser digital ou *netizen*. Este último vocábulo é muito difundido nos países anglo-saxónicos e deriva da fusão das palavras *net* e *citizen*, isto é, o cidadão da rede.

[28] Disponível em https://pt.wikipedia.org/wiki/Crime_informático (Acedido os 02-11-2019).

[29] **GOUVÊA**; Sandra. O direito na Era Digital. Crimes Praticados por Meio da Informática. MAUAD, Rio de Janeiro, 1997, p. 79.

[30] **MACEDO**, João Carlos Cruz Barbosa de, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, Coimbra Editora, 2009, p. 224.

[31] Disponível em https://pt.wikipedia.org/wiki/Crime_informático (Acedido aos 28-01-2020).

[32] Vale referir que a "introdução da interface gráfica ("WWW") deu-se igualmente nos anos 90, permitindo um rápido crescimento no número de usuários da Internet" e fazendo com que a informação estivesse disponível globalmente. **GERCKE**, Marco. Understanding cybercrime: Phenomena, challenges and legal response. ITU (International Telecommunication Union). September, 2012. Disponível em https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf (Acedido aos 28-01-2020).

digitais do mundo real, ou seja, seriam crimes tradicionais se não fosse a adição do elemento virtual ou ciberespacial"[33].

O tratamento desse tipo de delito é tão recente e problemático que até a presente data não há unanimidade no que tange a sua designação[34], isto é, os crimes informáticos são igualmente designados por crimes virtuais, crimes digitais, crimes cibernéticos, crimes informático-digitais, *e-crimes* ou crimes eletrónicos[35].

Neste trabalho adotaremos a expressão ***crimes informáticos*** por ser aquela que melhor se enquadra na legislação angolana.

Não existe uma definição única de crime informático; e a dificuldade dessa determinação tem várias razões. Uma delas prende-se com o facto de que "os dados e sistemas informáticos tanto podem constituir objeto material de determinada conduta, bem como o instrumento utilizado para cometê-la"[36]. Outro motivo, se calhar o de maior realce, tem que ver com as "várias espécies de condutas humanas"[37] suscetíveis de representarem esse tipo de delito.

Crimes informáticos são aqueles orientados para o computador, ou seja, é um tipo de crime que pressupõe a existência de um computador e de uma rede. O computador tanto pode ser utilizado para praticá-lo ou ser apenas o alvo de tal prática.

Nesta ordem de ideias, doutrinariamente os crimes informáticos podem ser definidos como "qualquer acção ilícita perpetrada com a ajuda de uma operação electrónica contra a segurança de um sistema informático ou de dados que ele contém, qualquer que seja o fim visado"[38].

Essa definição procura elencar a multiplicidade de ações que constituem esses delitos, porém não as discrimina na sua totalidade.

---

[33] **MENEZES**, Umbelina Teresa João de. O Papel das Forças e Serviços de Segurança no Combate aos Crimes Cibernéticos em Angola. Dissertação para a obtenção do grau de Mestre em Segurança da Informação e Direito no Ciberespaço no Instituto Superior Técnico de Lisboa. Dezembro de 2016. Disponível em https://fenix.tecnico.ulisboa.pt/downloadFile/563345090415229/Dissertacao.pdf (Acedido aos 19-07-2019), p. 28.

[34] **VERDELHO**, Pedro. "Cibercrime." Direito da Sociedade da Informação, Vol. IV, Coimbra Editora, Junho de 2003, p. 347.

[35] As designações inglesas *high technology crimes* (crimes tecnológicos) e *computer-related crime* são igualmente usadas por alguns autores lusófonos (in **DIAS**, Vera Marques. A problemática da investigação do cibercrime. DATA VENIA – Revista Jurídica Digital. Ano 1. N.º 01. Julho-Dezembro 2012, p. 65).

[36] **DELGADO**, Vladimir Chaves. Cooperação internacional em matéria penal na convenção sobre o cibercrime. Dissertação apresentada como requisito parcial para conclusão do Programa de Mestrado em Direito das Relações Internacionais do Centro Universitário de Brasília, BRASÍLIA 2007, p. 18 e 19. Disponível em https://repositorio.uniceub.br/jspui/bitstream/123456789/3562/3/vladimir.pdf (Acedido aos 19-07-2019).

[37] **DELGADO**, Vladimir Chaves. Ibdem, idem, p. 19.

[38] **RODRIGUES**, Benjamim Silva. Idem, p. 78, 79.

Este tipo de ilícito atenta, de modo particular, contra a própria pessoa ou contra a sua segurança financeira e, de modo geral, contra o bem-estar social.

Pode envolver ações que atentam contra os direitos autorais, a garantia dos direitos e liberdades fundamentais dos cidadãos (que é ferida pela vigilância massiva não autorizada), a extorsão sexual (também designada pelo neologismo *sextorsão*[39]), a pornografia infantil e outras más práticas que perigam os menores de idade.

A informática trouxe duas grandes problemáticas à legislação penal: serve como elemento potenciador da criminalidade e traz novas realidades que requerem a devida proteção legal.

A gravidade dos crimes digitais agudiza-se pelo facto de atentarem contra a confidencialidade, a integridade e a disponibilidade de dados e sistemas informáticos.

Existem vários crimes informáticos e a sua nomenclatura altera de país para país, apesar de a maioria deles seguir a denominação estabelecida na Convenção de Budapeste. Não é pretensão nossa elencarmos todos eles, contudo, dentre os mais frequentes destacam-se a falsidade informática, o dano informático, a sabotagem informática, o acesso ilegítimo, a intercetação ilegítima, a reprodução ilegítima de programas de computador, a burla informática e a devassa por meio da informática.

Além da designação e da tipologia, outra temática isenta de unanimidade por parte dos distintos doutrinários é a relativa à sua classificação[40][41]. As designações mais frequentes são as seguintes: crimes informáticos próprios e impróprios[42]; crimes informáticos puros, mistos e

---

[39] Disponível em https://www.jn.pt/justica/extorsao-sexual-na-net-nao-para-de-aumentar-4774319.html (Acedido aos 03-11-2019).

[40] **RODRIGUES**, Benjamim Silva. Idem, p. 19.

[41] A Comissão Europeia engloba no cibercrime três categorias de atividade criminosa, a saber, os **crimes tradicionais** cometidos com o auxílio do computador e redes informáticas, os **crimes relacionados com o conteúdo**, nomeadamente a publicação de conteúdos ilícitos por via de meios de comunicação eletrónicos, e os **crimes exclusivos das redes eletrónicas** (**DIAS**, Vera Marques. A problemática da investigação do cibercrime. Data Venia – Revista Jurídica Digital. Ano 1, Nº 01. Julho-Dezembro, 2012, p. 66).

Já Pedro Verdelho os engloba em três grupos essenciais:

1- Os crimes que recorrem a meios informáticos;
2- Os crimes referentes à proteção de dados pessoais; e
3- Os crimes informáticos propriamente ditos.

Mais adiante acrescenta o grupo relativo aos crimes contra o conteúdo (a violação dos direitos de autor e a difusão de pornografia infantil). **VERDELHO**, Pedro. "Cibercrime." Direito da Sociedade da Informação, vol. IV, Coimbra Editora, Junho de 2003, p. 356 e 368.

Pedro Dias Venâncio defende uma classificação diferente, distinguindo entre Criminalidade informática em sentido amplo e Criminalidade informática em sentido estrito. *In*: **VENÂNCIO**, Pedro Dias – Lei do Cibercrime – Anotada e Comentada. 1ª ed. [S.l.]: Coimbra Editora – Grupo Wolters Kluwer, 2011. ISBN 978-972-32-1906-7, p.16 a 18.

[42] **CASTRO**, Carla Rodrigues Araújo de. Ibdem, p. 230.

comuns[43]; e crimes de informática comum e específicos[44]. A primeira é a que nos confere melhor acolhimento.

Os crimes informáticos próprios ou puros são aqueles que só podem ser realizados fazendo recurso à informática, são tipos penais recentes, tendo surgido com o crescimento tecnológico. O bem jurídico tutelado é a inviolabilidade dos dados informáticos. Ou seja, "são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado"[45].

Já os crimes impróprios ou impuros surgiram porque a informática veio potenciar os delinquentes, por isso são crimes tradicionais cometidos por meio da informática, o que significa que são crimes comuns praticados na Internet. Aqui o bem jurídico tutelado não é a inviolabilidade dos dados, mas sim outro.

No crime impróprio o resultado do delito repercute-se no meio natural, lesando o mundo físico ou causando ameaça a outros bens jurídicos não informáticos.

Nesta dupla classificação, a distinção fundamental reside no bem jurídico que se pretende tutelar, ou seja, os primeiros têm em consideração aos crimes cometidos contra bens jurídicos informáticos; os segundos, aos cometidos contra bens jurídicos habituais.

A problemática do surgimento da criminalidade informática tem servido de impedimento à plena implementação e expansão da sociedade de informação e comunicação devido aos inúmeros riscos que causa, situação que examinaremos a seguir.

1.3. Introdução ao conceito de sociedade da informação e riscos que a mesma apresenta para a prática de crimes

---

[43] **VIANNA**, Túlio & **MACHADO** Felipe. Crimes Informáticos. Belo Horizonte. Editora Fórum, 2013, p. 29-35. Nesta obra os **crimes mistos** são definidos como sendo "crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa. São delitos derivados da invasão de dispositivo informático que ganharam *status* de crimes *sui generis*, dada a importância do bem jurídico protegido diverso da inviolabilidade dos dados informáticos."
Para além da trilogia classificativa, os autores apresentam um quarto elemento de classificação que designam de **crime informático mediato ou indireto**, que sucede "nos casos em que um delito informático próprio é praticado como crime-meio para a realização de um crime-fim não informático", como exemplo apresentam a seguinte situação:

> *"Se alguém invade um dispositivo informático de um banco e transfere indevidamente dinheiro para sua conta, estará cometendo dois delitos distintos: o de invasão de dispositivo informático e o furto; o primeiro, crime informático, o segundo, patrimonial."*

[44] **ALBUQUERQUE**, Roberto Chaconde. A criminalidade informática. São Paulo, SP: Juarez de Oliveira, 2006, p. 241.

[45] **JESUS**, Damásio E. de *apud* **ARAS**, Vladimir. Crimes de Informática. Jus Navigandi, Ed. 12, out. 2001. Disponível em http://www1.jus.com.br/doutrina/texto.asp?id=2250 (Acedido em 03-11-2019).

A importância e a imprescindibilidade da Internet são hodiernamente incontestáveis. Esta rede faz parte da vida das pessoas, sendo impossível resistir ao seu crescimento.

A Internet trouxe muitas vantagens para diversas instituições, sobretudo governos e empresas[46]. Contudo, apesar desses benefícios, a Internet traz também consigo alguns malefícios, tais como, a perda da liberdade de expressão e informação como resultado da tentativa de controlo e da pressão exercida por parte de alguns regimes políticos.

Sendo assim, é impreterível analisar o conceito, os principais intervenientes e o respetivo grau da sua participação para o estabelecimento daquilo que se designa por ***sociedade da informação***.

A sociedade de informação representa "o modo de desenvolvimento económico e social baseado na aquisição, tratamento e difusão da informação por via de redes de comunicações digitais"[47] que infestou o quotidiano das pessoas e instituições e colocou a informação à disposição de todos de forma livre e aberta.

Os Estados Unidos da América tiveram um papel preponderante na implementação da interligação da rede de computadores. Na primeira metade da década de 90 iniciaram um grande investimento na tecnologia como forma de potenciar o desenvolvimento económico e tal aposta possibilitou-lhes posicionar-se acima de outras nações incluindo o seu antigo rival que liderava o bloco do leste – a União Soviética.

As Nações Unidas também tiveram um papel de destaque. No início desse milénio surgiram várias resoluções e cimeiras ou cúpulas relacionadas às telecomunicações, à sociedade da informação e à governança na Internet. Uma dessas cimeiras criou o ***Grupo de Trabalho sobre o Governo na Internet*** (GTGI)[48].

Foram traçadas diretrizes no sentido dos Estados criarem um ambiente jurídico que propicie a implementação da sociedade de informação, visando o aproveitamento das suas potencialidades económicas[49].

---

[46] As empresas "nela vêm uma excelente oportunidade de implementar e desenvolver os seus negócios à escala mundial". **RODRIGUES**, Benjamim Silva. Idem, p. 79.
Ainda na p. 323 da obra supra citada temos que as empresas e a Administração Pública "encontram-se, mais do que nunca, dependentes dos sistemas informáticos".

[47] **VERDELHO**, Pedro. "Cibercrime." Direito da Sociedade da Informação, vol. IV, Coimbra Editora, Junho de 2003, p. 348.

[48] Foi criado na cimeira de Genebra de 2003 onde saíram dois grandes documentos: o Plano de Ação e a Declaração de Princípios. Dentre as Recomendações formuladas pelo GTGI destacam-se as que têm a ver com a administração dos ficheiros da zona base e dos servidores base do sistema dos nomes de domínio; a atribuição de endereço IP; os custos de conexão; a estabilidade e segurança da Internet e a ***ciberdelinquência***; a luta contra o Spam; a liberdade de expressão; a participação efetiva na elaboração de políticas mundiais; a proteção dos dados e respeito pela vida privada; os direitos do consumidor e o multilinguismo. *Vide* **RODRIGUES**, Benjamim Silva. Idem, p. 80-85.

[49] Disponível em http://www.itu.int/net/wsis/implementation/index.html (Acedido aos 04-11-2019).

É nesse clima que em 17 de Maio de 2005 é instituído em Túnis – num encontro da Cúpula Mundial d8*a Sociedade da Informação por via da Resolução 252 da 60ª sessão da Assembleia Geral das Nações Unidas – ***o dia mundial da sociedade da informação***. Este feito relevante visou despertar o mundo para a necessidade da luta pela redução da "exclusão digital"[50].

Seguindo a pretensão americana, a União Europeia em 1993 estabeleceu o caminho para uma "era comum de informação" como um dos seus desafios para o crescimento no século XXI[51].

Em finais deste ano foi criado o Grupo de Alto Nível[52] liderado pelo alemão Martin Bangemann para analisar as transformações sociais relacionadas à Sociedade da Informação[53]. Era formado por especialistas seniores do setor europeu da informática, que refletiam sobre a necessidade do aumento da interoperabilidade de redes para simplificar a difusão de informações e sistemas de comunicação interativa.

Foi este grupo que preparou uma apresentação sobre o desenvolvimento da "sociedade da informação" na União Europeia para a Cúpula Europeia em Corfu, que decorreu de 24 a 25 de Junho de 1994 e salientou a necessidade de criar um enquadramento legal, geral e flexível que estimulasse o desenvolvimento da sociedade da informação na Europa.

Estava assim lançada "a marcha para a sociedade da informação", surgindo em 1995 uma Diretiva[54] que definia pela primeira vez importantíssimos conceitos ligados à Internet tais como: *dados pessoais, tratamento de dados e consentimento sem causa*. Nesse documento já

---

[50] Disponível em https://pt.wikipedia.org/wiki/Dia_Mundial_da_Sociedade_da_Informação (Acedido aos 04-11-2019).

[51] Tal foi manifestado no ***Livro Branco da Comissão Europeia*** sobre o *Crescimento, competitividade, emprego. Desafios e pistas para entrar no século XXI quando* o eminente **Jacques Delors** era o presidente da Comissão Europeia.
Neste documento oficial da União Europeia foi estabelecido um Plano de Ação que definiu as seguintes prioridades:

1ª Promover o uso das tecnologias da informação;
2ª Fornecer serviços básicos entre a Europa e resto do mundo;
3ª Continuar a criação do enquadramento jurídico apropriado;
4ª Apostar na formação das novas tecnologias; e,
5ª Melhorar o desempenho industrial e tecnológico.

Vide **RODRIGUES**, Benjamim Silva. Idem, p. 86-87.

Em 1999 na "cimeira do emprego" realizada em Lisboa e presidida por Portugal, o então primeiro-ministro português **António Guterres** propôs que se transformasse "no lançamento de uma estratégia europeia para a sociedade do conhecimento". Disponível em https://www.publico.pt/1999/12/03/jornal/uma-agenda-europeia-para-a-sociedade-do-conhecimento-127314 (Acedido aos 04-11-2019).

[52] Um relatório desse grupo contendo inúmeras recomendações e intitulado ***Building the European information society for usall – Final policy report of the high-level expert group*** pode ser lido em http://aei.pitt.edu/8692/1/8692.pdf (Acedido aos 04-11-2019).

[53] Disponível em https://cordis.europa.eu/event/rcn/2139/es (Acedido aos 04-11-2019).

[54] Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046 (Acedido aos 05-11-2019).

foi notório o reconhecimento da não restrição ou proibição da "livre circulação de dados entre os Estados-membros".

Nos anos seguintes surgiram outros instrumentos normativos, todavia foi em 1999 que o Parlamento Europeu manifestou a urgência de ser fomentada "uma utilização mais segura da Internet através do combate aos conteúdos ilegais e lesivos"[55] por intermédio da implementação de um plano de ação plurianual[56].

O novo milénio trouxe a inquietação relacionada com a "organização e gestão da Internet"[57]. Seguiram-se as preocupações concernentes aos "direitos do autor e conexos"[58], bem como às "estatísticas comunitárias"[59], tudo dentro da sociedade de informação.

A importância da adoção de instrumentos comunitários destinados a combater e sancionar *a criminalidade informática, a cibercriminalidade e a pornografia infantil* – reforçando a segurança no acesso à Internet – ficou patente em 2001 na Comunicação da Comissão das Comunidades Europeias eEurope 2002[60]. No seu ponto 1.1. com a epígrafe *Respostas nacionais e internacionais,* lê-se a seguinte explanação interessante:

> *"A criminalidade informática ou cibercrime afecta todo o ciberespaço e não pára nas fronteiras tradicionais dos Estados. Estas infracções podem, em princípio, ser cometidas a partir de qualquer ponto e contra qualquer utilizador de computador,*

---

[55] Veja-se a Recomendação 98/560/CE do Conselho de 24 de Setembro de 1998 relativa ao desenvolvimento da competitividade da indústria europeia de serviços audiovisuais e de informação através da promoção de quadros nacionais conducentes a um nível comparável e eficaz de protecção dos menores e da dignidade humana. Disponível em https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:31998H0560 (Acedido aos 05-11-2019).
Essas preocupações foram reiteradas anos depois pelo Comité das Regiões por via do parecer de 20 de Novembro de 2002.

[56] O documento orientador desse plano é a Decisão n° 276/1999/CE do Parlamento Europeu e do Conselho de 25 de Janeiro de 1999 que adopta um plano de acção comunitário plurianual para fomentar uma utilização mais segura da Internet através do combate aos conteúdos ilegais e lesivos nas redes mundiais.

[57] Resolução do Conselho de 3 de Outubro de 2000 relativa à organização e à gestão da Internet. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000Y1014(02)&from=EN (Acedido aos 05-11-2019).
Na parte final dessa resolução que versa sobre a incumbência da Comissão pode ler-se o seguinte:

> *"criar uma rede europeia que reúna as competências científicas, técnicas e jurídicas existentes nos Estados-Membros que se encontrem ligadas à gestão dos nomes de domínio, dos endereços e dos protocolos Internet".*

[58] Directiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de Maio de 2001, relativa à harmonização de certos aspectos do direito de autor e dos direitos conexos na sociedade da informação. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001L0029 (Acedido aos 05-11-2019).

[59] Regulamento (CE) n° 808/2004, de 21 de Abril de 2004, relativo às estatísticas comunitárias sobre a sociedade da informação. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32004R0808 (Acedido aos 05-11-2019).
Nessa matéria a estatística é muito importante porque permite tomar ações concretas e corrigir os problemas detetados.

[60] Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social e ao Comité das Regiões – Criar uma Sociedade da Informação mais segura reforçando a segurança das infra-estruturas de informação e lutando contra a cibercriminalidade – eEurope 2002 de 26 de Janeiro de 2001. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52000DC0890 (Acedido aos 05-11-2019).

independentemente do local onde se encontra. Reconhece-se de uma forma geral que se impõe uma acção eficaz, tanto a nível nacional como internacional, a fim de lutar contra a criminalidade informática".

É nesse clima que em Novembro desse ano surge a Convenção de Budapeste sobre o Cibercrime[61] e quatro anos depois a Decisão-Quadro 2005/222/JAI, de 24 de Fevereiro relativa a ataques contras sistemas de informação, que serão objeto de tratamento aprofundado no próximo capítulo.

Apesar da ameaça que o cibercrime apresenta, a Comissão Europeia reconhecia que as tecnologias da informação, devido a facilidade de interação, geravam maior produtividade e que a nova sociedade do conhecimento devia ser inclusiva, por isso na Comunicação da Comissão ao Conselho – i2010[62] – persistiu-se na tónica da construção de "um espaço europeu da informação" que responda à "convergência digital".

As preocupações com "a literacia e competência digitais, inovação e investigação, segurança e interoperabilidade digital, o mercado único digital e a qualidade de acesso à Internet"[63] foram levantadas em Junho de 2010 quando foi aprovada a Agenda Digital, que substituiu o programa eEurope, constituindo assim "uma das iniciativas-bandeira da Estratégia Europa 2020"[64].

De tudo o que acima foi referido podemos notar que as tecnologias que motivaram o surgimento da sociedade de informação não são em si mesmo perniciosas, mas sim neutras. A sua periculosidade e os crimes que surgem nesses ambientes devem-se a sua má utilização.

Com o surgimento das redes sociais torna-se necessário a implementação de uma ampla campanha de formação preventiva[65] aliada à sensibilização[66] dos usuários, porque só

---

[61] A título meramente explicativo, importa dizer que a Convenção de Budapeste não é um diploma da União Europeia, mas sim um tratado internacional feito sob a égide do Conselho da Europa que não é órgão da União Europeia, ou seja, o Conselho da Europa e a União Europeia são duas organizações europeias distintas.

[62] Comunicação da Comissão ao Conselho, ao Parlamento Europeu, ao Comité Económico e Social Europeu e ao Comité das Regiões "i2010 – Uma sociedade da informação europeia para o crescimento e o emprego" de 01-06-2005. Disponível em https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PT:PDF (Acedido aos 05-11-2019).
Um ano antes era criada a Agência Europeia para a Segurança das Redes e da Informação (ENISA sigla em inglês) por via do Regulamento (CE) n° 460/2004 do Parlamento Europeu e do Conselho, de 10 de Março de 2004. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32004R0460 (Acedido aos 05-11-2019).

[63] Disponível em http://euroogle.com/dicionario.asp?definition=487 (Acedido aos 05-11-2019).

[64] Idem.

[65] A prevenção e a segurança no uso da informática são consideradas por Lourenço Martins como sendo indispensáveis. Este autor conforta-nos dizendo que "a tecnologia constitui uma parte do problema e também da solução". **MARTINS,** A. G. Lourenço. "Criminalidade Informática." Direito Da Sociedade Da Informação, vol. IV, Coimbra Editora, Junho de 2003, p. 15.

banindo a ignorância virtual teremos cidadãos menos suscetíveis aos ataques e maquinações dos criminosos cibernéticos.

E, por tudo exposto, comungamos com a aspiração segundo a qual "*se o alastramento do uso do computador e das redes de telecomunicações* vem potenciando a extensão da *cibercriminalidade*, que chegue o momento em que se converta no *melhor meio de a combater*. Sob a envolvência do direito"[67].

[66] José Macedo aponta "a prevenção, a consciencialização e celeridade" como sendo as melhores armas para combater a criminalidade informática. **MACEDO**, João Carlos Cruz Barbosa de, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, Coimbra Editora, 2009, p. 259.

[67] **MARTINS,** A. G. Lourenço. "Criminalidade Informática." Idem, p. 41.

Capítulo II – ENQUADRAMENTO INTERNACIONAL DA CRIMINALIDADE INFORMÁTICA

2.1. A Convenção de Budapeste sobre o cibercrime

Comprovando as imensas preocupações que iam sendo levantadas na última década do milénio passado derivadas da virtualização e globalização constantes das redes informáticas, em 23 de Novembro de 2001 o Conselho da Europa aprovou a Convenção de Budapeste sobre o Cibercrime visando "a protecção da sociedade da c*ybercriminalidade".*[68]

Como tratado de direito internacional, veio em substituição da Recomendação nº (89)9[69] e desde os seus primórdios manifestou ter "vocação universal", quer dizer que "pretendeu que a adesão a este tratado se alargasse à generalidade dos países do globo"[70].

É o mais significativo e abrangente tratado internacional em matéria dos crimes na Internet e no computador, sendo ratificado por vários países não pertencentes ao Conselho Europeu[71], dentre os quais alguns países africanos[72]. Em Setembro de 2019, 64 estados ratificaram a convenção, enquanto outros quatro a assinaram, mas não a ratificaram[73]. Desde então muitas outras leis que versam sobre essa temática têm seguido o espírito e a configuração desse tratado europeu, o que, reconhece seu pioneirismo legislativo.

Este diploma procura conciliar as leis nacionais através do aperfeiçoamento das técnicas aplicadas à investigação criminal e ao direito processual penal, adotando medidas de segurança cibernética e aprimorando a colaboração entre países, isto é, concebendo a implementação de um mecanismo de cooperação internacional.

---

[68] De acordo ao preâmbulo corresponde ao objeto da convenção.

[69] "Em 1989 o objecto geral da Recomendação era o *ambiente* dos computadores. Agora, além dos computadores, estão em causa as redes e os sistemas". **VERDELHO**, Pedro. "A Convenção Sobre Cibercrime do Conselho da Europa – Repercussões na Lei Portuguesa." Direito da Sociedade da Informação, vol. VI, Coimbra Editora, 2006, p. 260.

[70] Idem, p. 257.

[71] Já na sua elaboração teve a participação dos países observadores do Conselho da Europa: Canadá, Japão, Filipinas, África do Sul e Estados Unidos. Disponível em https://en.wikipedia.org/wiki/Convention_on_Cybercrime (Acedido aos 07-11-2019).

[72] Foi ratificado pelo Gana, Marrocos, Senegal e Cabo-Verde (sendo este o único país africano lusófono a fazê-lo). África do Sul foi o primeiro a assiná-lo em 23 de Novembro de 2001. Para além destes países foram ainda convidados a assinar, ratificar ou a aceder o Benim, a Nigéria e a Tunísia. (*vide*: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures Acedido aos 07-11-2019).

[73] Idem.

Preocupa-se igualmente com a problemática da densificação conceitual. No seu primeiro capítulo relativo a terminologia, apresenta as definições de "sistema informático", "dados informáticos", "prestador de serviços" e "dados de tráfego" respetivamente.

No tratamento dos cibercrimes a convenção separa-os em cinco categorias: "infracções contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos"; "infracções relacionadas com computadores"; "infracções relacionadas com o conteúdo"; "infracções respeitantes a violações do direito de autor e dos direitos conexos" e "outras formas de responsabilidade e sanções".

Na primeira estão incluídas as seguintes infrações: Acesso ilícito (art.º 2º), Intercepção ilícita (art.º 3º), Dano provocado nos dados (art.º 4º), Sabotagem informática (art.º 5.º) e Utilização indevida de dispositivos (art.º 6º). Na segunda temos apenas dois crimes: Falsificação informática (art.º 7º) e Burla informática (art.º 8º).

A terceira categoria diz respeito aos crimes de conteúdo relacionados com a Pornografia infantil (art.º 9º). Os direitos de autor e conexos são retratados na penúltima categoria para a "Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão" e "os Aspectos dos Direitos de Propriedade Intelectual" (art.º 10º).

Por fim, e representando uma avançada preocupação legislativa para a época, achamos a "Tentativa, auxílio ou instigação" (art.º 11º) e "Responsabilidade das pessoas colectivas"[74] (art.º 12º); culmina com o art.º 13º que aborda as "Sanções e medidas".

Sobre os crimes previstos podemos dizer resumidamente que a CB "trata basicamente de violações de direito autoral, fraudes relacionadas a computador, pornografia infantil e violações de segurança de redes"[75].

No Título 3 sobre a Rede 24/7 prevê que cada estado signatário tenha um ponto de contacto que deverá funcionar "24 horas por dia, sete dias por semana, a fim de assegurar de imediato a prestação de auxílio nas investigações e nos procedimentos relativos a infracções penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma electrónica, da prática de infracções penais" (art.º 35º nº 1).

Parece-nos que essa exigência tem motivado muitos países, principalmente africanos, a não aderirem a CB pela incapacidade de criarem um ponto de contacto que funcione

[74] Previsto no art.º 12º nº 2, pretende-se com esta previsão responsabilizar não apenas quem comete um crime informático a título individual como também quem o cometa estando sob autoridade de uma entidade pública. O nº 3 estatui aos estados-parte a necessidade de incluírem no seu direito interno conteúdos jurídicos que levem a responsabilização de uma pessoa coletiva, não só do ponto de vista penal, mas também civil ou administrativo.

[75] Disponível em https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes (Acedido aos 07-11-2019).

diariamente[76]. Tal seria impossível num país com carências básicas tais como a falha de luz elétrica, debilidade no acesso à *Internet*, a inexistência (ou existência em número reduzido) de pessoal tecnologicamente habilitado e carência de equipamento eletrónico adequado (art.º 35º nº 3).

Um país com as insuficiências supracitadas colocaria em causa, por exemplo, o auxílio mútuo internacional que é um dos aspetos de maior realce na CB.

Em 1 de Março de 2006 a CB foi enriquecida com a entrada em vigor do Protocolo Adicional à Convenção sobre Crimes Cibernéticos (doravante PACB). A sua ratificação impõe ao estado a criminalização da disseminação de material racista e xenófobo por meio de sistemas de computadores, bem como as ameaças e os insultos motivados por racismo ou xenofobia.

Apesar de já passarem mais de 18 anos desde a sua aprovação, este instrumento do direito público internacional que começou apenas com a subscrição de trinta países, sua importância e influência ainda são muito notórias em diversas legislações, por isso, representa deveras um grande feito não só para europa, como para toda Humanidade.

2.1.1. Países africanos que acederam à Convenção de Budapeste sobre o cibercrime[77]

Tal como já mencionamos, a CB já vigora em alguns países africanos, entretanto existem outros que unicamente a assinaram bem como alguns que foram convidados a assinar.

A África do Sul foi o primeiro país africano a assinar a CB bem como o PACB. À convenção fê-lo no mesmo ano em que foi aprovada, propriamente em 23 de Novembro de 2001. Tal compreende-se por ser a segunda maior economia de África[78] e em 2013 foi considerado o terceiro país com a maior taxa de cibercrimes, vitimando 73% da população[79].

---

[76] Tais dificuldades dos PoC (Points of Contact), ou seja, dos Pontos de Contacto, abrangem também países asiáticos como pode ler-se no ponto nº 4 do Relatório e Recomendações do Projeto ISEC *"Although in general terms the responses involving EU countries are acceptable, there are difficulties with Asian and African countries"*, p. 8. Disponível em https://www.canterbury.ac.uk/social-and-applied-sciences/law-criminal-justice-and-policing/docs/poc/PoC-24-7-Final-Report.pdf (Acedido aos 31-01-2020).

[77] A lista completa dos países que assinaram, ratificaram e adotaram a convenção está disponível em https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Acedido aos 10-11-2019).

[78] Atrás da Nigéria. Disponível em https://pt.wikipedia.org/wiki/África_do_Sul (Acedido aos 10-11-2019).

[79] Apenas foi superado pela Rússia (83%) e pela China (77%). De acordo ao *South African Banking Risk Information Centre (SABRIC)* a perda anual da África do Sul é estimada em 156 milhões de dólares. Disponível em https://africacheck.org/reports/does-south-africa-rank-third-in-the-world-for-online-crime-losing-r2-2bn-a-year/ (Acedido aos 10-11-2019).

De acordo com a organização internacional das telecomunicações em 2017 a África do Sul foi o terceiro país africano mais desenvolvido em termos das TICs[80] e tem um renomado Centro de Pesquisa em Informação na Universidade Nelson Mandela[81].

Em 2015 houve o projeto de lei sobre *Cybercrimes and Cybersecurity*[82] que, usava estruturas da Convenção de Budapeste sobre o cibercrime de 2004, porém foi reprovada pelas organizações empresariais e de direitos civis[83].

Contudo, um novo projeto de lei foi adotado em Novembro de 2018 e enviado à Assembleia Nacional para debate. O Conselho Nacional de Províncias fez as submissões por escrito do público em 8 de Março de 2019, aguarda-se a entrada em vigor.

As Ilhas Maurícias ratificaram em 16 de Dezembro de 2013 e implementaram em 1 de Março de 2014.

Seguiu-se o Senegal que ratificou em 16 de Dezembro de 2016, entrando em vigor no dia 1º de Abril do ano seguinte.

Esses foram os três primeiros países africanos a ratificar CB. Seguiram-se Cabo-Verde, Marrocos e Ghana. Os países convidados que ainda não manifestaram o seu acolhimento são a Nigéria e a Tunísia.

Cabo-Verde é o único lusófono a fazê-lo. Ratificou em 16 de Junho de 2018 e no dia 1º de Outubro do mesmo ano registou-se a entrada em vigor.

Já foi referido anteriormente, Cabo Verde aparece como o quarto em implementação das TICs em África e de acordo com as estatísticas da Agência Nacional das Comunicações (ANAC) em 2016 a taxa de penetração de acesso à Internet era já de 70%[84], uma percentagem verdadeiramente notável para um país africano.

Em 11 de Abril de 2019 o Conselho da Europa solicitou a adesão à CB aos países lusófonos por formas a falarem de "uma só voz".

Tal apelo foi feito por Manuel Almeida Pereira, gestor de projeto no Gabinete de Cibercriminalidade do Conselho de Europa, no âmbito duma conferência internacional que decorreu na cidade de Praia sobre o cibercrime e a prova eletrónica para a CPLP[85].

---

[80] Ultrapassado apenas pela Malásia e Seychelles, em 4º lugar aparece Cabo Verde. Angola aparece no modesto 160º lugar. Disponível em https://www.itu.int/net4/ITU-D/idi/2017/index.html (Acedido aos 10-11-2019).

[81] Em inglês *Centre for Research in Information and Cyber Security*. Disponível em *https://crics.mandela.ac.za* (Acedido aos 10-11-2019).

[82] Disponível em http://cybercrime.org.za/docs/Cybercrimes_and_Cybersecurity_Bill_2015.pdf (Acedido aos 10-11-2019).

[83] Disponível em https://portswigger.net/daily-swig/south-africa-welcomes-new-cybercrime-legislation (Acedido aos 10-11-2019).

[84] Disponível em https://cvtradeinvest.com/tics (Acedido aos 10-11-2019).

[85] Disponível em https://www.dn.pt/lusa/conselho-de-europa-pede-adesao-de-paises-lusofonos-a-convencao-sobre-cibercrime–10785869.html (Acedido aos 10-11-2019).

Angola, Moçambique e São Tome já requereram a intervenção do Conselho da Europa por formas a ajudá-los.

Preocupante é a situação da Guiné-Bissau, onde nem sequer "existe uma única palavra legislativa contra o cibercrime."[86]

Portanto, as taxas de adesão da CB por parte dos países africanos são ainda muito baixas. Num total de 54 países somente em 5 deles essa legislação vigora, resultando numa taxa de implementação de 9%, por isso mais esforço deve ser envidado por formas a reverter-se esse quadro.

2.2. A Convenção da União Africana sobre a cibersegurança e proteção de dados pessoais

A Convenção da União Africana sobre a cibersegurança e proteção de dados pessoais[87] foi adotada em 27 de Junho de 2014 em Malabo, Guiné Equatorial[88], por esse facto é também designada Convenção de Malabo (doravante CM), aliás como sucede com a Convenção de Budapeste.

Tal como a sua designação evidencia, tem uma dupla abrangência, isto é, além de referir-se à criminalidade cibernética, trata igualmente do regime que deve ser aplicado em matérias relativas ao respeito pelos dados das pessoas.

Seguindo o espírito da CB, visou materializar os princípios gizados pela Iniciativa da Sociedade de Informação Africana (AISI)[89] e do Plano de Ação Regional para a Economia do Conhecimento (ARAPKE)[90] que tinham em vista a construção da Sociedade de Informação.

---

[86] Idem.

[87] Disponível em https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (Acedido aos 12-11-2019).

[88] Por esse facto é também designada de **Convenção de Malabo**. Por exemplo confira-se em http://www.parlamento.cv/GDiploApro3.aspx?CodDiplomasAprovados=80329 (Acedido aos 31-10-2020) e também pode ler-se em *Directrizes relativas à Protecção de Dados Pessoais para África – Uma iniciativa conjunta da Internet Society e Comissão da União Africana 9 de Maio de 2018*, p. 9. Disponível em https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_201809June_Final_Portuguese.pdf (Acedido aos 31-10-2020).

[89] **African Information Society Initiative** (AISI) é uma estrutura regional implementada em 1996 resultante de uma Resolução (812 – XXXXI) adotada pela Conferência de Ministros da ECA (**Economic Comission for Africa**, Comissão Económica para África). Visou a construção da

Dos vários objetivos que apresenta destaca-se a determinação de "normas de segurança essenciais para a criação de um espaço digital credível para as transacções electrónicas, protecção de dados pessoais e luta contra o cibercrime"[91].

A CM realça também a fixação de desafios para progresso do "comércio eletrónico ligados a problemas de segurança", o que se compreende devido ao impulso dado pela Comissão Económica Africana para o surgimento da convenção.

No que ao direito penal substantivo e adjetivo diz respeito pretende, respetivamente, "modernizar os instrumentos de repressão ao crime" e definir um "quadro de adaptação de procedimentos normativos" relativos às TICs.

Já nesta época reconhecia-se que "a actual situação da criminalidade informática" constituía realmente uma ameaça à "segurança das redes informáticas", sendo por esse motivo urgente "definir as grandes orientações da estratégia à regressão" do cibercrime.

Tem 38 artigos repartidos em quatro capítulos, mas antes deles aparece o art.º 1º que apresenta de forma sucinta a definição das expressões fundamentais a serem referidas na convenção, começando por definir a pornografia infantil.

O primeiro capítulo trata das transações ligadas ao comércio eletrónico, o que denota mais uma vez que as preocupações económicas é que motivaram o combate à generalidade dos crimes digitais. Abrange um total de cinco artigos (do 2º ao 7º).

O tema abordado no segundo capítulo é o da proteção de dados pessoais, ocupando maior parte da convenção, indo do 8º ao 23º artigos. O art.º 11º aconselha a criação da Autoridade Nacional de Proteção de Dados cujas atribuições aparecem no artigo seguinte.

Releva-se neste capítulo a apresentação no art.º 13º dos Princípios de Base que regem o Processamento de Dados Pessoais, num total de seis.

O direito a correção dos dados e ao apagamento ou esquecimento também são instituídos (art.º 19º). O capítulo culmina com os comprometimentos do responsável pela proteção de dados.

O terceiro capítulo, o que mais nos interessa por estar intrinsecamente ligado ao nosso tema, trata da promoção da cibersegurança e da luta contra o cibercrime. Dividido em três

---

Sociedade da Informação de África por formas a ajudar o continente a "acelerar seus planos de desenvolvimento, estimular o crescimento e oferecer novas oportunidades em educação, comércio, assistência médica, criação de empregos e segurança alimentar, ajudando os países africanos a ultrapassar os estágios de desenvolvimento e aumentar seus padrões de vida". Disponível em https://www.uneca.org/publications/african-information-society-initiative-aisi-decade's-perspective (Acedido aos 12-11-2019).

[90] **African Regional Action Plan on the Knowledge Economy** (APARKE) foi adotado em Agosto 2005 como resposta ao Plano de Ação de Genebra da Cúpula Mundial sobre a Sociedade da Informação (WSIS, **World Summiton the Information Society**) de 2003 e dos Compromissos de Accra para a WSIS Tunis realizado em 4 de Fevereiro de 2005 em Accra, Ghana, que estabeleceu uma agenda digital africana em um mundo globalizado. (Disponível em http://www.itu.int/net/wsis/docs2/regional/outcome-accra.pdf Acedido Acedido em 12-11-2019)

[91] Lê-se na p. 1 do preâmbulo.

secções, a primeira elenca as medidas de cibersegurança a serem tomadas a nível nacional (art.º 24º ao 28º).

O art.º 24º começa por apresentar o "Quadro Nacional da Cibersegurança". No seu nº 1, sobre a política nacional, fala da necessidade de cada estado-membro reconhecer e identificar as Infraestruturas Críticas de Informação (ICI) assim como os riscos que as mesmas representam. O nº 2, sobre a estratégia nacional, aconselha os estado-membros a implementarem uma política nacional de cibersegurança por intermédio de uma reforma legislativa e que estabeleçam prazos para a sua implementação.

Sobre os prazos pensamos que seria bom que a própria convenção os apresentasse[92], não deixando ao critério de cada estado estabelecer os seus próprios.

O art.º 25º apresenta os padrões normativos a seguir, sugerindo cada estado a:

1. Legislar sobre o combate ao cibercrime;
2. Instituir as Autoridades Reguladoras Nacionais;
3. Assegurar os Direitos dos Cidadãos; e a
4. Proteger as infraestruturas críticas.

O art.º 26º diz que o Sistema Nacional de Cibersegurança deve envolver a cultura de cibersegurança, o papel dos governos, a parceria público-privada e educação e formação. Este último aspeto é de grande importância e passaria pela introdução de conteúdos que ensinassem os cidadãos a terem um uso preventivo da Internet, expondo os principais perigos e ataques que podem estar sujeitos[93].

A criação de estruturas nacionais de acompanhamento da cibersegurança é o mote do art.º 27º.

Essa estrutura deve assegurar a "Gestão da Cibersegurança" pela existência de um responsável para o efeito, uma liderança forte coadjuvada por profissionais competentes; devem

[92] Serviria como forma de pressão positiva e faria com que os estados trabalhassem com maior preocupação.

[93] Nesse aspeto Cabo-Verde é um grande exemplo e implementou no ano letivo 2009/2010 a integração das TICs nas escolas do ensino secundário, tendo atualmente repercussões muito positivas em toda sociedade.
No Decreto-legislativo nº 2/2010 que revê as Bases do Sistema Educativo, de 7 de Maio de 2010, nela consagrou-se com exclusividade um capítulo sob o título **"Tecnologias de Informação e Comunicação e a Sociedade do Conhecimento"**. O Artigo 60º deste documento propugna o seguinte: "O Estado promove a utilização das tecnologias da informação e comunicação no sistema educativo, de modo a contribuir para a elevação da qualidade e da eficácia do ensino, (...) ". *Vide* **SILVA**, José da Cruz Andrade e. A integração das TIC no ensino secundário em Cabo Verde: Um estudo de caso. Departamento de Educação e Ensino a Distância. Mestrado em Comunicação Educacional Multimédia. Universidade Aberta, Lisboa. Novembro de 2014, p. 4 e 5. Disponível em https://repositorioaberto.uab.pt/bitstream/10400.2/3904/1/TMCEM_JoseSilva.pdf (Acedido aos 12-11-2019).

também estar envolvidas as entidades privadas e abranger um maior número possível de áreas. Deve igualmente criar um "Quadro Institucional" de combate a criminalidade cibernética.

A "Cooperação Internacional" é retratada no art.º 28º que deverá concretizar-se através da:

- ✓ ***Harmonização*** não somente a nível nacional como também a nível regional*;*
- ✓ ***Cooperação judiciária*** pondo-se a tónica ao estabelecimento de acordos de assistência mútua em matérias de cibercriminalidade*;*
- ✓ ***Troca de informações*** incentivando-se a Criação de uma Equipa de Resposta à Emergências Informáticas (CERT – Computer Emergency Response Team) ou de Equipas de Respostas a Incidentes no Domínio da Cibersegurança (CSIRTS – Computer Security Incident Response Team) que trocam informações sobre as eventuais ciberameaças bem como a avaliação de vulnerabilidades*;* e
- ✓ ***Meios de cooperação*** que podem ser intergovernamentais, regionais ou em parceria público-privadas.

A secção II, referente às disposições penais, começa por discriminar as infrações que representam ofensas específicas contra as TICs (art.º 29º), sendo: os ataques contra sistemas informáticos[94]; as violações de dados informatizados[95]; as infrações relativas ao conteúdo[96] e as relativas às medidas de segurança das trocas comerciais e eletrónicas[97].

A adaptação de algumas infrações às TICs está consignada no art.º 30º e diz respeito às ofensas contra a propriedade[98] e à responsabilidade das pessoas coletivas[99].

O capítulo II termina com o art.º 31º que continua fazendo a adaptação já de sanções penais ligadas às TICs. Recomenda a punição das ofensas citadas, incluindo multas que sirvam como meios de dissuasão. Também as violações da confidencialidade de dados e do segredo profissional aconselha-se a serem condenadas.

---

[94] Esse ponto nº 1 começa por criminalizar o acesso ilegal e o dano informático, mas importa destacar a alínea g) que estatui que os estados-membros devem obrigar "os vendedores de tecnologia de comunicação e informação a realizar, através de peritos ou investigadores independentes na área de cibersegurança, ensaios de vulnerabilidades e avaliações de garantia de segurança e divulgar aos consumidores todas as vulnerabilidades detetadas nos produtos assim como as soluções recomendadas para a sua correção".

[95] No nº 2 incluem os comportamentos que preenchem os ilícitos penais de burla informática, interceção ilegal e sabotagem informática.

[96] Nessas infrações previstas no nº 3 está a pornografia infantil em maior percentagem; os aspetos relativos a discriminação como o racismo e a xenofobia; a apologia ao genocídio e outros crimes contra a humanidade. Não menciona a proteção aos direitos de autor e conexos, mas entendemos que aplica-se *mutatis mutandis*. Quanto a matéria do crime impõe o seu confisco.

[97] Traz uma questão muito sucinta e moderna: a necessidade de admissão da prova digital.

[98] No cometimento de "furto, fraude, transação de bens roubados, abuso de confiança, extorsão de dinheiro, terrorismo e branqueamento de capitais", a convenção recomenda a considerar como circunstância agravante o uso das TICs.

[99] Não exclui "a responsabilidade das pessoas singulares autoras ou cúmplices".

Sobre o direito processual, o último item do art.º 31º estabelece as medidas relativas a garantir o curso normal da investigação e as competências e atribuições do juiz de instrução.

O último capítulo (art.º 32º a 38º), como é habitual, é o referente às disposições finais e reforça a importância do combate à violação dos direitos humanos no ciberespaço e a assessoria que o Presidente da Comissão deve prestar aos governos africanos (art.º 32º).

No caso de litígios, o art.º 34º diz que os mesmos "devem ser resolvidos de forma amigável por via da negociação direta entre os estados interessados", mas caso não haja êxito então devem recorrer a meios pacíficos tais como "bons-ofícios, mediação e conciliação".

A convenção pode ser assinada, ratificada ou aderida (art.º 35º) e está sujeita a emendas ou revisões por qualquer estado-parte (art.º 37º).

Em seguida, analisaremos alguns países que, com base nas convenções europeia e africana, implementaram na sua jurisdição a lei de combate ao cibercrime.

2.3. A regulação dos crimes informáticos em alguns países africanos

De acordo com a consultoria britânica Ovum[100], mais de um bilhão de pessoas em África terão acesso à Internet até 2022[101].

Atualmente, as África está entre os continentes em que mais se regista um crescimento das atividades ligadas aos crimes cibernéticos[102]. A região é igualmente uma fonte de ataques cibernéticos significativos direcionados a outras partes do mundo. No entanto, várias medidas têm sido tomadas por vários países para enfrentar essas ameaças e melhorar a segurança cibernética.

Esses estados desenvolveram legislações para combater as ameaças do ciberespaço, também reforçaram as medidas de execução e envidaram esforços para desenvolver o setor privado e consequentemente fortalecer a segurança cibernética por intermédio da regulação.

Com base em um relatório de Novembro de 2016 da Comissão da União Africana (AUC – African Union Commission) e da empresa de segurança cibernética Symantec, dos 54 países da África, 30 careciam de disposições legais específicas para combater o cibercrime e lidar com

---

[100] A **Ovum** é uma empresa de consultoria independente, com sede em Londres, especializada em cobertura global dos setores de telecomunicações, mídias e tecnologia.

[101] Disponível em https://www.consultancy.africa/news/30/africa-will-break-through-1-billion-mobile-internet-connections-by-2022 (Acedido aos 14-11-2019).

[102] **KSHETRI**, Nir. Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management. Published online: 09 Apr. 2019.
Disponível em https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527 p. 77 (Acedido aos 14-11-2019).

provas digitais[103] o que significa que mais da metade dos países não tinha legislação sobre o crime digital nesse ano.

Estudaremos as legislações de alguns desses países tocando nos seus aspetos essenciais. Os países selecionados são as Ilhas Maurícias, a Nigéria e Cabo-Verde.

Esta seleção é propositada e justifica-se pelo facto dos três países fazerem parte do GLACY+[104].

Importa ainda referir que as Ilhas Maurícias foi o primeiro país africano a elaborar uma lei de combate ao cibercrime, dois anos após a implementação da Convenção de Budapeste.

A Nigéria além de ser a maior economia africana é igualmente o país mais populoso do continente, tem sido objeto de vários ataques informáticos e regista avanços significativos na regulação das infrações cibernéticas.

Quanto a Cabo-Verde, a preferência é óbvia. É o primeiro país dos PALOP a ter uma lei sobre os cibercrimes[105], sendo por isso um exemplo para os demais, em especial para Angola. No que concerne as TICs tem tido uma evolução legislativa exemplar muito impulsionada pela estreita cooperação que tem com Portugal e com a própria União Europeia.

2.3.1. Ilhas Maurícias[106]

Este país insular do índico, que aderiu a Convenção de Budapeste em Novembro de 2013, implementou em 30 de Julho 2003 a ***Lei de Uso Indevido de Computadores e Crimes Cibernéticos***[107] para prever a repressão de atividades criminosas perpetradas através de sistemas de computador. Representou uma significativa evolução legislativa para época, estreando-se no continente em tal procedimento.

---

[103] Idem p. 78.

[104] O GLACY+ é um projeto conjunto da União Europeia (Instrumento que Contribui para a Paz e a Estabilidade) e o Conselho da Europa.
Visa estender a experiência do projeto GLACY (2013 – 2016) e apoia doze países prioritários e centrais na África, Ásia-Pacífico e América Latina e região do Caribe – **Cabo Verde**, Chile, Costa Rica, República Dominicana, Gana, **Ilhas Maurícias**, Marrocos, **Nigéria**, Filipinas, Senegal, Sri Lanka e Tonga.
Esses países podem servir como *hubs* para compartilhar suas experiências em suas respetivas regiões.
Disponível em https://www.coe.int/en/web/cybercrime/glacyplus (Acedido aos 14-11-2019).

[105] Em 20 de Março de 2017. Seguiu-se São Tomé que aprovou a sua lei do cibercrime em 6 de Outubro de 2017.

[106] O progresso legislativo deste país é impulsionado pelo facto de fazer parte ao mesmo tempo da Commomwealth, da Francofonia e da União Africana. Destaca-se também por ser o segundo país africano melhor classificado no índice de desenvolvimento humano. Disponível em https://pt.wikipedia.org/wiki/Maurícia (Acedido aos 14-11-2019).

[107] A sua designação original é *The Computer Misuse And Cybercrime Act 2003*. Disponível em https://www.wipo.int/edocs/lexdocs/laws/en/mu/mu012en.pdf (Acedido aos 14-11-2019).

É um país que desde muito cedo preocupou-se com a regulação das TICs e já em 2001 tinha aprovado a Lei da Informação e das Tecnologias de Comunicação (Information and Communication Technologies Act 2001)[108]. Em 2004 aprovou a Lei de Proteção de Dados[109] e em 2014 a Lei dos Direitos do Autor[110] que regula também a reprodução, adaptação de programas de computador e descompilação (21º ponto).

O governo desta ilha acredita que o seu desenvolvimento económico está ligado ao estabelecimento das TICs, sendo este o sector chave e para tal tem muitas agências[111] que trabalham neste sentido.

No seu programa *A Visão das Maurícias para 2030 – Inovação e Competitividade Globalmente*[112] – fala da intenção de transformá-la numa ilha inteligente (*smart island*), cibernética (*cyber island*) e no *hub* do oceano pacífico.

É uma lei de 23 itens, distribuídos em 4 secções, aí designadas de "Partes".

A primeira Parte faz uma exposição introdutória em dois artigos – apresenta a nomenclatura da lei e como ela deve ser interpretada. Descreve as novas realidades da sociedade da informação e faz referência às atividades ilegais emergentes na rede. Ainda explica o que é a Convenção de Budapeste sobre Cibercrime e sublinha a importância de ser considerado apenas um único instrumento internacional vinculativo no combate ao cibercrime.

O item 2 explica as noções principais ligadas à computação, onde são definidos dentre outros o "acesso", "os serviços de computação", "o sistema de computador", "a criptografia assimétrica", "os dados", "a palavra-passe" e "a chave privada". Algumas dessas designações atualmente sofreram alterações, o que se compreende por ser uma lei com mais de quinze anos.

A segunda Parte apresenta o quadro nominal dos tipos de crime sobre a matéria, expondo do item 3 ao 10 todas as ilicitudes.

---

[108] Disponível em https://www.icta.mu/docs/laws/ict_act.pdf (Acedido aos 14-11-2019).

[109] Data Protection Act 2004. Disponível em https://www.wipo.int/edocs/lexdocs/laws/en/mu/mu011en.pdf (Acedido aos 14-11-2019). Esta lei foi revogada pela Data Protection Act 2017 que pode ser encontrada em https://rm.coe.int/dpa-2017-maurice/168077c5b8 (Acedido aos 14-11-2019).

[110] The Copyright Act 2014. Disponível em https://www.wipo.int/edocs/lexdocs/laws/en/mu/mu024en.pdf (Acedido aos 14-11-2019).

[111] Essas agências são:

- The Cibercrime Unit:
- Information & Communication Tecnology Authority;
- National Cybercrime Prevention Committee (NCPC);
- The Mauritian Computer Emergency Response Team (CERT-UM).

[112] Mauritius and the Vision 2030 – Innovation and Competitiveness Globally. Disponível em https://www.un-page.org/files/public/mauritius_jan-feb_2017_reprint_compr.pdf (Acedido aos 14-11-2019).

Dito isto, os oito crimes previstos são os seguintes:

- Acesso não autorizado a dados do computador;
- Acesso com intenção de cometer delitos;
- Acesso não autorizado e intercetação de serviços de informática;
- Alteração não autorizada de material informático;
- Dano ou negação de acesso ao sistema do computador;
- Divulgação não autorizada de palavra-passe;
- Posse ilegal de dispositivos e dados;
- Fraude eletrónica.

A terceira Parte trata dos aspetos ligados aos procedimentos de investigação criminal e instrução processual, tais como as formas de preservação das provas; as regras de divulgação de dados preservados; a ordem de produção dos dados; os poderes de acesso, busca e apreensão para fins de investigação; a coleta em tempo real de dados de tráfego; o pedido de exclusão, e; o limite no uso de dados e informações divulgados.

A quarta Parte dos diversos aborda nos itens 19, 20 e 21 as questões relativas à jurisdição, à cooperação internacional (propriamente a extradição) e ao confisco dos bens ligados ao crime.

O item 23 faz algumas alterações como consequência da entrada em vigor da presente lei. Inicia por alterar a Lei de Proteção à Criança de 1994[113], fazendo uma mudança significativa visando combater a pornografia infantil. Reequaciona o tratamento das imagens das crianças no subtítulo *Indecent photographs of children*.

O mesmo item altera as secções 86 e 105 do Código Penal, esta última que fala do documento eletrónico ou da composição literária, por manifesta preocupação aos direitos do autor.

No último item revoga as seções 369A e 369B do Código Penal.

De forma resumida esses são os assuntos essenciais abordados nessa lei.

Não obstante, as preocupações desta nação com a cibersegurança continuam até os dias de hoje e em Agosto de 2017 o Ministério da Tecnologia, Comunicação e Inovação publicou

[113] Child Protection Act. Disponível em http://dpp.govmu.org/English/Documents/Legislation/CHILD%20PROTECTION.pdf (Acedido aos 14-11-2019).

a *Estratégia para o Cibercrime 2017-2019*[114] onde é exposta a visão, a missão, os objetivos, as prioridades, o plano de ação e a resposta nacional para a luta contra as ameaças cibernéticas.

Estudaremos a seguir os aspetos de realce da lei nigeriana.

2.3.2. Nigéria

A institucionalização dos pagamentos eletrónicos na República Federativa da Nigéria fez crescer os crimes ligados à fraude eletrónica, o que motivou o setor financeiro nigeriano a criar em 2000 o Fórum Nigeriano da Fraude Eletrónica (Nigerian Electronic Fraud Forum – NEFF).

Este fórum tem por objetivo "permitir o intercâmbio de informações e o compartilhamento de conhecimentos sobre questões de fraude entre os principais interessados, com o objetivo de garantir uma abordagem colaborativa e proactiva para combater/mitigar fraudes e limitar ocorrências e perdas. Ainda este fórum deseja "servir como um órgão oficial para representar a posição do setor em questões relacionadas à fraude, oferecendo soluções que restauram a confiança do público no uso de cartões e pagamentos eletrónicos em geral".

Procurando melhorar a segurança e a confiança dos pagamentos com cartão, nos anos de 2014[115], 2015[116] e 2016[117] o NEFF publicou relatórios anuais sobre as suas atividades intitulados *e-Fraud: Fighting the Battle, Wining the War; Improving and Securing Cyber Environment* e *A Changing Payments Ecosystem: The Security Challenge*, respetivamente.

Em 1 de Janeiro de 2005 iniciou oficialmente a operacionalização da Unidade de Inteligência Financeira da Nigéria (Nigerian Financial Intelligence Unit – NFIU)[118] com a missão de assegurar a "aplicação da lei, investigações, recolha de evidências eletrónicas e justiça criminal em crimes cibernéticos"[119].

---

[114] Cybercrime Strategy 2017-2019. Disponível em http://cert-mu.govmu.org/English/Documents/Cybercrime%20Strategy/National%20Cybercrime%20Strategy-%20August%202017.pdf (Acedido aos 14-11-2019).

[115] Disponível em https://www.cbn.gov.ng/Out/2016/CCD/NEFF%202014%20Annual%20Report%20.pdf (Acedido aos 14-11-2019).

[116] Disponível em https://www.cbn.gov.ng/Out/2016/CCD/NeFF-%20Annual%20Report%202015.pdf (Acedido aos 14-11-2019).

[117] Disponível em https://www.cbn.gov.ng/Out/2017/CCD/A%20CHANGING%20PAYMENTS%20ECOSYSTEM%20NeFF%202016%20Annual%20Report.pdf (Acedido aos 14-11-2019).

[118] Disponível em https://egmontgroup.org/fr/node/2528. Para mais informações sobre essa organização pode ler-se Nigerian financial intelligence unit serves as a tool to protect the integrity of the nigerian financial system 2013. Disponível em https://www.academia.edu/11145613/NIGERIAN_FINANCIAL_INTELLIGENCE_UNIT_SERVES_AS_A_TOOL_TO_PROTECT_THE_INTEGRITY_OF_THE_NIGERIAN_FINANCIAL_SYSTEM (Acedido aos 14-11-2019).

[119] Disponível em https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Nigeria_2.pdf (Acedido aos 14-11-2019).

É no âmbito dessas e outras preocupações que esse país pôs em vigor em 5 de Maio de 2015 a Lei do Cibercrime (na versão original *Cybercrime Act 2015*[120]), seguida de conferências de esclarecimentos aos interessados, feitas pela Sociedade de Segurança da Informação da África. Subdividida em sete partes que serão a seguir descritas.

A primeira parte refere-se aos objetivos e a aplicação. No seu art.º 1º pode ler-se que esta lei tem como objetivo:

a) Fornecer uma estrutura legal, regulamentar e institucional eficaz e unificada para a proibição, prevenção, deteção, acusação e punição de crimes cibernéticos na Nigéria;

b) Garantir a proteção da infraestrutura crítica de informações nacionais; e

c) Promover a cibersegurança e a proteção de sistemas e redes de computadores, comunicações eletrónicas, dados e programas de computador, propriedade intelectual e direitos de privacidade.

Na segunda parte temos vários sub-temas. Começa por tratar da Proteção das Infraestruturas Críticas de Informação Nacional; trazendo depois, consecutivamente, a designação de certos sistemas ou redes de computadores, como infraestrutura crítica de informações nacionais, e auditoria e inspeção de infraestrutura crítica de informações nacionais.

Apenas dois artigos são reservados a esta parte inicial. Na terceira temos a fração de maior abordagem, indo do art.º 5º ao 20º.

Tem como sub-tema Delitos e Penalizações e vai abordando em cada artigo os seguintes crimes: Infrações contra infraestruturas críticas de informação nacionais; Acesso ilegal a um computador; Interceção ilegal de comunicações; Modificação não autorizada de dados do computador; Interferência do sistema; Uso indevido de dispositivos; Falsificação relacionada a computadores; Fraude relacionada a computadores; Roubo de identidade e representação; Pornografia infantil e crimes relacionados; *Cyberstalking*[121]; *Cybersquatting*[122]*;* Ciberterrorismo;

[120] Disponível em https://www.unodc.org/res/cld/document/cybercrime-act_html/CYBERCRIMEACT-2015.pdf (Acedido aos 14-11-2019).

[121]... consiste no uso de ferramentas tecnológicas com o objetivo de perseguir ou assediar uma pessoa. Disponível em https://pt.wikipedia.org/wiki/Cyberstalking (Acedido aos 14-11-2019).

Infrações racistas e xenófobas; Tentativa, conspiração, auxílio e cumplicidade; Responsabilidade corporativa.

Pelos crimes acima discriminados damos conta que a lei nigeriana segue não só a CB como o seu Protocolo Adicional, por isso procura combater os delitos ligados a pornografia infantil e os relacionados com o racismo e a xenofobia. Responsabiliza ainda as pessoas coletivas.

Mas nesse aspeto a lei vai mais além, pois faz menção expressa de ataques específicos como o *Cyberstalking* e *Cybersquatting,* por serem muito frequentes naquele país.

Na quarta parte relata os deveres dos prestadores de serviços. Esses deveres referem-se a:

- Retenção de registros e proteção de dados; quer dizer que "um provedor de serviços deve manter todos os dados de tráfego e informações de assinantes, conforme prescrito pela autoridade relevante por enquanto responsável pela regulamentação dos serviços de comunicação na Nigéria";
- Interceção de comunicações eletrónicas "quando houver motivos razoáveis para suspeitar que o conteúdo de qualquer comunicação eletrónica seja razoavelmente necessário para os fins de uma investigação ou processo criminal"; e
- Falha do prestador de serviços em executar determinadas tarefas, para essas situações a lei prevê a pena de prisão e multas altíssimas ao "diretor, gerente ou oficial do prestador de serviços que for o responsável".

Para mais esclarecimentos sobre o assunto pode ler-se: **NDUBUEZE**, Philip; **HUSSEIN**, Mustapha D. & **SARKI**, Zakariyya Muhammad. *Cyberstalking Awareness and Perception among Undergraduate Students in Nigeria.* Dutse Journal of Humanities and Social Sciences Vol. 2, N° 2, September 2017. Disponível em https://www.researchgate.net/publication/325103033_Cyberstalking_Awareness_and_Perception_among_Undergraduate_Students_in_Nigeria (Acedido aos 14-11-2019).

De acordo a EFF (Eletronic Frontier Foundation), uma organização estadunidense sem fins lucrativos que defende a privacidade digital, a liberdade de expressão e a inovação, há uma preocupação gritante desse delito principalmente no campo político. Disponível em https://www.eff.org/deeplinks/2019/09/nigeria-misuses-overbroad-cyberstalking-law-levels-charges-against-political (Acedido aos 14-11-2019).

[122] **Cybersquatting** (também conhecido como **domain squatting**), de acordo com a lei federal dos Estados Unidos conhecida como *Anticybersquatting Consumer Protection Act*, consiste em registrar, traficar ou usar um nome de domínio da internet com má-fé, visando lucrar com a boa vontade de uma marca pertencente a alguém. O **cybersquatter** então se oferece para vender o domínio para a pessoa ou empresa que possui uma marca registrada contida no nome por um preço inflacionado. Disponível em https://en.wikipedia.org/wiki/Cybersquatting (Acedido aos 14-11-2019).

Para melhor compreensão do cibersquatting na Nigéria pode ler-se em **IBEKWE**, Chibuko Raphael. The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions. A Thesis Submitted to the School of Law, University of Stirling for the Degree of Doctor of Philosophy (PhD). July 2015. Nas páginas 180 a 188 o autor fala sobre **New Era of cibersquatting**.

A Coordenação e a Execução, o Estabelecimento do Conselho Consultivo para o Cibercrime e as Funções e Poderes do Conselho, são os assuntos apresentados na quinta parte, intitulada *Administração e Execução*.

A parte seguinte aborda as revistas, as buscas e apreensões dos bens relacionados com o crime, delineando nos seus artigos (do 27º ao 32º) as entidades competentes.

Cabe ao agente da lei executá-las, desde que esteja devidamente autorizado pelo poder judicial, podendo apreender qualquer computador ou dispositivo e ainda um material relevante nele achado.

Compete aos agentes da lei conduzir as investigações e as buscas, porém só é admissível em casos urgentes em que o atraso prejudicaria a manutenção da ordem pública. Nos outros casos só poderão atuar se estiverem judicialmente mandatados.

Caso neste processo ocorram situações de obstrução ou recusa em divulgar informações, a pessoa implicada será sancionada com a pena de prisão que vai até dois anos acrescida de multa, competindo à Procuradoria-Geral da República exercer a ação penal de todos os crimes contidos nesta lei.

Esta sexta parte continua falando da ordem de confisco de ativos e finaliza abordando sobre a ordem de pagamento de compensação ou restituição.

A sétima parte, que vai do art.º 33º ao 39º, trata da jurisdição e da cooperação internacional. No art.º 35º nº 2 lê-se que a cooperação conjunta só será feita com países com os quais existe acordo bilateral.

Curiosamente nessa lei nigeriana as principais definições e conceitos em vez de constarem no início, são dados na última parte dos diversos, propriamente no art.º 42º, dentre eles destacamos o acesso autorizado, o dado de conteúdo, o programa de computador, a comunicação eletrónica e o registo eletrónico.

Na lei vem ainda anexada a discriminação dos Membros do Conselho Consultivo do Cibercrime[123] que têm as seguintes funções[124]:

---

[123] O Comitê Consultivo para o Crime Cibernético será composto por um representante de cada um dos Ministérios, Departamentos e Agências seguintes:

(a) Ministério Federal da Justiça;
(b) Ministério Federal das Finanças;
c) Ministério dos Negócios Estrangeiros;
(d) Ministério Federal do Comércio e Investimento;
(e) Banco Central da Nigéria;
(f) Conselheiro de Segurança Nacional;
(g) Serviço de Segurança do Estado;
h) Força Policial da Nigéria;

a) Criar um ambiente propício para o compartilhamento de informações e experiências;
b) Formular diretrizes de políticas relativas à implementação das disposições da Lei de Crimes Cibernéticos de 2015;
c) Assessorar em medidas preventivas e outras relacionadas a crimes cibernéticos e segurança cibernética;
d) Promover treinamento e educação, incluindo pesquisas e estágios.

Portanto, a Nigéria tem progredido na criminalização e punição dos crimes informáticos destacando-se na produção da prova digital, já tendo inclusive alguma jurisprudência em alguns processos do género[125].

2.3.3. Cabo Verde

Com a ajuda de Portugal, Cabo Verde tem dado passos significativos conducentes ao combate do cibercrime[126].

Tal como já referimos antes, o país aderiu à Convenção do Conselho de Europa (Convenção de Budapeste)[127] e tem aprovado, desde Março de 2017, a lei sobre o cibercrime (Lei 08/IX/2017)[128].

(i) Comissão de Crimes Económicos e Financeiros,
(j) Comissão Independente de Práticas Corruptas;
(k) Agência de Inteligência da Nigéria;
l) Corpo de Defesa Civil da Nigéria;
(m) Agência de Inteligência e Defesa;
(n) Agência de Inteligência Militar;
(o) Agência Nacional para a Proibição do Tráfico de Pessoas;
(p) Serviço Alfandegário da Nigéria;
q) Serviço Nigeriano de Imigração;
(r) Agência de Inteligência Financeira da Nigéria;
(s) Agência Nacional de Gerenciamento do Espaço;
t) Direção Nigeriana de Desenvolvimento da Tecnologia da Informação;
(u) Comissão de Comunicações da Nigéria.

[124] Disponível em https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/nigeria/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=fr_FR (Acedido aos 15-11-2019).

[125] Disponível em https://www.lexology.com/library/detail.aspx?g=f16ede4c-f04a-40a7-96c3-e6a4899f3cf0 (Acedido aos 15-11-2019) e http://nji.gov.ng/images/Workshop_Papers/2016/Refresher_Magistrates/s09.pdf (Acedido aos 15-11-2019)

[126] Por exemplo, nos dias 11 e 12 de Abril de 2019 teve lugar a 2ª Reunião do Fórum Cibercrime – o fórum dos Ministérios Públicos lusófonos, na Cidade da Praia. A Coordenação do Fórum foi assegurada pelo Gabinete Cibercrime da Procuradoria-Geral da República de Portugal. Dentre os objetivos do fórum sublinhamos o seguinte: "sensibilizar os Estados representados que ainda não aderiram à Convenção de Budapeste a fazê-lo". Disponível em http://cibercrime.ministeriopublico.pt/pagina/2a-reuniao-do-forum-cibercrime-praia-cabo-verde (Acedido aos 16-11-2019).
No início da realização desse fórum o Procurador-Geral da República de Cabo Verde anunciou a criação de uma unidade orgânica na Polícia Judiciária com responsabilidade para a investigação do fenómeno. Disponível em https://expressodasilhas.cv/pais/2019/04/11/pgr-quer-resposta-mais-efectiva-ao-cibercrime/63301 (Acedido aos 16-11-2019).

Esta lei define um conjunto de tipos penais e estabelece regras ao nível da recolha da prova digital, abarcando as partes substantiva e adjetiva bem como as disposições sobre a cooperação internacional relativas à cibercriminalidade.

A seguir faremos uma descrição sucinta da mesma.

Com cinco capítulos e 33 artigos, traz no primeiro os aspetos concernentes ao objeto e as definições.

Define no art.º 2º al. h) os "dados relativos ao assinante", algo que não acontece com as outras duas leis já analisadas.

As "disposições materiais penais" é o tema do segundo capítulo e os crimes ali previstos são os seguintes:

a) Falsidade informática (art.º 3º);
b) Dano relativo a programas informáticos ou outros dados informáticos (art.º 4º);
c) Sabotagem informática (art.º 5º);
d) Acesso ilícito (art.º 6º);
e) Intercessão ilícita (art.º 7º);
f) Utilização indevida de dispositivo (art.º 8º);
g) Pornografia infantil (art.º 9º); e
h) Pornografia de vingança (art.º 10º).

Este capítulo finaliza com a responsabilidade das pessoas coletivas e o tratamento dos bens recuperados.

Alguns crimes prevêem uma moldura penal abstrata muito elevada. A falsidade informática e a utilização indevida de dispositivos são punidos até 5 anos, os danos e a sabotagem informática até 10 anos. A intercessão ilícita tem a previsão mais branda, 3 anos acrescida de multa.

A pornografia infantil é igualmente punida de forma severa, dependendo da forma de ocorrência.

---

[127] Ratificou em 19/06/2018 e entrou em vigor em 01/10/2018.

[128] Angola seguiu com muita atenção todos os desenvolvimentos que antecederam a entrada em vigor desta lei.
A Agência Angola Press (ANGOP) comunicava em 25 de Novembro de 2016 a aprovação pela assembleia cabo-verdiana da lei do cibercrime. Disponível em https://www.angop.ao/angola/pt_pt/noticias/africa/2016/10/47/Cabo-Verde-Assembleia-aprova-lei-sobre-cyber-crime-recolha-provas-suporte-electronico,a67d4fa8-2dbc-47f9-bd63-270396e8c681.html (Acedido aos 16-11-2019).

Nos tipos penais o art.º 10º traz uma novidade e representa uma grande inovação legislativa: ***pornografia de vingança***[129]. Achamos que este crime tem uma punição muito suavizada (até 2 anos) em relação aos outros crimes, principalmente se tivermos em consideração aos danos morais e psicológicos que causa à vítima (muitas vezes irreversíveis). Por isso, seria recomendável o devido agravamento[130].

A parte processual tem tratamento no terceiro capítulo. Ali vemos que a lei do cibercrime é igualmente aplicável à intercessão de comunicações cometidas por meio de um sistema informático (art.º 20º) e em algumas situações de ações encobertas (art.º 21º).

O capítulo quatro retrata a cooperação internacional e, respeitando a solicitação da Convenção de Budapeste, o art.º 23º apresenta um ponto de contacto permanente, sendo para o efeito assegurado pela Procuradoria-Geral da República, podendo delegar competências à Polícia Judiciária, o que é bastante importante para a materialização do intercâmbio internacional.

O art.º 27º trata dos dados trans-fronteiriços.

O quinto e último capítulo das disposições finais e transitórias encerra esta lei.

Além desta lei, Cabo-verde tem "outro documento legal que vem conceder alguma proteção aos usuários das novas tecnologias informáticas e de comunicação e da Internet, é o Regime Jurídico Geral de Proteção de Dados Pessoais a Pessoas Singulares, aprovado pela Lei nº 133/V/2001, alterada pela Lei nº 41/VIII/2013[131], de 17 de Setembro"[132].

2.4. Comparação entre as convenções de Budapeste e Malabo

2.4.1. Antecedentes e âmbito

Confrontando a convenção europeia e a sua congénere africana, primeiramente devemos notar que ambas tiveram percursos completamente diferentes, senão vejamos.

---

[129] A pornografia de vingança (em inglês, *revenge porn*) é uma expressão que remete ao ato de expor publicamente, na Internet, fotos ou vídeos íntimos de terceiros, sem o consentimento dos mesmos, ainda que estes se tenham deixado filmar ou fotografar no âmbito privado. Isto geralmente ocorre após o fim de um relacionamento amoroso, quando um dos envolvidos divulga cenas íntimas do outro, como forma de "vingar-se" do antigo parceiro. Disponível em https://pt.wikipedia.org/wiki/Pornografia_de_vingança (Acedido aos 17-11-2019).
Depois da atualização de 2018, no Brasil a pornografia de vingança passou a punir-se no Código Penal (art.º 218º). Disponível em https://direitofamiliar.jusbrasil.com.br/artigos/597009198/pornografia-de-vinganca-o-que-e-isso (Acedido aos 17-11-2019).
Em Portugal esse delito é punido no âmbito da violência doméstica. Disponível em https://www.deco.proteste.pt/tecnologia/tablets-computadores/noticias/pornografia-de-vinganca-pode-dar-pena-de-prisao-ate-5-anos# (Acedido aos 17-11-2019).

[130] Portugal e Brasil atribuem a esse crime a pena máxima de 5 anos.

[131] Disponível em https://sniac.cv/wp-content/uploads/2018/03/SNIAC-Lei-n°-43-VIII-2013-Cria-e-Regula-SNIAC.pdf (Acedido aos 17-11-2019).

[132] Disponível em https://expressodasilhas.cv/eitec/2018/10/12/cibercrime-legislacao-evolui-mas-tecnologia-e-mais-rapida/60468 (Acedido aos 17-11-2019).

A Convenção do Conselho da Europa sobre a Criminalidade Informática, mais conhecida por Convenção de Budapeste, foi implementada nos finais de 2001, todavia foi antecedida de vários acontecimentos e instrumentos jurídicos[133] que influenciaram a sua concepção. Nestes destacam-se duas Recomendações:

a) N.º R (89)[134] 9 sobre a criminalidade informática que estabelece diretrizes para os legisladores nacionais respeitantes à definição de certos crimes informáticos; e

b) N.º R (95) 13 relativa a problemas processuais penais relacionados com as tecnologias da informação;

Notando os delitos que iam sendo cometidos por intermédio da rede mundial de computadores, o então Comité Europeu para os Problemas Criminais (CDPC), por via da Deliberação CPDC/103/211196 de Novembro de 1996, determinou a formação de um comité de especialistas para debaterem sobre essa problemática[135].

Outro facto que não deve ser ignorado, e que sucedeu dois meses antes da implementação da CB, foi o ataque terrorista da Al-Qaeda efetuado em 11 de Setembro de 2001, pois investigações feitas descobriram que os terroristas se comunicavam usando rascunhos de uma caixa de correio eletrónico. Deste modo, "sem que as mensagens fossem enviadas não houve como o serviço de inteligência do Pentágono efetivasse uma interceção"[136].

Por esses fatos, a CB "sugeriu a uniformização da legislação penal pelo mundo e os mecanismos e instrumentos de colaboração na luta contra a criminalidade no ambiente virtual"[137]. Ela foi concebida para ser um instrumento internacional, como se depreende do quarto e sétimo parágrafos do seu preâmbulo que assinalam o seguinte:

Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço,

---

[133] Para além das duas recomendações supra mencionadas outros diplomas legais relevantes foram as "Recomendações do Comité de Ministros N.º R (85) 10 relativa à aplicação prática da Convenção Europeia sobre Auxílio Judiciário Mútuo em Matéria Penal quanto às cartas rogatórias para a interceção de telecomunicações, N.º R (88) 2 sobre as medidas destinadas a combater a pirataria no domínio do direito de autor e dos direitos conexos, N.º R (87) 15 que regula a utilização de dados de carácter pessoal no sector da polícia, N.º R (95) 4 relativa à proteção dos dados de carácter pessoal no sector das telecomunicações, tendo em conta, designadamente os serviços telefónicos" como pode ler-se no preâmbulo.

[134] Esta recomendação já previa muitos crimes cuja designação foi mantida na Convenção de Budapeste. Disponível em http://www.oas.org/juridico/english/89-9&final%20Report.pdf (Acedido aos 17-11-2019).

[135] Trabalhos seguintes resultaram na Resolução n.º 1 adotada pelos Ministros Europeus da Justiça na sua 21ª Conferência (Praga, 10 e 11 de Junho de 1997) e na Resolução n.º 3, adotada na 23ª Conferência dos Ministros Europeus da Justiça (Londres, 8 e 9 de Junho de 2000).

[136] **BRITO**, Auriney. Direito Penal Informático. Editora Saraiva. 2013.

[137] Idem.

designadamente, através da adopção de legislação adequada e da melhoria da cooperação internacional (o sublinhado é nosso)*;*

Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate à cibercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias da informação (o sublinhado é nosso).

Nesta época notaram a necessidade da colaboração entre os países aderentes para o êxito do combate pretendido.

Já a lei africana é bem mais recente, surgiu 13 anos depois e visou somente assegurar a "Cibersegurança e a proteção de dados pessoais" nos estados-membros visando a construção de uma sociedade de informação no continente.

Não tem qualquer pretensão pluricontinental, não estando por isso aberta a ratificação por parte de países não pertencentes a União Africana. É puramente um tratado regional.

Foi influenciada pelos princípios apresentados pela Iniciativa da Sociedade de Informação Africana (ISIA) e do Plano de Ação Regional Africano para a Economia do Conhecimento (PAREC), aliás como já foi antes referido.

Duas declarações impeliram a sua proclamação, a Declaração de Abidjan de 22 de Fevereiro de 2012 e a Declaração de Adis Abeba de 22 de Junho do mesmo ano de 2012, que tratam da necessidade de harmonizar a legislação relativa a cibernética a nível de África.

As duas convenções distinguem-se no âmbito, a africana aporta-se na CB[138][139] inclusivamente muita da linguagem e designação utilizada é daí retirada. Porém, vai mais além, não tratando unicamente dos crimes mas também da proteção de dados pessoais.

2.4.2. Tipo de crimes informáticos previstos

[138] Apesar de não fazer qualquer menção à CB no preâmbulo nem no seu *corpus* tal se depreende da terminologia usada, na designação dos delitos e nos objetivos pretendidos.

[139] Num *Relatório do Debate Online Sobre a Convenção da União de África Sobre Cibersegurança* e enviado para a Comissão da UA, compilado por **Grace Githaiga** em Dezembro de 2013, dirigido pela *Rede de Ação de TIC do Quênia (KICTANet)*, destacaram-se as seguintes observações:
"Algumas das disposições parecem copiar e colar várias leis do primeiro mundo e, sim, em um contexto africano, algumas delas podem ser arriscadas". Mas reconhecem que "Os países africanos precisam da maioria delas para um quadro jurídico funcional para o cibercrime".
Notam que "Em certas seções, o texto é confuso e propenso a múltiplas interpretações" e que na verdade "Algumas das leis já existem nos países parceiros, mas existem mecanismos fracos de implementação". Por isso sugerem que "É necessário encontrar métodos para aplicá-las e educar as massas sobre seus direitos."
Ainda dão conta que "O maior desafio enfrentado pelos usuários é o desconhecimento da lei. A conscientização e a capacitação são necessárias para combater a ignorância".
Terminam referindo que "A Comissão da UA precisa urgentemente envolver-se com a indústria e a sociedade civil para encontrar e fornecer uma estrutura viável para a Convenção". Disponível em https://cipesa.org/?wpfb_dl=143 (Acedido aos 17-11-2019).

Ambas convenções também distinguem-se na tipologia criminal, embora haja alguma similitude.

Os crimes previstos na CB fazem parte de uma Secção intitulada *Direito Penal Material*. Posteriormente esses crimes são distinguidos em quatro títulos. O primeiro é o constante no Título 1 das *Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos*.

Os artigos e os referidos crimes aí previstos são os seguintes:

- Artigo 2º - Acesso ilegítimo
- Artigo 3º - Interceção ilegítima
- Artigo 4º - Interferência em dados
- Artigo 5º - Interferência em sistemas
- Artigo 6º - Uso abusivo de dispositivos

Depois temos no Título 2 as *Infrações relacionadas com computadores*, sendo:

- Artigo 7º - Falsidade informática
- Artigo 8º - Burla informática

No Título 3 aparecem aquelas *Infrações relacionadas com o conteúdo*, são elas:

- Artigo 9º - Infrações relacionadas com a pornografia infantil

Os ilícitos que preenchem todo o Título 4 são os referentes às *Infrações relacionadas com a violação do direito de autor e direitos conexos*.

- Artigo 10º - Infrações relacionadas com a violação do direito de autor e dos direitos conexos

Os artigos 11º e 12º previstos no Título 5 sobre as *Outras formas de Responsabilidade e Sanções* não são propriamente crimes, uma vez que devem ser enquadrados nos artigos antecedentes e tratam da *Tentativa e cumplicidade* bem como da *Responsabilidade de pessoas coletivas*.

Portanto, temos no total 9 crimes na CB.

Na convenção africana temos as Disposições Penais na Seção II. No seu art.º 29º relativo as *Ofensas Específicas Contra as Tecnologias de Informação e Comunicação* temos o seguinte:

- Ataques contra Sistemas Informáticos
- Violação de Dados Informatizados
- Infrações relativas ao conteúdo
- Infrações relativas às medidas de segurança das trocas comerciais eletrónicas

No art.º 30º[140] sob título *Adaptação de Algumas Infrações às Tecnologias de Informação e Comunicação,* surgem as:

- Ofensas Contra a Propriedade

Os crimes previstos na CM são apresentados de forma genérica e um tanto quanto abstrata, o que dificulta a sua discriminação.

Este normativo começa por tratar dos crimes que têm a ver com os ataques contra sistemas informáticos. Esses delitos podem suceder de várias maneiras mas na CM só conseguimos divisar o acesso ilegal, o dano informático, sabotagem informática e o uso abusivo ou indevido de dispositivos.

Nos crimes contra os dados informatizados achamos a interceção ilícita, a falsificação informática e a burla informática. Nos contra o conteúdo, para além da pornografia infantil, temos os que se referem à discriminação racial, ideológica, religiosa e outras.

De uma forma geral nos crimes contra a propriedade temos as fraudes nas transações informáticas e nestas incluem-se também a burla informática.

Dentre esses crimes a sabotagem informática e a burla informática destacam-se por apresentarem um tratamento pouco habitual como a seguir veremos com maior pormenor.

[140] Neste artigo fala-se também da *Responsabilidade penal das pessoas coletivas*.

2.4.3. Comparação dos tipos legais de crimes de ambas as convenções

Como já aludimos *supra*, a CM não discrimina explicitamente os ilícitos penais como sucede na CB em que a nomenclatura da infração surge na epígrafe dos respetivos artigos, todavia esses delitos podem ser subentendidos dentro do *corpus* dos artigos 29º e 30º que serão aqui confrontados com os crimes da CB estabelecidos do 2º ao 10º artigo.

O acesso ilícito do art.º 2º da CB tem correspondência com as alíneas a), b) e c) do nº 1 do art.º 29º da CM. Em ambos diplomas criminaliza-se a atuação que consiste em aceder ou manter-se na totalidade ou simplesmente em uma parte do sistema informático. Distinguem-se pelo facto da CB exigir intencionalidade na ação e não punir a tentativa, o que não acontece na CM. Além do mais, notamos que de uma forma geral, as infrações da CB pressupõem dolo, porém a CM deixa isso à consideração dos Estados aderentes.

A interceção ilícita do art.º 3º tem relação com a infração prevista na al. a) do nº 2 do art.º 29º, por termos nos dois cenários a punição da "intercepção não autorizada através de meios técnicos, de transmissão não públicas de dados informáticos"[141].

O crime de danos contra os dados informáticos é acolhido no art.º 3º da CB e nas al. e) e f) do nº 1 do art.º 29º. Prevêem penalizar a "danificação, o apagamento, a deterioração, a alteração, a supressão" ou a introdução desautorizada de dados informáticos, sendo que a CM determina que essas ações decorram todas de modo fraudulento.

Na CM o crime de sabotagem informática está prescrito na al. d) do nº 1 do art.º 29º e coincide parcialmente com o art.º 5º da CB, nos termos do qual criminaliza-se "quem dificultar ou distorcer o funcionamento do sistema informático", contudo o normativo africano não esclarece efetivamente que outras ações preenchem esse ilícito nem exige que o regular funcionamento do sistema seja perturbado de forma grave. Nessa ordem de ideias, a CB é muito mais esclarecedora, impondo que essas ações decorram "mediante inserção, transmissão, danificação, eliminação, deterioração ou supressão de dados informáticos".

O uso abusivo ou indevido de dispositivos do art.º 6º da CB, na CM afere-se no art.º 29º nº 1 al. h), nos termos dos quais considera-se como infração penal a "produção, venda, importação, disseminação, posse, oferta, cedência ou oferta de equipamento, um programa informático, qualquer dispositivo ou dado concebido ou adaptado especialmente para cometer

[141] A CB inclui na sua estatuição as "radiações eletromagnéticas emitidas por um sistema informático".

infrações", nessas incluem-se as *passwords*, os códigos de acesso ou dados equivalentes e que possibilitem alcançar na totalidade ou em uma parte do sistema informático.

Ambas previsões do acesso indevido de dispositivos corroboram ainda na não responsabilização criminal das ações nelas expostas quando decorrerem mediante testes devidamente autorizados e visarem a melhoria da proteção do próprio sistema informático. Ademais, a CM excede ao enunciado da CB exigindo que os vendedores de produtos ligados às TICs recorram a pesquisadores autónomos ou a peritos em cibersegurança no sentido destes realizarem "ensaios de vulnerabilidade e avaliações da garantia de segurança", impondo ainda que se façam comunicações aos consumidores sobre as eventuais falhas detetadas e os meios aconselháveis para que a respetiva correção se processe (art.º 29º nº 1 al. g)).

A falsificação informática prenunciada no art.º 7º da CB tem a sua correspondente no art.º 29º nº 2 al. b) da CM. Nos dois casos temos um tratamento análogo, abrangendo este ilícito as ações intencionais de "introdução, apagamento ou supressão de dados informáticos" desde que destes se obtenham outros dados não originais, com o intento de que sejam tidos ou usados para fins juridicamente relevantes como se fossem autênticos. Os dois artigos coincidem ainda na possibilidade dos estados-membros exigirem que exista uma intenção fraudulenta ou criminosa para que se efetive a responsabilização criminal.

A al. c) do art.º 29º da CM prevê a punição do uso de dados obtidos fraudulentamente de um sistema informático desde que o usuário tenha conhecimento da origem ilícita dos mesmos.

Distintamente da falsidade informática, no caso da burla informática já não vislumbramos tantas semelhanças. No art.º 9º da CB pressupõe-se que esta acarrete um "prejuízo patrimonial" a pessoa lesada, ou seja, a intenção do infrator é a de obter para si ou para outrem "um benefício económico". Por outro lado, a al. d) do nº 2 do art.º 29º da CM apesar de dispor que a ação decorra de forma fraudulenta, advoga apenas que a intenção do infrator seja a obtenção de qualquer benefício, podendo este ser económico ou não. Assim, o texto correspondente à burla informática da CM não remete necessariamente para a diminuição do património do ofendido.

Notemos que existe alguma doutrina que tem sobre a burla informática um entendimento semelhante ao constante no CM, considerando que "esta norma incriminadora embora prescreva a intenção de enriquecimento ilegítimo, não exige a verificação de um efetivo

enriquecimento para a consumação do crime, ... é, por isso, um crime de resultado parcial ou cortado"[142].

A nível da jurisprudência portuguesa também tem surgido algum entendimento similar ao acolhido pela CM. Por exemplo, o Acórdão do Tribunal da Relação de Évora de 20 de Janeiro de 2015 é categórico ao aludir que "no crime de burla informática está em causa não só o património, ou seja, a integridade patrimonial, mas também a fiabilidade dos dados e a sua proteção, tendo em linha de conta o específico *modus operandi* do sistema informático"[143].

Antes de confrontarmos os crimes relacionados com os conteúdos, temos duas situações delituosas previstas na CM que não têm similaridade na CB. São os casos das alíneas e) e f) do nº 2 do art.º 29º nos quais pede-se aos estados-partes a responsabilização penal de quem:

- Por negligência, processar ou mandar processar dados pessoais sem respeitar as formalidades prévias do processamento;
- Participar em uma associação formada ou num acordo estabelecido com vista a preparar ou cometer uma ou várias ofensas previstas na presente Convenção.

O primeiro caso diz respeito às infrações relacionadas com o tratamento de dados pessoais, o segundo reporta os delitos ora mencionados quando cometidos na esfera da criminalidade organizada.

Os delitos relacionados à pornografia infantil[144], do art.º 9º da CB, na CM encontram-se regulados nas al. a), b), c) e d) do nº 3 ponto 1 do art.º 29º. A convenção africana seguiu praticamente o mesmo texto da CB ao estabelecer a punição de quem por intermédio de um sistema informático "produzir, registar, oferecer, fabricar, disponibilizar, difundir, transmitir uma imagem ou representação de pornografia infantil".

---

[142] **CORREIA**, Pedro Miguel Alves Ribeiro & **JESUS**, Inês Oliveira Andrade de. Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas. Artigo Científico. Recebido: 10 de Março de 2015; Aceito: 04 de Abril de 2016. Online Version ISSN 2317-6172. Rev. Direito GV vol. 12 no. 2 São Paulo May/Aug. 2016. Disponível em https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322016000200542 (Acedido aos 21-07-2020).

[143] Acórdão do Tribunal da Relação de Évora de 20-01-2015. Proc. 90/11.0GCLLE.E1 em que foi relator João Amaro. Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/737b074e63612dc880257de100582533?OpenDocument (Acedido aos 21-07-2020).

[144] Dada a importância da temática, a definição de pornografia infantil é a primeira configurada no art.º 1º da CM. O seu texto vai de encontro a definição constante no nº 2 do art.º 9º da CB.

Ambos os textos incriminam também a aquisição para si ou para outrem de conteúdos ligados à pornografia infantil, a simples posse de tal material bem como a facilitação de acesso a imagens, documentos, sons e representação de pornografia envolvendo um menor[145] de idade.

Merecedor de referência é a previsão entre as infrações relacionadas com os conteúdos de crimes de ódio, tais como a xenofobia, o racismo, as distintas formas de discriminação, a apologia ao genocídio e a crimes contra a humanidade, quando praticados por via de sistemas informáticos. Estes estão estatuídos nas alíneas e), f), g), e h) do nº 3 ponto 1 da CM. Neste aspeto, achamos que a CM procurou acolher de forma sintetizada o Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adotado em Estrasburgo em 28 de Janeiro de 2003[146].

As outras infrações que reportam a violação dos direitos de autor e dos direitos conexos não têm acolhimento algum por parte da CM, porém na CB encontram-se plasmadas no art.º 10º.

Portanto, a CB é mais específica, contrariamente a CM é generalista[147] tendo um vasto escopo e dando uma maior liberdade aos estados-membros na determinação da tipologia criminal no momento de elaborar a sua lei nacional.

2.4.4. Países africanos que aderiram

A convenção africana foi adotada em 27 de Junho de 2014 e está disponível a assinatura e a adesão ou ratificação. A assinatura não implica necessariamente a implementação da convenção na esfera nacional, é apenas uma manifestação de boa vontade[148].

---

[145] As convenções apontam como sendo menor alguém que tenha uma idade inferior aos dezoito anos, mas a lei africana não dá a possibilidade aos estados de poderem adotar a menoridade fixada abaixo dos dezasseis anos como acontece com a parte final do nº 3 do art.º 9º da CB.
No texto original da CM define-se criança ou menor da seguinte forma:

- ***Child*** *or* ***minor*** *means every human being below the age of eighteen (18) years in terms of the African Charter on the Rights and Welfare of the Child and the United Nations Convention on the Rights of the Child respectively* (1ª article).

[146] Disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1481&tabela=leis&ficha=1&pagina=1 (Acedidos aos 07-02-2020).
[147] **Matteo Lucchetti**, estudioso das questões regulamentares da criminalidade informática, é da mesma opinião e afirma que "a convenção da União Africana é mais abrangente que a Convenção de Budapeste uma vez que ela cobre:

- Capítulo I – Transações Eletrónicas
- Capítulo II – Proteção de dados pessoais
- Capítulo III – Cibersegurança e cibercrime"

Antes destes capítulos a CM traz no art.º 1º uma vasta gama de definições das principais terminologias aí utilizadas.
Lucchetti continua dizendo que "A convenção da União Africana unifica diferentes aspetos relacionados com a lei de tecnologia da informação, também inclui questões não-digitais nem ligadas à justiça criminal". **LUCCHETTI**, Matteo. Cybercrime legislation in Africa: Regional and international standards. AUC HQ, Addis Abeba, 12 Abril de 2018, p. 8.

A lista dos países assinantes e aderentes[149] ainda não é satisfatória porque não atingiu sequer metade dos países do continente.

No ano da sua feitura, a convenção não teve nenhuma assinatura nem ratificação. Mas em 2015 foram assinando sucessivamente os seguintes países: Benim, Guiné-Bissau, Mauritânia, Chade e República do Congo. Infelizmente a Guiné-Bissau ficou por esta manifestação de intenção, não dando até agora nenhum passo significativo.

Curiosamente em 29 de Janeiro 2016 assinaram ao mesmo tempo a Serra Leoa, São Tomé[150] e a Zâmbia.

Em 2017 apenas o Gana a assinou. Em 2018 fizeram-no os Camarões e Moçambique.

Ano seguinte foram assinando Togo, Ruanda e Tunísia, respetivamente.

Somente cinco países ratificaram este diploma legal da União Africana: primeiro foi o Senegal em 2016, dois anos depois a Guiné Conacri e as Ilhas Maurícias. Em 2019 a Namíbia e o Gana.

É uma situação deveras preocupante. África tem 55 países, 54 membros da União Africana, contudo 14 países assinaram a convenção e 5 a ratificaram.

Apesar de reconhecermos as dificuldades que a maioria desses países apresenta, muitas das quais já por nós retratadas, e de sabermos que a ratificação pode implicar alterações no ordenamento jurídico interno, essa baixa percentagem afigura-se exagerada.

Basta vermos que a convenção foi adotada em Adis Abeba, na Etiópia, mas esse país que albergou o ato nem sequer se dignou pelo menos a assiná-la.

Apesar dessa fraca adesão devemos reconhecer que a adoção da Convenção de Segurança Cibernética da União Africana (doravante UA) representa um marco significativo na governança africana de segurança cibernética e ressalta os esforços do continente para promover o desenvolvimento de uma sociedade da informação segura.

---

[148]... a **assinatura** significa a intenção de um Estado em implementar o conteúdo do Tratado, enquanto a **ratificação** significa que o Estado tem leis que o obrigam a seguir o que foi colocado no Tratado. Disponível em https://16minionuapmbc2024.wordpress.com/2015/09/01/assinarratificar-faz-tanta-diferenca-assim/ (Acedido aos 17-11-2019).

[149] A lista completa de todos os países pode ser encontrada em https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (Acedido aos 17-11-2019).

[150] São Tomé aprovou em 6 de Outubro de 2017 a Lei nº 15/2017 designada Lei Sobre o Cibercrime. Muito semelhante a lei cabo-verdiana, tem cinco capítulos, dispostos com as seguintes matérias:

1. Objeto e definições
2. Disposições penais materiais
3. Disposições processuais
4. Cooperação internacional
5. Disposições finais e transitórias

Está disponível em http://cipstp.st/wp-content/uploads/2018/03/Lei_15_2017-Lei-sobre-Cibercrime.pdf (Acedido aos 17-11-2019).

No entanto, nos seus moldes atuais, há quem acha que "a Convenção não oferece esperança para uma ampla cooperação internacional entre todos os Estados da UA"[151]. E aconselham UA a tomar medidas no sentido de "impedir a limitação ou fragmentação da cooperação em cibersegurança de África"[152], ficando unicamente para acordos bilaterais ou para acordos sub-regionais (CEDEAO, SADC).

2.4.5. Posição de Angola

Depois da instituição da convenção africana, a posição inicial de Angola foi de não assinar nem ratificar esse instrumento jurídico.

Tal posição primordial compreende-se claramente, pois que a convenção surgiu num momento em que Angola começava a empenhar-se em fazer uma vasta reforma legislativa.

Com as eleições de 2017 e assunção de um novo Titular do Poder Executivo, muitos projetos então existentes começaram a ser reequacionados e reavaliados, o que retardou a implementação de alguns projetos ora iniciados.

Na exposição dos motivos desse atraso não podemos nos esquecer da crise económica e financeira que atingiu principalmente os países exportadores de petróleo – dos quais Angola[153] faz parte – o que implicou constantes revisões aos Orçamentos Gerais do Estado e o adiamento ou mesmo a cessação de certos planos.

Mesmo assim estas reformas estão ocorrendo e abrangem a legislação penal[154].

De acordo com o ACP de Angola, os crimes informáticos serão inseridos no futuro CP de forma dispersa e não numa lei avulsa como acontece por exemplo em Portugal[155], Cabo Verde[156] e São Tomé[157].

---

[151] **ORJI**, Uchenna Jerome. Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation? 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, p. 116. Constante em https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdf (Acedido aos 17-11-2019).

[152] Ibdem p. 117.

[153] Rita Atalaia do Sapo Notícias, em 22 Agosto 2017 considerou "a queda do petróleo tramou a economia angolana." Disponível em https://eco.sapo.pt/2017/08/22/como-a-queda-do-petroleo-tramou-a-economia-angolana/ (Acedido aos 17-11-2019).

[154] Pode ler-se no Diário Notícias de 14 de Março de 2019 que "*O Presidente angolano destacou hoje a aprovação do novo Código Penal do país, em substituição do secular diploma de 1886, por considerar um "momento histórico que marcou a justiça angolana"."* Disponível em *https://www.dn.pt/lusa/aprovacao-do-novo-codigo-penal-angolano-foi-momento-historico--presidente-10680112.html* (Acedido aos 18-11-2019).

[155] Lei n.º 109/2009 de 15 de Setembro, Lei do Cibercrime. Disponível emhttp://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis (Acedido aos 18-11-2019).

[156] Lei nº 8/IX/2017 de 20 de Março, Lei do Cibercrime. Disponível emhttp://www.cnpd.cv/leis/Lei%20de%20Cibercrime.pdf (Acedido aos 18-11-2019).

[157] Lei n.º 15/2017 06 de Outubro de 2017, Lei sobre Cibercrime. Disponível em http://cipstp.st/wp-content/uploads/2018/03/Lei_15_2017-Lei-sobre-Cibercrime.pdf (Acedido aos 18-11-2019).

Outro aspeto que não deve ser esquecido é o que tem que ver com a abrangência da convenção africana.

Não basta que Angola faça avanços no domínio da criminalidade digital e da cibersegurança. É preciso também progredir no tocante ao tratamento de dados pessoais.

A parte que se prende com a cibersegurança e a proteção de dados teve um avanço significativo com a aprovação e publicação em Diário da República no dia 16 de Fevereiro de 2017 da Lei n.º 7/17[158], designada Lei da Protecção das Redes e Sistemas Informáticos (doravante LPRSI), que veio impor uma série de obrigações novas a diversas entidades que atuam em Angola.

Com base nessa lei "As empresas de comunicações electrónicas, os prestadores de serviços da sociedade da informação, os prestadores de armazenagem principal e prestadores de serviços de infraestruturas críticas (como sejam as entidades que são responsáveis pelas cadeias de abastecimento, saúde, segurança e as utilities) e bem assim entidades que desempenhem funções sociais críticas (*e.g.*, empresas que actuem nos sectores financeiros, transportes, Oil & Gas), passaram a estar sujeita a obrigações de protecção e segurança das informações e dos seus sistemas informáticos; de conservação de dados; de retenção de dados para fins de investigação; de cooperação com autoridades competentes e intercepção de comunicações"[159].

Tudo isto representa uma grande "evolução do Direito Tecnológico Angolano"[160] e este diploma legal permite o estabelecimento de uma estreita cooperação entre a "Agência Nacional de Protecção de Dados (ANPD)[161][162] e o Instituto Nacional das Comunicações (INACOM)"[163].

---

[158] Disponível em https://animalexdominis.files.wordpress.com/2018/03/proteccc3a7c3a3o-das-redesesistemas-informc3a1ticos-2017.pdf (Acedido aos 18-11-2019).

[159] Disponível em https://www.vda.pt/xms/files/v1/O_QUE_FAZEMOS/NEWSLETTERS_E_FLASHES/Flash_informativo_Lei_Protecao_das_Redes_e_Sistemas_Informatico__Angola__PT.pdf.PDF (Acedido aos 18-11-2019).

[160] Disponível em http://www.avm.biz/conteudo/pt/1268/aprovacao-da-lei-de-proteccao-das-redes-e-sistemas-informaticos/ (Acedido aos 18-11-2019).

[161] Tal como informou a Lusa, a sua administração entrou em funcionamento em 19 de Outubro de 2019 e na sua tomada de posse a presidente do conselho de administração da ANPD, **Maria das Dores Jesus Correia Pinto** admitiu a existência de desvio de dados pessoais em instituições públicas e privadas e por isso deve-se "correr atrás do prejuízo" para fiscalizar e controlar o tratamento de dados. Mais tarde continuou dizendo que a agência vai "fiscalizar e controlar" o tratamento que as entidades públicas e privadas dão aos dados pessoas: "Vamos controlar o tratamento de dados pessoais, por exemplo, nos bancos, hospitais, clínicas".

A posse foi conferida pelo ministro das Telecomunicações e Tecnologias de Informação angolano, José Carvalho da Rocha. O conselho de administração da ANPD é composto por um presidente, dois administradores executivos e quatro administradores não executivos.

Essa entidade também visa "Sancionar o incumprimento da Lei de Proteção de Dados, promover a implementação dos códigos de conduta no âmbito da proteção de dados pessoais, apreciar e pronunciar-se sobre a transferência internacional de dados pessoais são algumas das atribuições da ANPD". Disponível em https://www.plataformamedia.com/pt-pt/noticias/sociedade/agencia-de-protecao-de-dados-admite-uso-indevido-de-dados-pessoais-em-instituicoes–11385102.html (Acedido aos 18-11-2019).

Tal como a própria denominação sugere, o diploma veio para regular o regime de salvaguarda do ciberespaço da República de Angola, pela feitura de um enquadramento punitivo das ações de roubo informático, ciberataques e outros incidentes informáticos.

Surpreendentemente no dia 3 de Março de 2020 a República de Angola aprovou para ratificação a convenção africana sobre a cibersegurança e proteção de dados por intermédio da Carta de Ratificação n.º 1/20 que é parte integrante do Diário da República – Iª Série n.º 23.

Surpreendeu-nos bastante porque apesar de estar em vigor a LPRSI, o tão esperado Código Penal "puramente" angolano ainda não foi aprovado, nestes termos notamos que, pelo menos legalmente, as condições para aprovação ou ratificação da convenção africana ainda não estão preenchidas.

Portanto, se bem que *grosso modo* o plano normativo é motivador, achamos essa "aprovação para ratificação" um pouco apressada visto que em diversos aspetos Angola tem ainda um longo caminho a percorrer. Todavia, considerando que *improbus omnia vincit*[164], basta que haja trabalho para que os objetivos sejam concretizados.

---

[162] Em 26 de Outubro de 2019 o *site* e-Global Notícias em Português já havia noticiado que o Secretário de Estado das Telecomunicações de Angola Mariano de Oliveira, informara um dia antes num encontro das Plataformas das Entidades Reguladoras das Comunicações Social dos Países de Língua Portuguesa (PEC) da entrada em vigor da ANPD. Disponível em https://e-global.pt/noticias/lusofonia/angola/angola-agencia-nacional-de-proteccao-de-dados-vai-funcionar-em-breve-no-pais/ (Acedido aos 18-11-2019).
Ainda pode consultar-se http://www.angonoticias.com/Artigos/item/59445/governo-prepara-lei-para-combater-noticias-falsas (Acedido aos 18-11-2019) e Decreto Presidencial n.º 277/19 (Presidente da República) 06/09/2019 que nomeia o Conselho de Administração da ANPD, em https://www.lexlink.eu/conteudo/geral/ia-serie/3908112/decreto-presidencial-no-27719/14793/por-tipo-de-documentolegal (Acedido aos 18-11-2019).

[163] Ibdem.

[164] O trabalho vence tudo ou o trabalho recompensa (provérbio latino).

Capítulo III – OS CRIMES INFORMÁTICOS NO ANTEPROJETO DE CÓDIGO PENAL ANGOLANO

3.1. Breve reflexão sobre o Anteprojeto de Lei de Combate à Criminalidade no Domínio das TICs e dos Serviços da Sociedade da Informação

A primeira manifestação expressiva de intenção em implementar em Angola uma lei que regule e puna a criminalidade informática aconteceu em 2011 quando o Ministério das Telecomunicações e Tecnologias de Informação apresentou a Versão Final do anteprojeto de *Lei de Combate à Criminalidade no Domínio das Tecnologias de Informação e Comunicação e dos Serviços da Sociedade da Informação*[165].

Este anteprojeto de 79 artigos estruturados em 5 capítulos foi publicado na página oficial do ministério acima referido em 29 de Dezembro de 2011. Entretanto não teve prosseguimento, mas antes de apresentarmos algumas razões que impossibilitaram a sua prossecução estudemos o seu conteúdo.

O Capítulo I é devotado às Disposições Gerais. No art.º 1º da parte referente ao *Objeto* patenteia que

> **"A presente lei estabelece as disposições penais, substantivas e adjetivas, relativas ao domínio da criminalidade no âmbito das tecnologias e da sociedade da informação e da recolha da prova em suporte eletrónico".**

Depreende-se que a lei não visava apenas a apresentação dos crimes informáticos, mas também tudo que envolvesse a instrução e o prosseguimento processual dos mesmos, tendo desta feita um espaçoso abrangimento.

A segunda parte do art.º 1º que trata do *Âmbito de Aplicação* diz no nº 1 que a lei se aplica a factos que

> **a) Sejam cometidos por cidadão angolano ou pessoa colectiva de direito angolano com domicílio em território angolano;**

[165] Disponível em http://www.mtti.gov.ao/VerLegislacao.aspx?id=456 (Acedido aos 18-11-2019).

b) Sejam fisicamente praticados, total ou parcialmente, em território angolano, ainda que visem sistemas de informação ou dados localizados fora desse território; ou

c) Visem sistemas de informação ou dados localizados em território angolano, independentemente do local onde esses factos forem fisicamente praticados.

O art.º 3º faz um esclarecimento mais aprofundado dos moldes em que a responsabilização criminal das pessoas coletivas e equiparadas é processada[166].

As definições constam do art.º 4º numa vastíssima lista[167]. Nelas é notória a introdução de terminologias geralmente não definidas em outras legislações semelhantes, como são os casos dos conteúdos discriminatórios, o IMEI ("International Mobile Equipment Identity") e o IMSI ("International Mobile Subcriber Identity") das alíneas h), s) e t) respetivamente.

Contudo, a preocupação do legislador em apresentar, quase que exaustivamente, as definições ligadas às TICs compreende-se por ter sido o primeiro anteprojeto de lei sobre a criminalidade informática e por isso trazia termos que não eram, pelo menos, do domínio da maioria dos juristas angolanos.

Encontramos igualmente a definição de expressões comuns do Direito Penal não cibernético, são os casos de *organização terrorista* e de *organização criminosa* das alíneas bb) e cc).

O Direito Penal, o Direito Processual Penal e as suas respetivas leis complementares são aplicados a título subsidiário (art.º 5º).

O Capítulo II foi reservado aos delitos. Na Secção I temos os crimes praticados contra os sistemas de informação que são:

I. Acesso ilegítimo (art.º 6º)
II. Intercepção[168] ilegítima (art.º 7º)
III. Sabotagem informática (art.º 8º)
IV. Burla informática e nas comunicações (art.º 9º)

[166] Este artigo julgamos ter sido muito bem elaborado e em vários aspetos corrobora com a estatuição dos art.º 12º da CB e 8º da DQ 2005/222/JAI do conselho de 24 de Fevereiro de 2005 relativa a ataques contra os sistemas de informação que também retratam a responsabilização criminal das pessoas coletivas. Para mais informações sobre essa temática consulte-se **VENÂNCIO**, Pedro Dias. Lei do Cibercrime, op. cit., p. 84-86.

[167] Da alínea a) até a uu).

[168] Estes termos estão escritos tal como se apresentam nesse anteprojeto, relembrando que Angola ainda não adotou o Acordo Ortográfico que vigora noutros países lusófonos.

Seguem-se as infrações praticadas contra os dados da Secção II, são elas:

V. Falsidade informática (art.º 10º)
VI. Danos relativos a dados (art.º 11º)

A Secção III traz os crimes perpetrados por intermédio de sistemas de informação, sendo:

VII. Pornografia infantil (art.º 12º)
VIII. Fraude, assédio e exibicionismo sexual (art.º 13º)
IX. Ameaça e coação (art.º 14º)[169]
X. Difamação, injúria e calúnia (art.º 15º)
XI. Gravações, fotografias e filmes ilícitos (art.º 16º)
XII. Mensagens electrónicas (art.º 17º)[170]
XIII. Atentado contra a segurança de serviços de utilidade pública (art.º 18º)
XIV. Instigação e apologia pública ao crime (art.º 19º)
XV. Representação de violência (art.º 20º)
XVI. Incitamento à discriminação (art.º 21º)
XVII. Incitamento ao ódio e apologia da guerra (art.º 22º)
XVIII. Terrorismo (art.º 23º)
XIX. Espionagem (art.º 24º)

A Secção IV traz outros crimes relacionados com os sistemas de informação que a seguir expomos:

XX. Tutela penal dos programas de computador (art.º 25º)
XXI. Tutela penal das topografias dos produtos semicondutores (art.º 26º)
XXII. Tutela penal das bases de dados (art.º 27º)
XXIII. Neutralização de medidas eficazes de caráter tecnológico (art.º 28º)

[169] Praticado através de sistema de informação, aliás o mesmo sucederá com os demais crimes.
[170] Essa designação parece-nos muito vaga, aliás a expressão "mensagens electrónicas" não nos remete de antemão a um crime. Achamos que era bom que fosse completada ou enunciada doutra forma, por exemplo "perturbação moral ou psicológica por via de mensagem eletrónica".

XXIV. Informação para a gestão electrónica de direitos (art.º 29º)

Este segundo capítulo termina com a Secção V que aborda os dispositivos ilícitos e códigos de acesso, contendo unicamente o art.º 30º.

No nosso humilde ver o legislador foi bastante inclusivo, trazendo em consideração ilícitos que deveriam ser unicamente tratados no domínio do Direito Penal e não em uma lei do género. Caso esse diploma seja reconsiderado no futuro recomendaríamos a supressão de alguns ilícitos.

O Capítulo III encontra-se subdividido em 3 Secções, que descrevem os tipos de penas a serem infligidas às pessoas que cometam cada um dos delitos.

O art.º 31º relativo a Secção I da disposição geral afirma que as medidas de segurança do Código Penal são aqui, com as devidas especificidades, aplicadas.

Temos na Secção II as principais penas aplicáveis às pessoas singulares e às coletivas (art.º 32º e 33º). Para as primeiras aplicam-se penas de prisão e multa, para as segundas aplica-se pena de multa e de dissolução[171].

Na Secção III estão expostas as penas acessórias. Para as pessoas particulares estão previstas a perda de bens, a proibição do exercício de funções e a suspensão do exercício de funções (art.º 40º). Para as pessoas coletivas temos no art.º 41º:

a) Perda de bens;
b) Injunção judiciária;
c) Interdição do exercício de atividade;
d) Proibição de celebrar certos contratos ou contratos com determinadas entidades;
e) Privação do direito a subsídios, subvenções ou incentivos;
f) Encerramento de estabelecimento;
g) Publicidade da decisão condenatória.

Essas penas são retratadas do art.º 42º ao 51º.

Os meios de prova e as formas da sua obtenção é o assunto do Capítulo IV que está subdividido em 6 Secções. Na Secção I, o art.º 52º diz que os meios referenciados no CPP são

[171] A admoestação é outra pena prevista (art.º 34º). A lei prevê também a medida de vigilância judicial (art.º 36º).

aqui também aplicados. A Secção II diz respeito a preservação dos dados, a III relata sobre a sua transmissão.

Seguem-se: a busca e apreensão de dados; a intercepção das comunicações; a destruição dos dados; as regras específicas aplicáveis a operadores de comunicações electrónicas acessíveis ao público e a prestadores de armazenagem e; a preservação da soberania e integridade nacional, segurança do estado e ordem pública, nas Secções IV, V, VI, VII e VIII respetivamente.

Este anteprojeto de lei encerra com o Capítulo V concernente às disposições finais, onde estão previstas a regulamentação da lei, as dúvidas e omissões, a revogação e a entrada em vigor.

Falando agora propriamente das causas da sua não aprovação, sucedeu que em 24 de Maio de 2011 o anteprojeto foi levado ao parlamento, porém a requerimento do executivo foi retirado da ordem de serviço da sessão plenária.

Depois de ter sido muito debatido na generalidade, o executivo justificou a retirada da ordem de serviço pela "necessidade de harmonizar a lei em referência com o Código Penal"[172] cuja pretensão de revisá-lo já era na altura notória.

Essa necessidade de harmonização surgiu da análise feita ao documento pelos representantes do Sindicato dos Jornalistas Angolanos. Estes afirmaram que o diploma colocava "seriamente em causa o livre exercício da liberdade de expressão, de imprensa e o acesso à informação"[173].

O Sindicato dos Jornalistas declarou que o anteprojeto entrava em "contradição com a Declaração dos Direitos Humanos e o Pacto Internacional dos Direitos Civis e Políticos ratificados pelo Estado angolano e também consagrados na Constituição"[174].

Os únicos diplomas que na altura foram aprovados na especialidade são as propostas de Lei-Quadro das Comunicações Electrónicas e dos Serviços da Sociedade de Informação[175] e de Lei da Protecção de Dados Pessoais[176].

---

[172] Noticiado pelo Jornal de Angola de 26 de Maio, 2011 por Bernardino Manje. Disponível em http://jornaldeangola.sapo.ao/politica/lei_contra_a_criminalidade_informatica_aguarda_revisao_do_actual_codigo_penal (Acedido aos 19-11-2019).

[173] Ibdem.

[174] Art.°s 12° e 13° da CRA.

[175] Resultou na aprovação da Lei n° 23/11 de 20 de Junho das Comunicações Electrónicas e dos Serviços da Sociedade de Informação. Disponível em https://www.inacom.gov.ao/fotos/frontend_6/editor2/lei_23_de_2011-20_de_junho_de_2011.pdf (Acedido aos 31-08-2020).

[176] Proposta que culminou na aprovação da Lei n° 22/11 de 17 de Junho da Protecção de Dados Pessoais. Disponível em https://media2.mofo.com/documents/Law_22_11_Data_Privacy_Law.pdf (Acedido aos 31-08-2020).

Por isso, ficou acordado que a aprovação da Lei contra a criminalidade informática ficaria a aguardar a revisão do atual Código Penal cujo anteprojeto será estudado no sub-tema a seguir.

Portanto, apesar de alguns aspetos que a nosso ver mereciam alguma alteração ou enriquecimento, achamos que esta lei tinha realmente uma elaboração digna de realce e, embora tenha sido redigida há quase dez anos atrás, o seu conteúdo permanece atual e responde aos requisitos básicos a que se propunha, sendo bastante útil tê-la como referência para as vindouras leis criminais relacionadas às TICs.

3.2. Definição e delimitação dos tipos legais

Tal como já mencionamos anteriormente, a legislação angolana prevê o tratamento da criminalidade informática dentro do próprio Código Penal, não adotando uma lei avulsa unicamente destinada para o efeito, tal como acontece por exemplo em Portugal, no Brasil, em Cabo-Verde e em São Tomé.

Sobre o tema em questão importa frisar que dentro do ACP só estão estabelecidas algumas disposições materiais. Quanto aos aspetos processuais, estes continuam em falta, pelo que a regulação dos mesmos afigura-se premente e recomendável[177].

Na verdade, o progresso tecnológico é galopante e surgem sempre novas feições de manipulação informática. Por este facto, um crime informático estando sujeito a uma "constante e aceleradíssima mutação tecnológica, melhor ficaria numa lei avulsa do que num Código, que deve, por definição, ser poupado a revisões frequentes"[178].

No anteprojeto, que continua aguardando aprovação, esses delitos são referenciados nos art.ºs 184º, 212º, 213º, 235º, 399º e 407º.

As definições de alguns entes informáticos estão configuradas no art.º 233º do Capítulo I relativo a Falsificação de Documentos, Dados Informáticos e Registos Técnicos, fazendo parte do Título III dos Crimes Contra a Fé Pública, sendo respetivamente:

---

[177] Em Angola o parlamento aprovou recentemente (22-07-2020) por unanimidade o Código de Processo Penal (a proposta desse normativo pode ser encontrada em http://www.parlamento.ao/documents/480657/559079/PROPOSTA+DE+LEI+CPP.pdf (Acedido aos 02-09-2020) que, depois da promulgação que ainda se aguarda, substituirá o anterior CPP que vigora desde o remoto ano de 1929. Disponível em http://m.portalangop.co.ao/angola/pt_pt/noticias/politica/2020/6/30/Angola-independente-tem-primeiro-Codigo-Processo-Penal,c4967838-c869-4d72-863b-1e2c4442974b.html (Acedido aos 02-09-2020). Mas nesse diploma pouco conseguimos divisar sobre a produção da prova digital, nele apenas faz-se referência às escutas telefónicas no Capítulo V (art.º 241º a 247º), pelo que os aspetos processuais atinentes aos delitos cibernéticos continuam por se legislar.

[178] Extrato do pronunciamento de José A. Barreiros quando criticou a inserção da burla informática no Código Penal de 1982. **RODRIGUES**, Benjamim Silva, idem, p. 462.

a) "**Documento**"

b) "**Sistema informático**"

c) "**Dado informático**"

d) "**Registo técnico**"

No total são quatro definições, o que mostra que o legislador procurou ser muito telegráfico, definindo unicamente as expressões que achou de maior relevância, não trazendo novas terminologias nem alterando aquelas habitualmente usadas.

Essa postura lacónica do legislador, que dispensa algumas definições, pode também ser explicada pela existência de uma larga lista de expressões já definidas nas alíneas a) até a kk) do art.º 4º da Lei de Protecção das Redes e Sistemas Informáticos[179] (LPRSI).

As definições constantes na LPRSI consideramos serem suficientes e não entram em contradição com as apresentadas no ACP[180].

Assim, no âmbito da análise dos crimes informáticos seguiremos a estruturação apresentada na CB e estudaremos sucessivamente os Crimes Contra a Confidencialidade, Integridade e Disponibilidade de Sistemas Informáticos e Dados Informáticos; os Crimes relacionados com Computadores e por fim os Crimes Relacionados com o Conteúdo. Apesar de não ser a sequência adotada no ACP[181], julgamos ser uma opção que melhor viabiliza a investigação que desejamos efetuar. No entanto, é importante mencionar que o ACP não faz qualquer alusão aos crimes relacionados com a violação dos direitos de autor e direitos conexos.

---

[179] Disponível em https://animalexdominis.files.wordpress.com/2018/03/proteccc3a7c3a3o-das-redesesistemas-informc3a1ticos-2017.pdf (Acedido em 04-12-2019).
As alíneas a) a ff) do art.º 4º do Regulamento das Tecnologias e dos Serviços da Sociedade da Informação (RTSI) também trazem algumas definições muito importantes para o nosso tema. Disponível em https://www.inacom.gov.ao/fotos/frontend_6/editor2/1_lei_202_de_2011-22_de_julho_de_2011.pdf (Acedido em 02-09-2020).

[180] O que nos parece uma boa prática legislativa, nem sempre seguida em Portugal, onde abundam contradições entre definições dadas em diferentes diplomas.

[181] Antes do ACP que representa a "única versão válida", havia um documento nunca tornado oficial, mas que chegou a ser do domínio público, designado por Proposta de Lei do Código Penal – disponível em http://www.parlamento.ao/documents/91841/0/PROPOSTA+DE+LEI+DO+CÓDIGO+PENAL (Acedido aos 03-03-2020) – no qual o legislador seguia a mesma estruturação da CB (faltando unicamente a inclusão dos crimes contra os conteúdos), pelo que desconhecemos o que motivou o legislador a adotar outra estruturação no ACP. Ali os crimes informáticos constavam todos no Título VIII e não tinham a dispersão patente no ACP. Este Título VIII comporta três capítulos. No primeiro temos as definições (art.º 439º); no segundo temos os crimes contra dados informáticos, sendo estes:

- Artigo 440.º (Acesso ilegítimo a sistema de informação e devassa através de sistema de informação);
- Artigo 441.º (Intercepção ilegítima em sistema de informação);
- Artigo 442.º (Dano em dados informáticos).

No último capítulo vêm os crimes contra as comunicações e sistemas informáticos, sendo estes:

- Artigo 443.º (Sabotagem informática);
- Artigo 444.º (Falsidade informática);
- Artigo 445.º (Burla informática e nas comunicações);
- Artigo 446.º (Reprodução ilegítima de programa de computador, bases de dados e topografia de produtos semicondutores).

3.2.1. Os Crimes Contra a Confidencialidade, Integridade e Disponibilidade de Sistemas Informáticos e Dados Informáticos

Nestes crimes o ACP prevê simplesmente três:

- Devassa por meio informático (art.º 212º);
- Violação de telecomunicações (art.º 213); e
- Dano informático (art.º 399º).

Primeiramente espanta-nos o facto de não serem consagrados neste grupo outros crimes[182] com destaque ao acesso ilegítimo e sobre o qual teceremos algumas considerações.

O crime de acesso ilícito[183] é dentre os crimes informáticos o mais frequente porque possibilita o cometimento dos outros crimes.

Tem como pedra de toque o acesso intencional e não autorizado a um sistema[184], o que quer dizer que fica objetivamente preenchido por qualquer ação que permita ao agente aceder a um sistema ou rede informática[185] e a sua investida pressupõe conhecimentos técnicos que possibilitam a ação de imiscuição.

Este vem precisamente dar cobertura "a área que se vem denominando por *hacking informático*"[186].

O bem jurídico-penal que visa preservar é a segurança do sistema informático e consequentemente o "domicílio informático"[187], por isso a sua efetivação se processa mediante a violação das regras de segurança.

---

[182] Intercepção ilegítima, interferência de dados, interferência em sistemas e uso abusivo de dispositivos.
[183] Termo usado no art.º 6º da lei do cibercrime de Cabo Verde.
[184] **VERDELHO**, Pedro. Comentário das Leis Penais Extravagantes. Op. cit, p. 516.
[185] **VERDELHO**, Pedro. "Cibercrime." Direito Da Sociedade Da Informação, vol. IV, op. cit, p. 366.

[186] **RODRIGUES**, Benjamim Silva, idem, p. 281.
[187] Sobre este conceito o acórdão proferido pelo Tribunal da Relação do Porto de 15-10-2008 salienta que «O bem jurídico protegido do crime de acesso ilegítimo é a segurança do sistema informático – a proteção ao designado "domicílio informático" algo de semelhante à introdução em casa alheia.» (*In* Ministério Público. Jurisprudência sobre cibercrime. Nota Prática nº 15/2020. Disponível em http://cibercrime.ministeriopublico.pt/pagina/jurisprudencia-sobre-cibercrime. Acedido aos 31-08-2020).

Benjamim Silva Rodrigues identifica três tipos de condutas distintas e lesivas da inviolabilidade do domicílio informático-digital:

1. *O acesso ilegítimo ganancioso* – tem intenção de obter um benefício ou lucro vantagens ilegítimos.
2. *O acesso ilegítimo perigoso ou insidioso* – processado com a exploração das vulnerabilidades ou falhas de segurança do sistema de rede informáticos.
3. *O acesso ilegítimo de exploração, aventureiro ou de curiosidade* – tem o intuito de satisfazer uma "veia explorativa" ou ainda uma "curiosidade", por intermédio da consulta de dados pessoais.

RODRIGUES, Benjamim Silva, idem, p. 286.

Um dos exemplos mais frequentes e que caraterizam a prática do ilícito de acesso ilegal é o uso infundado do nome do utilizador (*username*) e o uso da palavra-passe (*password*). Dito isto, o que geralmente se constata nesses casos é a utilização por parte do infrator de elementos de identificação de outrem[188] para que, por intermédio destes, possa aceder ao sistema global de rede de computadores.

Uma questão que tem sido muito levantada no estudo deste tipo penal é a de examinar que tipo de acesso deve ser punido, ou seja, que acesso merece realmente censura penal.

Em Angola um delito com nomenclatura semelhante está plasmado no art.º 56º da Lei de Proteção de Dados Pessoais (LPDP)[189], com a designação de *acesso indevido*[190][191]. O nº 1 deste artigo preceitua que

"Quem, sem autorização, aceder a dados pessoais cujo acesso lhe está vedado, incorre em crime punível com pena de prisão de 6 meses a 2 anos ou multa correspondente."

A doutrina e a jurisprudência defendem, e concordamos, que o acesso deve ser por si só penalizado sem que para tal existam mais outras exigências e ademais sem considerarmos a parcialidade ou a totalidade do acesso[192].

As motivações que justificam tal acesso, quer sejam de natureza pecuniária, patrimonial ou de outro caráter, são puramente irrelevantes[193]. O que é relevante para muitas leis e funciona como qualidade agravadora da pena a ser aplicada é o acesso ocorrer "através de violação de

---

[188] Este crime tem igualmente por fim a proteção de dados pessoais e corresponde em parte ao crime de acesso indevido do art.º 44º da Lei n.º 58/2019, de 08 de Agosto LGPD de Portugal.
[189] Lei nº 22/11 de 17 de Junho.

[190] Também está previsto no art.º 6º do Anteprojeto já estudado da Lei de Combate à Criminalidade no Domínio das Tecnologias de Informação e Comunicação e dos Serviços da Sociedade da Informação do ano de 2011, e aí tem a designação de *acesso ilegítimo.*
O acesso indevido difere-se do acesso ilegítimo embora tenham nomes similares. No caso do acesso indevido o que se pune não é o acesso ao sistema, mas sim o acesso/conhecimento ilícito de dados de determinada natureza (dados pessoais), logo o crime pode inclusivamente ser praticado em ambiente analógico/não digital.

[191] A legislação portuguesa também estabelece crimes informáticos em diferentes diplomas. A título de exemplo, o crime de devassa por meio informático é previsto no art.º 193º do CP, enquanto o crime de acesso ilegítimo está consagrado no art.º 6º da Lei do Cibercrime, isto é, Lei n.º 109/2009, de 15 de Setembro.
[192] Para mais informações sobre o enquadramento histórico e dogmático da punição e das possíveis causas de justificação e exculpação do acesso informático ilegítimo leia-se as p. 54-72 da obra de **HEITOR**, Pedro Levi Vieira de Oliveira. Contributo para a compreensão das causas de exclusão de ilicitude e da culpa no crime de acesso ilegítimo. Dissertação de Mestrado em Direito e Informática. Universidade do Minho, Outubro de 2015. Disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/40898/1/Pedro%20Levi%20Vieira%20de%20Oliveira%20Heitor.pdf (Acedido aos 27-11-2019).
[193] Por exemplo, no acórdão do Tribunal da Relação de Coimbra de 17 de Fevereiro de 2016 diz que o tipo subjetivo deste ilícito penal não exige qualquer intenção específica (como seja o prejuízo ou a obtenção de benefício ilegítimo), ficando preenchido com o dolo genérico de intenção de aceder a sistema. Disponível em http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/e4727d7882f56c9d80257f610055dc8e?OpenDocument (Acedido aos 05-05-2020).

regras técnicas de segurança", e possibilitar o "conhecimento de dados pessoais" ou resultar em "benefício ou vantagem patrimonial".

No entanto, nem todo o tipo de acesso ilegal tem a mesma intensidade de gravidade. Existe a mera intromissão informática representada pelo simples ato de aceder no todo ou em parte do sistema, no qual não se regista a obtenção de benefício algum – é o denominado "acesso mínimo". Noutra vertente temos o designado "acesso qualificado"[194] em que o autor da ilicitude com a sua conduta obtém uma vantagem ou proveito.

Num ou noutro caso, por norma, pune-se a tentativa e o procedimento criminal depende da apresentação da queixa.

Esta diferenciação entre o acesso mínimo e o qualificado tem por finalidade defender o *white hat hacking* ou "*hacker* inocente" cuja atuação, para além de não ser dolosa, é pautada pela ética.

É tarefa do administrador encetar diligências que permitam manter não só o acesso ao sistema como também os outros pilares da segurança da informação, mormente a confidencialidade, a disponibilidade e a integridade.

3.2.1.1. Devassa por meio de informática[195]

Está previsto no Capítulo VII relativo aos Crimes Contra a Reserva da Vida Privada[196].

Essa infração tem razão de ser já que a informática catalisou as preocupações da proteção da vida privada. O potencial lesivo da informática é tão elevado ao ponto de deixar a intimidade de toda gente sujeita a ser devassada a qualquer o instante[197].

---

[194] Denominação que pode ser encontrada no art.° 154° da Lei n° 12.737/12, conhecida extraoficialmente como Lei Carolina Dieckmann, que foi acrescida ao Código Penal brasileiro.

[195] Pela elevada relevância que este crime dá a proteção dos "dados individualmente identificáveis", João Macedo discorda da sua inclusão num Código Penal, sugerindo ("por uma questão de coerência e unidade") a sua inserção numa Lei Extravagante, particularmente a Lei de Proteção de Dados Pessoais. **MACEDO**, João Carlos Cruz Barbosa de, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, Coimbra Editora, 2009, p. 257.
Entendemos que está infração é substancialmente consumida pelo crime de ***Incumprimento das obrigações relativas a protecção de dados pessoais*** do art.° 54.° do ALPDP. Assim, quando este diploma for aprovada teremos uma espécie de duplicação de punição da mesma infração, o que é "inconveniente" e macula "a unidade normativa desejável".

[196] Os crimes prescritos neste capítulo são ao todo os seguintes:

Artigo.° 209.° - (Introdução em casa alheia)
Artigo.° 210.° - (Introdução em lugar vedado ao público)
Artigo.° 211.° - (Perturbação e devassa da vida privada)
Artigo.° 212.° - (Devassa por meio de informática)
Artigo.° 213.° - (Violação de correspondência)
Artigo.° 214.° - (Violação de telecomunicações)
Artigo.° 215.° - (Violação de segredo)
Artigo.° 216.° - (Violação de sigilo profissional)

De acordo com o art.º 212º do ACP, comete o crime de devassa por meio informático

1. Quem:

a) proceder a tratamento informático de dados ou informações individualmente identificáveis sem estar devidamente autorizado ou, estando autorizado, não tomar as precauções necessárias para garantir a segurança desses dados, por forma a impedir que sejam divulgados, alterados, destruídos ou inutilizados;

b) aceder, sem autorização, a dados informaticamente tratados que contenham informações individualmente identificáveis;

c) transmitir, sem autorização, a terceiros ou para fins diferentes dos autorizados, dados ou informações informaticamente tratadas é punido com pena de prisão até 1 ano ou com a de multa até 120 dias.

2. Quem, sem estar competentemente autorizado, criar, mantiver ou utilizar ficheiro informático de dados pessoalmente identificáveis relativos a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical ou à vida privada de outrem é punido com pena de prisão até 2 anos ou com a de multa até 240 dias.

O seu modo de atuação compreende o acesso ilegal a um computador ou o acesso por qualquer forma aos ficheiros armazenados num computador que contenham dados pessoais, designadamente imagens ou vídeos, sobre a vida privada e que quando acedidos por terceiros os colocam na hasta pública, difundindo-os por intermédio da Internet.

Pressupõe atuação intencional (art.º 12º) e na al.) b) deste artigo está parcialmente subentendido o crime de acesso ilegítimo.

Em todo o seu *corpus* nada se menciona sobre a punição da tentativa, todavia, tal como sucede na legislação portuguesa[198], defendemos que a tentativa deve ser sancionada.

A penalidade é agravada de um terço nos seus limites máximo e mínimo quando o crime for praticado com a pretensão de conseguir uma recompensa ou visar prejudicar alguém (art.º

---

[197] **ASCENSÃO,** José de Oliveira – "Criminalidade informática", *in* Direito da Sociedade da Informação, Vol. II, Coimbra Editora, Coimbra, 2001, p. 264.

[198] Nº 2 do art.º 193º do CP.

217º), ficando o procedimento criminal dependente da apresentação de queixa por parte do lesado (art.º 218º), por isso é um delito semipúblico.

Este crime que atenta contra o *Direito à identidade, à privacidade e à intimidade,* constitucionalmente consagrado no art.º 32º nº 1 da CRA[199] que estipula o seguinte:

> **«A todos são reconhecidos os direitos à identidade pessoal, à capacidade civil, à nacionalidade, ao bom nome e reputação, à imagem, à palavra e à reserva de intimidade da vida privada e familiar.»**

A falta de precaução dos utilizadores, o armazenamento de conteúdo pessoal libidinoso em dispositivos informáticos, agravado pelo excesso de exposição da vivência íntima em ambientes virtuais são comportamentos que devemos evitar, porque deixam-nos propensos a sermos vítimas de devassa informática[200].

Facilmente notamos que o bem jurídico em consideração tem a ver com a proteção da vida privada, pois os dados relativos a ela são considerados sensíveis.

Ainda alinhamos do entendimento segundo o qual este ilícito pretende garantir "o direito à autodeterminação informacional e comunicacional, no sentido de que qualquer pessoa tem o direito a não ver processados determinados *dados sensíveis,"*[201] já que este direito garante a cada um a capacidade de controlar e dominar os fluxos informacionais e comunicacionais que envolvem o seu ciberespaço.

---

[199] Em Portugal – e seguindo o acórdão do Tribunal da Relação do Porto – o crime de devassa por meio de informática estabelecido no art.º 193º do CP é resultante do art.º 35º da CRP e pretende dar guarida a reserva da vida privada contra as eventuais ações de "discriminação que o uso dos meios informáticos torna exponencialmente perigosos."
Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b54faf2d4330b8d480257c6e004ff2df?OpenDocument (Acedido aos 6-12-2019).

[200] Em face disso, a polícia judiciária portuguesa aconselha aos cidadãos o seguinte:

- Não coloquem imagens ou vídeos pessoais contendo actos sexuais em computador acessível à rede Internet; Se o fizerem devem ter sempre em conta que o computador pode ser acedido a qualquer momento por terceiro autorizado ou não que poderá aproveitar as imagens para as difundir;
- Quando enviar o computador para reparação ou actualização com o disco rígido certifique-se que a informação pessoal nomeadamente imagens, informação bancária e outros dados pessoais não estão acessíveis;
- No caso de tomar conhecimento do facto de que os seus dados pessoais independentemente da sua natureza foram divulgados contra a sua vontade contacte de imediato identificando-se o prestador de serviços de Internet ou a Comissão Nacional de Protecção de Dados por forma a que os seus dados sejam retirados;
- Ao reencaminhar um correio electrónico com imagens, vídeos ou outros dados pessoais de terceiros ou se os publicita num site pode incorrer em procedimento criminal;
- Quem contribuir para a difusão deste tipo de dados pessoais mesmo que a estes não tenha tido acesso em primeiro lugar e já proveniente de outras difusões pode incorrer de igual forma no crime mencionado;
- Participe às autoridades;
- No caso de ser vítima e pretender apoio psicológico contacte entidades e associações especializadas em apoio pessoal/personalizado.

Disponível em https://www.policiajudiciaria.pt/acesso-ilegitimo-a-centrais-telefonicas-e-devassa-da-vida-privada-por-meios-informaticos-2/ (acedido aos 6-12-2019).

[201] **RODRIGUES**, Benjamim Silva, idem, p. 462.

3.2.1.2. Violação de telecomunicações

Para além do crime de devassa por meio da informática, no Capítulo VII temos igualmente mais dois crimes que estão relacionados à informática e geralmente tratados em códigos penais: a violação de correspondência e a violação de telecomunicações[202]. Para o nosso estudo interessa-nos somente o segundo delito.

O crime de violação de telecomunicações vem consagrado no art.º 214º e tem a seguinte conteúdo

> **1. Quem, sem consentimento, se intrometer no conteúdo de telecomunicação e dele tomar conhecimento é punido com pena de prisão até 1 ano ou com a de multa até 120 dias.**
> **2. A mesma pena é aplicada a quem, sem consentimento, divulgar o conteúdo de telecomunicação referido no número anterior.**

Este tipo penal tem acolhimento no art.º 34º da CRA relativo a "Inviolabilidade da correspondência e das comunicações"[203], porém nele ficam excetuados os casos em que tal ingerência se processa por "decisão de autoridade judicial". Tem similarmente abrigo no art.º 32º da CRA que retrata o direito à privacidade, neste particular à *"privacidade electrónico-digital"*[204].

O elemento objetivo do delito de violação de telecomunicações tem dois aspetos, o primeiro dá-se com a "intromissão em conteúdo de telecomunicações ou dele tomar

---

[202] No Código Penal português esses dois crimes são tratados conjuntamente no artigo 194.º (Violação de correspondência ou de telecomunicações), fazendo parte do Capítulo VII dos crimes contra a reserva da vida privada, pelo que no caso de Angola essa aglutinação também seria recomendável, dadas similitudes de ambos os ilícitos penais e ainda por terem a mesma penalidade.

[203] Na CRP a inviolabilidade e a não ingerência nas telecomunicações é objeto de previsão do art.º 34º nº s 1 e 4 que consagram expressamente que:

> 1. O domicílio e o sigilo da correspondência e dos outros meios de comunicação privada são invioláveis.
> 4. É proibida toda a ingerência das autoridades públicas na correspondência, nas telecomunicações e nos demais meios de comunicação, salvos os casos previstos na lei em matéria de processo criminal.

[204] **RODRIGUES**, Benjamim Silva. Idem, p. 452.

conhecimento"; o segundo efetiva-se pela "divulgação de tal conteúdo"[205][206]. Em ambos os casos exige-se que tanto a intromissão como a divulgação sejam efetuadas sem consentimento.

Do *corpus* do artigo não divisamos nada sobre o seu elemento subjetivo, todavia a atuação do agente infrator deve ser dolosa (art.º 12º ACP).

A confidencialidade das telecomunicações ou das comunicações eletrónicas constitui o bem jurídico[207] tutelado por este crime que não prevê a exigência de queixa para a concretização do procedimento criminal, sendo por isso um crime público.

Analisando a moldura penal prevista para essa infração (1 ano de prisão ou 240 dias de multa), nos termos do art.º 21º ACP podemos concluir que somente é punida a sua forma consumada.

3.2.1.3. Dano informático[208][209]

Semelhante ao crime de dano comum[210], é o segundo e último crime contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos do ACP.

Está previsto propriamente no art.º 399º na Secção IV[211] dos Crimes de Dano que é parte integrante do Capítulo II relativo aos Crimes Contra a Propriedade, nele pode ler-se o seguinte:

---

[205] A publicidade por meio informático constitui sempre uma agravante nos termos do nº 2 do art.º 201º do ACP.

[206] De acordo ao acórdão do TRL de 09-04-2013, nem toda divulgação é punida. "Apenas a divulgação de conteúdo da comunicação integra a modalidade de conduta em causa". Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/505fcfb3e621198980257be30035d463?OpenDocument (Acedido aos 15-01-2020).

[207] Para Pedro Dias Venâncio "O bem que se protege é aqui não só a privacidade mas também a confiança da comunidade na integridade dos meios de comunicação, nomeadamente das telecomunicações". **VENÂNCIO,** Pedro Dias. Breve introdução da questão da investigação e meios de prova na criminalidade informática. Compilações Doutrinais Verbo Jurídico. Dezembro 2006. Disponível em https://www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf (Acedido aos 15-01-2020).

[208] Em outros diplomas legais este crime tem tido outras designações. Na já revogada Lei da Criminalidade Informática – Lei nº 109/91 de 17 de Agosto – tínhamos o crime de *dano relativo a dados ou programas informáticos* (art.º 5º) que na Lei de Proteção de Dados Pessoais (Lei nº 67/98 de 26 de Outubro) foi complementado com o crime de *viciação ou destruição de dados pessoais* (art.º 45º).
Na Lei n.º 109/2009, de 15 de Setembro – Lei do Cibercrime – temos no art.º 4.º o crime de dano relativo a programas ou outros dados informáticos.
Pensamos ser aceitável a designação adotada para esse delito no ACP e achamos ser "incoerente e redundante" a designação *dano relativo a dados ou programas informáticos* uma vez que na definição de dado informático já estão subentendidos os programas informáticos. Para mais informações sobre essa incoerência terminológica leia-se **VENÂNCIO**, Pedro Dias, Lei do Cibercrime, Op. cit., p. 47 e 48.

[209] Também Duarte Nunes acha esse *nominem juris* "incoerente e redundante" e sugere que se designe apenas por "Dano relativo a dados informáticos". **NUNES**, Duarte Alberto Rodrigues, O crime de dano relativo a programas ou outros dados informáticos, Revista do Ministério Público, Lisboa, Ano 39, nº 153 (Janeiro-Março 2018), p. 142.

[210] Entre os dois crimes "jamais existirá qualquer sobreposição". (**NUNES**, Duarte Alberto Rodrigues, O crime de dano relativo a programas ou outros dados informáticos, p. 142). O crime de dano do art.º 390º tem por objeto de tutela bens corpóreos, enquanto o crime de dano informático tutela bens incorpóreos.

[211] Os crimes desta Secção são os seguintes:

Artigo.º 396.º - (Dano)
Artigo.º 397.º - (Dano de coisas com valor e interesse públicos)
Artigo.º 398.º - (Dano com violência)
Artigo.º 399.º - (Dano informático)

1. Quem, com intenção de causar prejuízo a terceiro, alterar, deteriorar, inutilizar, apagar, suprimir, destruir ou, de qualquer forma, causar dano a sistemas ou dados informáticos, conforme os define o artigo 233.º[212], é punido com pena de prisão de 6 meses a 3 anos ou com a de multa até 360 dias.

2. A mesma pena é aplicável a quem, mediante a introdução ou transmissão de dados informáticos ou, por qualquer outra forma, interferir no funcionamento de sistema informático, causando intencionalmente dano a alguém.

3. Em cada um dos casos descritos nos números anteriores, a pena é de:

a) prisão de 1 mês a 3 anos ou de multa de 120 a 360 dias, se o valor do prejuízo não for elevado;

b) de prisão de 1 a 5 anos ou de multa de 120 a 600 dias, se o prejuízo for elevado;

c) de prisão de 2 a 8 anos, se o valor do prejuízo for consideravelmente elevado.

4. Se o dano causado não for relevante, nos termos do artigo 396.º[213], não há lugar a qualificação.

Na sua forma simples dos números 1 e 2 é um crime semipúblico, tendo uma moldura penal a prisão de seis meses a três anos ou multa. Torna-se um crime público quando se enquadrar nas circunstâncias modificativas agravantes das al. b) e c) do nº 3, ou seja, se os danos resultarem em prejuízo grandioso ou notavelmente alto, punindo-se nestes casos com penas de prisão de um a cinco anos ou de um a oito anos, respetivamente.

O ACP define 'valor elevado' e 'valor consideravelmente elevado' nas al. a) e b) do art.º 377º[214].

---

[212] A al. c) deste artigo define **Dado informático** como sendo "qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo programas que permitam a um sistema informático executar uma função."

[213] O seu nº 2 afirma que "*Considera-se dano relevante o que se traduzir num prejuízo superior a metade do salário mínimo nacional da função pública*".
O problema que aqui se levanta é da possibilidade ou não de avaliar-se pecuniariamente todos os danos informáticos, uma vez que nem sempre incidem sobre bens materiais com preços preestabelecidos ou quantificáveis. Portanto, para melhor precisão legislativa esse ponto deveria ter o seu conteúdo modificado ou enriquecido.

O anteprojeto não faz menção alguma da punição da tentativa[215]. Parece-nos que tal opção deve-se ao facto de não se tratar de um crime de perigo. Quanto à modalidade de consumação do ataque ao bem jurídico, espelhada no nº 1, é um crime de resultado.

No que se refere ao bem jurídico penalmente tutelado[216], o delito de dano informático visa defender "a integridade e a fiabilidade de dados e ao bom funcionamento dos programas informáticos"[217][218], ou seja, pretende proteger a integridade funcional dos dados informáticos, no que tem que ver com a disponibilidade e usabilidade dos mesmos[219].

Serão apenas objeto de punição os danos que sejam significativos[220], tendo o causador do dano o completo conhecimento do valor que o bem tem para a vítima, o que quer dizer que o elemento cognitivo dolo deve ser tido em consideração.

Infelizmente o nº 4 remete a relevância do dano causado simplesmente ao seu respetivo valor monetário, colocando de parte outros aspetos importantes como a utilidade e a afetividade. Essa omissão está eventualmente ligada a dificuldade do autor do crime poder avaliar ou imaginar que bem tenha valoração utilitária ou afetiva para a vítima; além disso, muitas vezes o valor sentimental apesar de ser inestimável pode suplantar o valor económico.

Os dados informáticos são o objeto material desse ilícito penal que "apenas poderá ser cometido dolosamente"[221].

As formas de sua perpetração são diversas[222], uma das mais frequentes é a divulgação de vírus de computador e a dos chamados "cavalos de Tróia" que podem danificar os dados informáticos, corromper programas ou causar caos ao computador.

---

[214] "**Valor consideravelmente elevado**", o que exceder 500 vezes o salário mínimo mensal da função pública, no momento em que o facto for praticado.
b) "**Valor elevado**", o que exceder 100 vezes o salário mínimo mensal da função pública, no momento em que o facto for praticado.

[215] Na Lei n.º 109/2009, de 15 de Setembro já citada, o art.º 4.º do crime de dano relativo a programas ou outros dados informáticos, diz no seu nº 2 que "A tentativa é punível".
Perece-nos que mesmo que tal fosse possível, a tentativa de cometimento do crime de dano informático seria de difícil comprovação técnica.

[216] Duarte Nunes aponta a inexistência de unanimidade quanto ao bem jurídico tutelado por esse crime. Segundo este autor, alguns defendem que o bem jurídico tutelado é a "integridade dos dados e o bom funcionamento dos programas", enquanto outros acham ser o património. Por fim, dá razão aos defensores da primeira ideia, pelo que corroboramos. **NUNES**, Duarte Alberto Rodrigues, O crime de dano relativo a programas ou outros dados informáticos, idem, p. 144.

[217] **ALBUQUERQUE**, Paulo Pinto de & **BRANCO**, José. Idem, p. 510.

[218] Para Túlio Lima Vianna o património é o bem jurídico penalmente tutelado no delito de dano informático (também Pedro Dias Venâncio é da mesma opinião na Lei do Cibercrime, p. 45) e este deve abranger não somente o conjunto de bens de valor económico como também aqueles que tenham um "valor-utilidade e valor afetivo para seu proprietário" **VIANNA**, Túlio Lima. Do delito de dano e de sua aplicação ao Direito Penal informático, 2014. Disponível em https://jus.com.br/artigos/5828/do-delito-de-dano-e-de-sua-aplicacao-ao-direito-penal-informatico (Acedido em 26-12-2019).

[219] **ALBUQUERQUE**, Paulo Pinto de & **BRANCO**, José. Idem, p. 511.

[220] Parece-nos que essa opção legislativa surge como forma de corroborar com o *princípio da insignificância* ou da *bagatela* que preconiza a não punição dos crimes que geram uma ofensa irrelevante.

[221] **NUNES**, Duarte Alberto Rodrigues, O crime de dano relativo a programas ou outros dados informáticos, idem, p. 157.

[222] Todas as condutas típicas deste crime que exigem lesão efetiva ao sistema ou aos dados informáticos são as que configuram uma alteração, deterioração, inutilização, apagamento, supressão ou destruição; aliás como se depreende do próprio *corpus* do artigo em estudo.

Duarte Nunes assinala quatro comportamentos que são subsumíveis a essa infração, sendo:

A introdução deliberada de vírus informáticos suscetíveis de danificar os sistemas informáticos é "não só a forma mais perigosa de prática deste crime, como aquela que será mais frequente e que mais justificará a necessidade da sua penalização criminal"[223].

A difusão de *malware* e a propagação de vírus por via de *spam* são outras ações dignas de realce.

Constatamos que na maior parte delas temos o acesso não autorizado como instrumento essencial para o cometimento do crime[224], efetivando-se por meio da adulteração ou alteração de conteúdos.

Os testes aos mecanismos de segurança dos sistemas das redes não são punidos por este crime nos casos de serem autorizados pelo respetivo dono do sistema, já que o delito de dano informático visa somente punir atuações ilegítimas.

Apesar de respeitarmos a opção legislativa, entendemos que como forma de facilitar a aplicabilidade da lei, o *corpus* do artigo deveria ser enriquecido pela introdução ou inserção de novas matérias, isto é, sugerimos ajustamentos na redação.

Deste modo, é recomendável que o legislador faça uma diferenciação no que se refere aos danos causados por vírus de computador, por exemplo, achamos que a lei deveria punir de forma desigual quem insere vírus a um computador desconectado ou "*stand alone* e aquele que realiza essa conduta em rede de computadores, com resultado lesivo muito mais grave"[225].

3.2.2. Os Crimes relacionados com Computadores

Contrariamente aos crimes contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos, nos crimes relacionados com computadores o legislador foi mais afortunado prevendo no ACP ambas as infrações prenunciadas na CB:

---

1. O envio de vírus informático através de um *e-mail*.
2. *Defacing* (alteração ilícita de páginas da Internet com a finalidade de transmitir ideias ou provocações).
3. Disseminação de "bombas lógicas" ou "programa *crash*".
4. Modificação da *password* de um dado programa informático (v.g. o *Facebook*).

NUNES, Duarte Alberto Rodrigues, O crime de dano relativo a programas ou outros dados informáticos, idem, p. 152 e 153.

[223] **VENÂNCIO**, Pedro Dias. Lei do Cibercrime, idem, p. 47.

[224] Embora o acesso ilegítimo seja a base de perpetração dos demais delitos informáticos, ou seja, só há possibilidade de praticar outros crimes se tiver existido uma penetração num sistema, há na verdade a possibilidade de não ser sempre assim, e como exemplo temos o caso de alguém estar autorizado a aceder um sistema mas não o destruir. Neste caso não haverá acesso ilegítimo mas haverá o crime de dano sobre dados ou programas. Portanto, apesar de ser raro, é possível haver o crime de dano informático sem ter sido precedido de um acesso ilícito.

[225] **CAPANEMA**, Walter Aranha. Crime de dano e o vírus de computador, pág. 11. Disponível em https://www.academia.edu/2515494/Crime_de_dano_e_o_vírus_de_computador (Acedido em 26-12-2019).

- Falsidade informática (art.º 235º); e
- Burla informática e nas telecomunicações (art.º 407º).

3.2.2.1. Falsidade informática

É provavelmente o tipo mais comum de crime cibernético.

De fato, é o mais conhecido e talvez o mais antigo, tendo sido constatado desde o surgimento da terceira geração de computadores, quando surgiram na vida de empresas financeiras e bancárias[226].

O crime de falsidade informática é parte integrante do Capítulo I relativo a Falsificação de Documentos, Dados Informáticos e Registos Técnicos[227]. Por sua vez este capítulo está incluso no Título III respeitante aos Crimes Contra a Fé Pública.

É muito semelhante ao crime comum de falsificação e com base no art.º 235º do ACP incorre na prática desse delito

> **1. Quem, com intenção de enganar, introduzir, alterar, eliminar ou suprimir dados em sistema informático ou, em geral, interferir no tratamento desses dados, por forma a dar origem a dados falsos que possam ser considerados verdadeiros e utilizados como meio de prova, é punido com pena de prisão de 6 meses a 5 anos ou com a de multa de 60 a 600 dias.**
> **2. A mesma pena é aplicável a quem, não sendo o falsificador, com igual intenção, utilizar os dados informáticos falsos ou falsificados.**
> **3. Se o autor dos factos descritos nos números anteriores for funcionário público no exercício das suas funções, a pena é de prisão de 1 a 6 anos.**

O crime de falsidade informática funda-se no manuseamento dos dados introduzidos num sistema informático ou do seu tratamento por intermédio desse mesmo sistema, acabando

---

[226] De acordo a *Octopus Cybercrime Community* do Conselho da Europa. Disponível em https://www.coe.int/en/web/octopus/blog/-/blogs/computer-related-forgery-and-computer-related-fraud-the-need-to-build-and-include-these-new-criminal-types-in-a-modern-penal-code/ (Acedido aos 11-012-2020).

[227] Os artigos previstos neste capítulo são os seguintes:

> Artigo.º 233.º - (Definições)
> Artigo.º 234.º - (Falsificação de documento)
> Artigo.º 235.º - (Falsidade informática)
> Artigo.º 236.º - (Falsificação de registos e aparelhos técnicos)
> Artigo.º 237.º - (Destruição, inutilização ou subtracção de documento e registo técnico)
> Artigo.º 238.º - (Tentativa)

por resultar desse facto a criação de documentos ou dados dissimulados, colocando em causa a segurança e a fiabilidade dos documentos[228] no tráfico jurídico-probatório[229], tal como sucede com os documentos "em sentido clássico" falsos no âmbito do crime de falsificação de documento p. e p. pelo art.º 256.º do CP[230].

A jurisprudência portuguesa tem discutido os bens jurídicos protegidos por este ilícito penal, segundo o Acórdão do Tribunal da Relação do Porto, neste crime o prejuízo não tem de ser patrimonial, pois o bem jurídico que nele se protege não é o património, mas a confidencialidade, integridade e disponibilidade de sistemas informáticos, das redes e dados informáticos[231]. Porém, o Tribunal da Relação de Évora teve outro entendimento, concluindo que este crime "visa proteger a segurança das relações jurídicas enquanto interesse público essencial que ao próprio Estado de Direito compete assegurar e não a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e de dados informáticos"[232].

O nº 1 do art.º 235º do ACP prevê o crime cometido na sua forma simples, ou seja, na sua forma não qualificada, acarretando uma pena de prisão que vai dos seis meses a cinco anos ou com a pena de multa de sessenta a seiscentos dias. Neste aspeto, as condutas de "introduzir" e "alterar" ou modificar são de fácil compreensão, já o mesmo não acontece com o comportamento de "eliminar" ou apagar e "suprimir". Sendo assim, entendemos que apagar consiste na eliminação de dados que se encontrem num sistema informático e "suprimir" consiste em reter, ocultar, tornar temporariamente indisponíveis dados que aí se encontrem[233].

No tocante ao termo "interferir" está em consideração o ato de "influenciar o modo de tratamento informático de dados, a fim de esse tratamento não ocorrer do modo como, sem a atuação do agente, ocorreria"[234].

Pune-se não só quem falsifica como também quem se aproveita desses dados informáticos adulterados (nº 2). Pensamos que para esse caso o anteprojeto deveria punir de

---

[228] No art.º 3º nº 1 e nº 5 do Decreto-Lei n.º 290-D/99 que aprova o Regime Jurídico dos Documentos Electrónicos e da Assinatura Digital os documentos informáticos são equiparados aos documentos físicos.
Também no ordenamento jurídico angolano al. p) do art.º 4º do Decreto Presidencial n.º 202/11 de 22 de Julho (Regulamento das Tecnologias e dos Serviços da Sociedade da Informação) menciona que o Documento electrónico oferece "as mesmas garantias de fidedignidade, inteligibilidade e conservação de um documento em suporte papel".

[229] **NUNES**, Duarte Alberto Rodrigues. O crime de falsidade informática. Julgar Online, Outubro de 2017. Disponível em https://www.academia.edu/36977372/O_crime_de_falsidade_informática (Acedido em 03-01-2020), p. 1.

[230] **MACEDO**, João Carlos Barbosa de, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, Coimbra Editora, 2009, p. 236.

[231] Ac. TRP de 24-04-2013. Disponível em http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/872f3063233d8de480257b78003e60f3?OpenDocument (Acedido em 06-01-2019).

[232] Ac. TRE de 19-05-2015. Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/d97beb78d90d426b80257e5800393b9d?OpenDocument (Acedido em 06-01-2019).

[233] **PEREIRA**, Joel Timóteo Ramos, Compêndio Jurídico da Sociedade da Informação. Quid Juris, Abril de 2004, p. 522.

[234] **NUNES**, Duarte Alberto Rodrigues. Idem, p. 14.

forma diferente, aliás, com uma moldura penal mais branda ao infrator que apenas se beneficia dos dados já previamente defraudados.

No nº 3 estamos perante o crime de falsidade informática qualificada, que representa uma situação modificadora agravante consistente na qualidade do agente, que tem de ser necessariamente funcionário público e estar no exercício das suas funções. A pena para esses casos é a de prisão efetiva de um a seis anos.

De acordo com o art.º 238º do ACP a tentativa é sempre punível, aliás o mesmo acontece com os demais crimes deste capítulo.

O tipo objetivo[235] tem a ver com a manipulação de dados que resultam na produção de documentos não autênticos com o intento de que sejam considerados ou usados para fins juridicamente relevantes e, desta forma, provocar logro nas relações jurídicas, resultando deste cometimento prejuízo ou benefício ilícito.

Quanto ao tipo subjetivo, o crime de falsidade informática pressupõe o dolo no seu cometimento. É um *dolo duplo*[236] consubstanciado primeiramente na intenção específica de "provocar engano nas relações jurídicas", seguidamente, desta pretensão devem resultar documentos digitais falsos que sejam usados com fins de relevância jurídica como se fossem reais.

Corroboramos com a ideia segundo a qual, "o crime de falsidade informática não está limitado à manipulação de dados informáticos (ou do seu tratamento) alheios, pelo que se o agente manipular os dados ou o seu tratamento no âmbito de um programa ou sistema informático seu, desde que se verifiquem os demais elementos objetivos e subjetivos do tipo, comete o crime de falsidade informática"[237].

Verifica-se esse ilícito penal em transações bancárias, em operações de contabilidade e pagamento bem como na criação de perfis não genuínos[238]. Outras condutas que podem ser subsumidas neste crime são o *phishing*[239], o *pharming*[240], o *carding*[241] e todas aquelas que

---

[235] Dizer apenas que o tipo objetivo deste crime consiste em "introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer forma interferir num tratamento de dados" não é suficiente, visto que estes elementos assemelham-se ao tipo objetivo do crime de dano e, além disso, pouco se diferem dos factos relacionados ao crime de sabotagem informática. *In* **ALBUQUERQUE**, Paulo Pinto de & **BRANCO**, José. Idem, p. 506.
Segundo Pedro Verdelho, o crime de falsidade informática para que se verifique exige ainda "que dos actos típicos descritos resulte a produção de dados ou documentos não genuínos".

[236] Ibidem, Idem.

[237] **ASCENSÃO,** José de Oliveira – "Criminalidade informática", *in* Direito da Sociedade da Informação, Vol. II, Coimbra Editora, Coimbra, 2001, p. 222.

[238] Ac. TRP de 24-04-2013. Idem.

[239] Uma das técnicas de *phising* usada no cometimento desta infração é a criação de *sites* na Internet parecidos aos legítimos visando a obtenção de elementos bancários ou reservados, induzindo deste modo o usuário em erro. **MACEDO**, João Carlos Cruz Barbosa de, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, Coimbra Editora, 2009, p. 236.

[240] Para mais informações sobre o phishing e o pharming leia-se o Acórdão do STJ de 18/12/2013. Disponível em www.dgsi.pt (Acedido em 03.01.2020).

envolvam "a manipulação de dados informáticos registados ou incorporados, por exemplo, num cartão de débito ou crédito ou dispositivos (desde logo, computadores) que permitam o acesso a redes de pagamentos ou transferências de dinheiro como as redes Multibanco, Visa, Mastercard, American Express, Paypal, etc., ou do seu tratamento"[242].

Como podemos verificar, o crime de falsificação informática é um tanto quanto complexo e a sua complexidade resulta do facto de poder convergir com outros crimes informáticos[243].

3.2.2.2. Burla informática e nas telecomunicações

A burla informática ou a fraude de computador[244] é o ato de usar um computador para obter ou alterar dados eletrónicos ou para possibilitar a utilização ilegal de um computador ou sistema, conseguindo "uma transferência não consentida de activos patrimoniais de outrem"[245].

É o segundo e o último crime relacionado com computadores constante no ACP, fazendo parte do Capítulo III que aborda os Crimes Contra o Património em Geral, especificamente na Secção I relativa aos Crimes de Burla[246]. Vem enunciado no art.º 407º da seguinte maneira

Quem, com o propósito de obter para si ou para terceiro vantagem patrimonial ilícita:

a) interferir no resultado de tratamento de dados mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização, ou mediante intervenção, por qualquer outro modo não autorizado, no processamento;

---

[241] *Carding* é uma prática ilegal que envolve fraudes com cartões de créditos, usados por *Carders* a fim de fazer compras para si próprios e seus colegas e amigos. Disponível em https://pt.wikipedia.org/wiki/Carding (Acedido em 03-01-2020).

[242] **VERDELHO,** Pedro – "A nova Lei do Cibercrime", *in* Scientia Ivridica, T. LVIII (2009), p. 717 e ss, Universidade do Minho, Braga, 2009, p. 724-725.

[243] Por exemplo, segundo Pedro Verdelho não é óbvia a distinção entre este crime com o de dano informático e de sabotagem informática, uma vez que todos eles pressupõem a manipulação de dados informáticos. No entanto ele advoga que se distinguem em dois aspetos: primeiro, "na falsificação o dolo é mais complexo e supõe a intenção de provocar danos nas relações jurídicas; por outro lado, os dados em causa têm de ser susceptíveis de virem a dar origem a um documento falso que possa ser utilizado para finalidade juridicamente relevante como se fosse autêntico". *In* **ALBUQUERQUE**, Paulo Pinto de & **BRANCO**, José. Idem, p. 508 e 509.

[244] Fazendo paralelismo com a tradução *ad litteram* da designação inglesa: *computer fraud*.

[245] **RODRIGUES**, Benjamim Silva. Direito Penal, p. 358.

[246] Ao todo esta Secção comporta os artigos seguintes:

Artigo.º 404.º - (Burla)
Artigo.º 405.º - (Burla qualificada)
Artigo.º 406.º - (Burla para obtenção de alimentos, bebidas, combustíveis ou serviços)
Artigo.º 407.º - (Burla informática e nas telecomunicações)
Artigo.º 408.º - (Burla relativa a trabalho ou emprego)
Artigo.º 409.º - (Abuso de incapazes)
Artigo.º 410.º - (Punição da tentativa)
Artigo.º 411.º - (Restituição ou reparação)
Artigo.º 412.º - (Procedimento criminal)

b) usar programas, dispositivos electrónicos ou outros meios que, separada ou conjuntamente, se destinem a diminuir, alterar ou impedir, no todo ou em parte, o normal funcionamento ou exploração do serviço de telecomunicações e, pelas formas descritas, causar a outrem prejuízos de natureza patrimonial é punido com as penas do artigo 405.º.

Sendo um crime de dupla abrangência (informática e telecomunicações), é dos mais frequentes no ambiente virtual e tecnológico, constituindo "uma das formas de criminalidade informática mais impressivas da actualidade"[247].

Do *corpus* do artigo percebemos que o elemento objetivo do tipo legal de burla praticada no meio informático e nas telecomunicações consubstancia-se no ato de "interferir no resultado de tratamento de dados mediante estruturação incorrecta[248] de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização[249], ou mediante intervenção, por qualquer outro modo não autorizado, no processamento", podendo também consistir em "usar programas, dispositivos electrónicos ou outros meios que, separada ou conjuntamente, se destinem a diminuir, alterar ou impedir, no todo ou em parte, o normal funcionamento ou exploração do serviço de telecomunicações".

Subjetivamente esta infração pressupõe que o comitente aja de forma dolosa, visando a obtenção de um enriquecimento ilegal para si próprio ou para outrem, causando na esfera jurídica do lesado um prejuízo de natureza patrimonial.

Este ilícito penal tem por finalidade proteger o património privado por intermédio da garantia da segurança jurídica, exprimida na credibilidade nos sistemas informáticos e nas próprias telecomunicações[250].

O ACP considera a burla informática e nas telecomunicações como sendo uma subespécie da burla clássica[251][252] embora tenha especificidades próprias[253]. Significa que é um

---

[247] **SANTOS**, Rita Coelho. O tratamento jurídico-penal da transferência de fundos monetários através da manipulação ilícita dos sistemas informáticos. Coimbra Editora, 2005, p. 9.

[248] Por *estruturação incorreta* entenda-se "a modificação do programa em ordem a que as suas instruções sejam diferentes das inicialmente concebidas pelo proprietário – por exemplo, a introdução de novas instruções ou funções no programa, a eliminação ou alteração do seu processo de funcionamento, a modificação dos sistemas de controlo do próprio funcionamento". **ROCHA**, Manuel António Lopes. A revisão do código penal: soluções de neocriminalização. *In* Jornadas de direito criminal: revisão do código penal. Centro de Estudos Judiciários. 1° Vol., 1998, p. 95.

[249] Oliveira Ascensão considera a previsão da "*utilização de dados sem autorização* um equívoco completo, visto que a existência ou não de autorização é de todo irrelevante". Continua dizendo que "*o que importa é o meio ardiloso da manipulação de dados ou do resultado*, sob pena de, na sua opinião, o próprio acesso ilegítimo ter de ser abrangido no âmbito de protecção da norma". **ASCENSÃO**, José Oliveira de. Criminalidade informática, p. 216, *apud* **RODRIGUES**, Benjamim Silva. Direito Penal, p. 376.

[250] Sobre o bem jurídico protegido, Benjamim Rodrigues reforça dizendo o seguinte: "O que se protege é também a confiança social na fiabilidade e segurança dos serviços e redes das comunicações electrónicas que proporcionam vários tipos de serviços, nomeadamente no que respeita aos *modus* eletrónico-digitais de pagamento". **RODRIGUES**, Benjamim Silva. Direito Penal, p. 359.

tipo de burla qualificada e por esta razão é punida de acordo com o art.º 405º que remete às penalidades do crime de furto do art.º 378º[254].

Em resumo, prevê uma moldura penal abstrata que vai dos 6 meses aos 7 anos de acordo com o valor do prejuízo causado, ficando isentos de punição os casos que resultem em prejuízo reduzido (art.º 405º nº 3).

Embora corroboremos com os autores que advogam que estamos perante a criminalidade "económico-informática"[255], no nosso modesto ver, achamos que a lei deveria igualmente prever a punição da burla informática que incida sobre um bem que não seja quantificável monetariamente, pois tal é um cenário muito provável no mundo digital.

A futura lei salvaguarda a punibilidade da tentativa, exceptuando-se os cenários em que a lesão representa um valor ínfimo, nos termos do art.º 410º, contudo achamos que como forma de persuadir as pessoas ao não cometimento dessa infração, independentemente da situação e do valor do bem do particular lesado, a tentativa deveria ser sempre punida[256].

Prevê-se também a possibilidade de restituição ou reparação do prejuízo produzido quando tal seja exequível (art.º 411º).

Sendo um delito equiparado à burla qualificada, por regra o procedimento criminal não depende de queixa como estabelece o nº 1 art.º 412º, configurando deste modo um crime público.

Todavia, se

> **"o agente for cônjuge, ascendente ou descendente, adoptante ou adoptado, parente ou afim até ao terceiro grau da linha colateral da vítima ou com ela viva em condições análogas às dos cônjuges"**

---

[251] Apesar de não se constatar "qualquer actuação astuciosa do sujeito activo sobre o passivo" como acontece na "burla tradicional". Para mais desenvolvimentos consulte-se **SANTOS**, Rita Coelho. Op, cit., p. 230.

[252] Na burla em apreço, apesar de prever a intenção de enriquecimento próprio ou de outrem, *"não se exige que seja provocado engano ou ludíbrio na vítima"* como acontece com a burla tradicional, por esse motivo o Conselho da Europa defendia que esse ilícito fosse designado por fraude informática. **MARTINS,** A. G. Lourenço. "Criminalidade Informática." Op. cit., p. 20.

[253] Por exemplo, neste crime "não há engano, erro, nem relação causal com o acto de disposição. Por outro lado, a vítima não cede nada ao autor, sendo este o que toma directamente a coisa". **SERRANO GOMEZ**, Alfonso. Derecho Penal. Parte Especial. 7ª ed. Dykinson. Madrid, 2002, p. 408; *apud* **RODRIGUES**, Benjamim Silva. Direito Penal, p. 359.

[254] As penas aí previstas são as de

> a) prisão até 3 anos ou multa até 360 dias, se o valor da coisa subtraída não for elevado;
> b) prisão de 6 meses a 5 anos ou multa de 60 a 600 dias, se o valor da coisa subtraída for elevado;
> c) prisão de 1 a 7 anos, se o valor da coisa subtraída for consideravelmente elevado.

[255] **COSTA**, José de Faria & **MONIZ**, Helena, Algumas reflexões sobre a criminalidade informática em Portugal, Boletim da Faculdade de Direito, Coimbra, Vol.73, 1997, p. 322.

[256] Como atesta o nº 1 art.º 412º do CP português (crime de burla informática e nas comunicações).

então o procedimento criminal dependerá da acusação particular (nº 2 art.º 412º).

É um delito de "execução vinculada" (art.º 407º nº 1) e também de resultado[257] que pode estar em concurso real[258] ou efetivo com o crime de falsidade informática.

Ações como a distribuição de *e-mails* fraudulentos, o engajamento na mineração de dados via *spyware* e *malware,* a invasão de sistemas de computadores para aceder ilegalmente informações pessoais – como as que possibilitam o uso abusivo de cartão de crédito[259] ou de garantia – e o furto de tempo de acesso à Internet[260] podem preencher este ilícito penal.

Constituem ainda infrações cominadas propriamente no nº 2 do artigo *subjudice* as ações de *blackboxing* e *blueboxing* por serem "formas de perturbação das telecomunicações"[261] que possibilitam ludibriar "as operadoras telefónicas, de modo a não pagar qualquer tarifa ou a pagar um valor mais baixo comparativamente ao valor devido"[262].

3.2.3. Os Crimes relacionados com Conteúdos

No ACP, e tal como sucede na Convenção de Budapeste sobre o Cibercrime, prevê-se unicamente a inclusão nesta categoria a chamada pornografia infantil[263]. Todavia, julgamos que

---

[257] Acórdão do STJ de 20-09-2006. Disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/f271eacc3559b1cf8025724b0051dcf6?OpenDocument (Acedido aos 11-01-2020).

[258] Acórdão do TRP de 14-09-2016.
Disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/6f02100f48f04ae880258045004ea54d?OpenDocument (Acedido aos 11-01-2020).

[259] Para mais informações sobre a burla informática envolvendo cartões multibanco leiam-se os acórdãos, ambos do TRE, de 20-01-2015 (Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/737b074e63612dc880257de100582533?OpenDocument Acedido aos 11-01-2020) e de 29-11-2016 (Disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/f16dd7af9fdfd50d802580b2003fa644?OpenDocument Acedido aos 11-01-2020).

[260] O furto de tempo na internet sucede "quando alguém descobre o nome de utilizador (*login*) e palavra-passe de outrem e usa esses dados para aceder ao provedor de serviços de Internet, sendo este acesso pago, de modo a utilizar a Internet à conta do utilizador".
In **PEREIRA**, Joel Timóteo Ramos, Compêndio Jurídico da Sociedade da Informação, Quid Juris? Sociedade Editora, Lisboa, Outubro, 2004, p. 520, *apud* **SANTOS**, Ana Felícia Canilho. O Cibercrime: Desafios e Respostas do Direito. Dissertação de Mestrado para a obtenção do grau de Mestre em Direito, especialidade em Ciências Jurídicas. Universidade Autónoma de Lisboa. Setembro de 2015, p. 119.

[261] Nestes casos, o agente faz uma interferência nas frequências das linhas telefónicas (*blackboxing*), onde liga estes dispositivos eletrónicos (*blueboxing*), cujo efeito, de entre outros, é o impedimento total ou a diminuição da taxa devida à operadora de telecomunicações.
In **PEREIRA**, Joel Timóteo Ramos, *idem*, pp. 521 e 522, *apud* **SANTOS**, Ana Felícia Canilho, idem, p. 122.

[262] **SANTOS**, Ana Felícia Canilho, idem.

[263] O Escritório das Nações Unidas sobre Drogas e Crime ou Gabinete das Nações Unidas contra a Droga e o Crime (UNODC – United Nations Office on Drugs and Crime) discorda com a terminologia "pornografia infantil" considerando-a suave demais para o caso, e em vez desta propõe a expressão "abuso sexual infantil" e justifica a opção que apresenta nos seguintes termos:

> *"O termo material de abuso sexual infantil deve ser usado sobre pornografia infantil, porque o termo pornografia infantil minimiza a gravidade da ofensa. O que a pessoa está vendo não são atividades sexuais entre uma criança e um adulto, mas o abuso sexual de uma criança. No entanto, leis internacionais, regionais e nacionais usam o termo pornografia infantil em vez de material de abuso sexual infantil".*

No texto original em inglês pode ler-se

> *"The term child sexual abuse material should be used over child pornography because the term child pornography minimizes the seriousness of the offence. What the person is viewing, is not sexual activities between a child and an adult, but the sexual abuse of a child. Nevertheless, international, regional, and national laws use the term child pornography instead of child sexual abuse material".*

outros crimes relativos a conteúdo também deveriam ser incluídos nesta previsão legal, referimo-nos especificamente aos "atos de natureza racista ou xenófoba", cometidos por intermédio de sistemas informáticos, pois reclamam igualmente por censura penal[264].

3.2.3.1. Pornografia Infantil[265]

Pornografia infantil consta no art.º 184º compreendido na Secção III dos Crimes Contra a Autodeterminação Sexual[266], sendo esta secção por sua vez parte integrante do Capítulo IV que trata dos Crimes Sexuais e tem a seguinte redação

> **1. Quem:**
> **a) promover, facilitar ou permitir que menor de 16 anos participe de leitura obscena, assista a espectáculo, projecção de filmes, audição de gravações, exposição de fotografias ou observe ou examine instrumentos, pornográficos;**
> **b) utilizar menor de 16 anos em fotografia, filme ou gravação pornográficos;**
> **c) ceder a menor de 16 anos, escritos, fotografias, filmes, gravações ou instrumentos de natureza pornográfica é punido com pena de prisão até 2 anos.**
> **2. Quem:**

Disponível em https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/content-related-offences.html (Acedido aos 12-01-2020).

[264] Aliás, como previsto no **Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos,** adoptado em Estrasburgo em 28 de Janeiro de 2003, onde pode ler-se no seu art.º 2º nº 1 o seguinte:

> *Para efeitos do presente Protocolo, entende-se por:*
> *«**Material racista e xenófobo**» qualquer material escrito, imagem ou outra representação de ideias ou teorias que defende, promove ou incita ao ódio, à discriminação ou violência contra um qualquer indivíduo ou grupo de indivíduos em razão da raça, cor, ascendência, origem nacional ou étnica e religião, se for utilizado como pretexto para qualquer um destes elementos.*

Disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1481&tabela=leis&ficha=1&pagina=1 (Acedido aos 12-01-2020).

[265] O Código Penal Português no seu art.º 176º adota a designação "Pornografia de menores".
No Código Penal Brasileiro a punição do armazenamento; produção; troca e publicação de vídeos e imagens contendo pornografia infantojuvenil é punida nos art.ºs 241 e 241-A, do ECA (Estatuto da Criança e do Adolescente – Lei nº 8.069, de 13 de julho de 1990), neste mesmo estatuto incrimina-se o Assédio e aliciamento de crianças no art.º 241º-D.
O Código Penal Angolano ainda em vigor não prevê esse ilícito penal. No seu Capítulo IV dos Crimes Contra a Honestidade, a Secção II referente ao Atentado ao Pudor, Estupro Voluntário e Violação no seu art.º 394º somente temos o crime violação de menor de doze anos como sendo o único que incide diretamente sobre criança.

[266] A estrutura total desta secção é a seguinte:

> Artigo 179.º - (Abuso sexual de menor de 14 anos)
> Artigo 180.º- (Abuso sexual de menor de 16 anos)
> Artigo 181.º - (Abuso sexual de menor dependente)
> Artigo 182.º - (Lenocínio de menores)
> Artigo 183.º - (Tráfico sexual de menores)
> Artigo 184.º - (Pornografia infantil)

a) produzir pornografia infantil para ser difundida através de sistema informático; ou

b) difundir ou transmitir pornografia infantil através de um sistema informático é punido com pena de prisão até 3 anos.

3. Se, nos casos dos números anteriores, a vítima for menor de 14 anos, a pena é de prisão de 6 meses a 3 anos.

4. Se o agente fizer profissão dos actos descritos nos números anteriores ou os praticar com fim lucrativo, a pena é de prisão de 1 a 4 anos.

5. Para os efeitos do n.º 2, entende-se por:

a) pornografia infantil qualquer material pornográfico que represente visualmente um menor de 16 anos ou pessoa aparentando ser menor de 16 anos, envolvidos em comportamentos sexualmente explícitos;

b) sistema informático o definido na alínea b) do artigo 233.º[267].

A previsão deste ilícito penal visa, precisamente, a proteção das crianças e dos adolescentes contra a exploração e o abuso sexual muito potenciado pela disseminação de material pedo-pornográfico com conteúdos inadequados no ambiente virtual, muitos dos quais utilizados para fins comerciais.

O elemento objetivo do ilícito penal de pornografia infantil efetiva-se pela "promoção, facilitação ou permissão que menor de 16 anos participe de leitura obscena, assista a espectáculo, projecção de filmes, audição de gravações, exposição de fotografias ou observe ou examine instrumentos pornográficos"; pela utilização de "menor de 16 anos em fotografia, filme ou gravação pornográficos" ou pela cedência "a menor de 16 anos de escritos, fotografias, filmes, gravações ou instrumentos de natureza pornográfica".

Os elementos mencionados supra correspondem às infrações constantes no nº 1 e, atendendo a moldura penal para elas prevista, percebe-se claramente que o legislador ordinário entende que a ilicitude concretizada apenas pela "promoção, utilização ou cedência" de pornografia infantil é menos gravosa, por isso pune-a de forma mais branda – com a pena de prisão até 2 anos.

Outra parte integrante do elemento objetivo ligado à está infração tem que ver com a produção de "pornografia infantil para ser difundida através de sistema informático" e também a

[267] No art.º 233º define-se "Sistema informático" como sendo *qualquer dispositivo ou conjunto de dispositivos interconectados ou relacionados entre si que, isolada ou conjuntamente, asseguram, em execução de um programa, o tratamento automatizado de dados.*

difusão ou a transmissão de "pornografia infantil através de um sistema informático". Estas ações constantes do nº 2 são tidas como mais ofensivas por refletirem o aspeto da publicitação por via da reprodução de conteúdo ilegal e lesivo afeto a exploração sexual das crianças, daí serem punidas de forma mais severa que a prevista no nº 1 – com a pena de prisão até 3 anos.

Os números 3 e 4 apresentam outras circunstâncias agravantes. O primeiro agrava a pena de seis meses a três anos se a vítima da pornografia infantil tiver uma idade inferior a catorze anos. Já o segundo estabelece a pena privativa de liberdade entre um a quatro anos se o autor fizer da pornografia infantil sua profissão ou ainda se a praticar pretendendo obter lucro.

Finalmente temos as agravantes constantes no art.º 185º nº 1 que eleva a pena para *um terço nos seus limites mínimo e máximo, se a vítima for:*

> ***a) ascendente ou descendente, adoptante ou adoptado, parente ou afim até ao terceiro grau da linha colateral do agente ou se encontrar sob sua tutela ou curatela; ou***
> ***b) se encontrar numa relação de dependência hierárquica, económica ou de trabalho do agente e o crime for praticado com aproveitamento dessa relação.***

A pornografia infantil é definida no nº 5 al. a) e representa "qualquer material pornográfico que represente visualmente um menor de 16 anos ou pessoa aparentando ser menor de 16 anos, envolvidos em comportamentos sexualmente explícitos". O seu cometimento requer dolo.

A lei nada refere relativamente a punibilidade da tentativa pelo que se depreende que só haverá punição nos casos em que a pena exceder aos três anos de prisão (art.º 21º nº 1 ACP). Mas estando em questão a autodeterminação sexual de crianças nos seus mais diversos aspetos, achamos que a tentativa devia ser sempre punida em todos casos, tal como sucede na lei penal portuguesa (art.º 176º nº 8).

Compulsado o artigo também notamos que a lei não pune a posse[268][269] de material ligado ao abuso sexual infantil destinado ao uso pessoal, o que corroboramos pois no caso da simples

---

[268] Sobre a punição da posse o Tribunal da Relação de Coimbra no seu Acórdão de 02-04-2014 teve outro entendimento, tendo considerado que:

> 2. Preenche o crime de pornografia de menores o arguido que guarda no seu computador imagens de crianças do sexo masculino, nuas e em poses de exibição dos órgãos sexuais.

posse não há produção nem divulgação de conteúdo lascivo, pelo que se afasta a censura penal por não haver bem jurídico lesado, respeitando-se o princípio da materialidade penal, apesar de ser uma postura moralmente censurável.

Um protótipo da comercialização da exploração sexual de crianças "é a transmissão ao vivo de abuso sexual infantil, que envolve a transmissão e difusão em tempo real de abuso sexual infantil, pelo qual os espectadores podem ser passivos ou ativos (ou seja, eles podem assistir e/ou interagir com a vítima ou pedir para determinados atos serem realizados pela criança, sozinhos, ou para adultos realizarem certos atos contra uma criança)"[270].

Nestes crimes atrativos para pedófilos, frequentemente «os agentes entram nas salas de conversação (salas de chat) usando *nicknames* (nomes falsos) sugestivos, como "*like young*" ou "*pre-teen girls*", de modo a atrair um maior número de potenciais agentes (pedófilos). Apresentam-se como adolescentes, ou como adultos interessados em pornografia envolvendo crianças, esperando ser solicitados para conversa (chat)»[271].

Este tipo de crime não deve ser encarado com despreocupação e tem de merecer a atenção de todas autoridades[272] pois, para além da especificidade da população alvo (menores e logo seres mais vulneráveis), tem fortes laços com outros tipos de exploração, incluindo o tráfico de mulheres e crianças e o abuso sexual de crianças e jovens através da prostituição e do chamado turismo sexual.

3.3. Adequação dos tipos legais à realidade angolana

3.3.1. Considerações preliminares

As leis constantes no Código Penal visam estatuir e tipificar ações que são consideradas ilícitas, sendo por isso passíveis de cominação penal – por multa ou por privação de liberdade

---

Disponível em http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/4ab28f88e6e98b2880257cb7004ee59f?OpenDocument (Acedido aos 12-01-2020).

[269] Na verdade a punição da posse nos crimes de pornografia infantil representa uma problemática na doutrina e tem sido motivo de acesos debates. Para melhores desenvolvimentos leia-se **MORAIS**, Felipe Soares Tavares. Internet, Pornografia e Infância: a Criminalização da Posse de Pornografia Infantil. Revista do Ministério Público do Rio de Janeiro nº 64, Abr./Jun. 2017.

[270] Disponível em https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/content-related-offences.html (Acedido aos 12-01-2020).

[271] **PEREIRA**, Joel Timóteo Ramos, *idem*, pp. 511, *apud* **SANTOS**, Ana Felícia Canilho, idem, p. 151.

[272] Na mesma linha de pensamento Manuel Magriço chama alerta o seguinte:

> "Tendo presente que as crianças e os mais jovens sentem grande atratividade pelas novas tecnologias, a condução de um estudo que tem como sujeitos seres humanos nos primórdios da sua formação emocional, salvaguarda do futuro da sociedade, impõe que a abordagem do tema seja realizada com enorme delicadeza e se lhe reconheça primordial importância".

MAGRIÇO, Manuel Eduardo Aires. Dissertação para a obtenção de grau de mestre em Guerra da Informação da Academia Militar. A exploração sexual de crianças no Ciberespaço – aquisição e valoração de prova forense de natureza digital. Setembro de 2012. Disponível em https://comum.rcaap.pt/bitstream/10400.26/6822/1/DISSERTACAO-EXPLORACAO-SEXUAL-CRIANCAS-CIBERESPACO.pdf, p. 3, (Acedido aos 12-01-2020).

(prisão). E estas leis penais surgem em função da constatação – geralmente repetida – de comportamentos que ferem bens jurídicos relevantes, tais como o património, a privacidade, o sigilo das telecomunicações e o direito à liberdade e à segurança; regularmente beliscados pelo mau uso das TICs.

As leis que regulam os crimes informáticos incluídos no ACP têm precisamente essa pretensão. No entanto, passaremos a analisar se efetivamente do jeito que estes crimes estão configurados adequam-se ou não à realidade angolana.

Angola, apesar de ter ainda uma taxa de penetração da Internet relativamente baixa[273], tem registado uma melhoria na disponibilidade e facilidade de acesso. O próprio Estado tem desempenhado "o papel determinante na promoção da sociedade de informação"[274], promovendo a implementação das TICs[275][276] e sua regulação[277]. Atualmente verifica-se um crescendo dos crimes cometidos em ambiente digital devido fundamentalmente ao crescimento do uso da Internet. Esse crescimento estimulou os cidadãos a afluírem mais aos ciber-cafés, a migrarem os seus pagamentos para a via *online* usando os recursos disponíveis na *Internet banking* – criando-se deste modo ambientes propícios para ataques informáticos.

O aumento do uso da telefonia móvel[278] e o consequente recurso ao uso de *smartphones* é outro fator marcante.

Quanto à prestação de serviços o quadro é o seguinte: a empresa estatal de petróleo, Sonangol, detém três dos dezoito ISPs do país (MSTelcom[279], Nexus[280] e ACS[281]) e é acionista maioritária em outros dois, Unitel e Angola Cables[282]. A Unitel é o maior ISP do país[283], é

---

[273] De acordo com a The International Telecommunication Union (ITU) em 2017 esta taxa era de 14,34%, suplantando a taxa de 11% registada em 2000. Disponível em https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (Acedido aos 13-01-2020).

[274] Lê-se no preâmbulo da Lei 23/11 de 20 de Junho – a Lei das Comunicações Eletrónicas e dos Serviços da Informação. Disponível em https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjF2-u1od7pAhWORhUIHZdTCEUQFjAEegQIBhAB&url=http%3A%2F%2Fwww.mtti.gov.ao%2Fdownload.aspx%3Fid%3D1202%26tipo%3Dlegislacao&usg=AOvVaw2Q3Bt3c4xvog1qcHn0Sc7Y (Acedido aos 31-05-2020).

[275] Uma demonstração desta implementação das TICs pelo governo angolano foi o lançamento do Angosat 1 no dia 26 de Dezembro de 2017. Este foi mal sucedido, mas já se encontra desde Abril de 2018 a construção do Angosat-2 cuja previsão de lançamento está para esse ano. Disponível em https://pt.wikipedia.org/wiki/AngoSat-1 (Acedido aos 13-01-2020).

[276] Em Angola os serviços de TV Cabo é uma *joint venture* entre a Angola Telecom e a empresa portuguesa Visabeira. Russell Southwood, "The Case for 'Open Access' Communications Infrastructure in Africa: The SAT-3/WASC cable – Angola case study," Association for Progressive Communications, p. 12. Disponível em https://www.apc.org/fr/pubs/case-"open-access"-communications-infrastructure-africa-sat-3wasc-cable (Acedido aos 13-01-2020)

[277] Sobre esse assunto a Freedom House diz que "O Ministério dos Correios e Telecomunicações (MCT) é responsável pela supervisão do setor de TIC, enquanto o Instituto Angolano de Comunicações (INACOM), criado em 1999, atua como órgão regulador do setor. Reportando-se ao MCT, o INACOM determina os regulamentos e políticas do setor, define preços dos serviços de telecomunicações e emite licenças". Disponível em https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (Acedido aos 13-01-2020).

[278] Em 2018 a taxa de penetração da telefonia móvel foi de 43,13%, enquanto em 2000 era apenas de 16%. Disponível em https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (Acedido aos 13-01-2020).

[279] Disponível em https://www.mstelcom.co.ao (Acedido aos 13-01-2020).

[280] Disponível em https://empresas.verangola.net/show/13425 (Acedido aos 13-01-2020).

[281] Disponível em https://1635-ao.all.biz (Acedido aos 13-01-2020).

[282] Disponível em https://www.angolacables.co.ao (Acedido aos 13-01-2020).

[283] Sonangol's Telecom subsidiary, MSTelcom, discloses its fullownershipof Nexus and ACS in: *Sonangol Notícias*, "9° Aniversário da MSTelcom: Ligando o País e o Mundo," August 2008, n° 17, Sonangol.

igualmente a maior operadora móvel[284], tendo sido a primeira a operar com a tecnologia GSM no mercado angolano[285]. A empresa nacional de telecomunicações, Angola Telecom, é um dos principais acionistas da Angola Cables, com 51%, e fornece seus próprios serviços de Internet[286].

Nas fraudes com computadores, nota-se que a maior parte das burlas informáticas relacionam-se a pagamentos e transações feitas em ATM.

Também digno de menção foi o surgimento de novas universidades públicas e institutos superiores privados que albergam nos seus centros faculdades com cursos ligados às TICs, mormente Engenharia Informática e Ciências da Computação. Os alunos destas instituições desenvolvem capacidades e conhecimentos muito profundos sobre a informática, o que pode ser usado como potencial delituoso. Por esse facto, a polícia angolana, como forma de sensibilização, tem feito palestras nestas instituições[287].

Apesar de tudo que foi acima referido, a realidade delituosa angolana ainda não é alarmante, se bem que especialistas alertam para uma tendência de aumento de ataques informáticos[288].

A escassez de estudos relacionados com a matéria impede-nos de termos dados estatísticos concretos para podermos fazer uma avaliação mais consistente.

Uma dificuldade de investigação é acrescida pela opção, principalmente entre as empresas e bancos, em não divulgar os ataques informáticos que sofram para não verem beliscada a sua boa imagem a nível do mercado, impedindo assim a fuga de clientes para outras instituições que se revelem informaticamente mais seguras.

3.3.2. Crimes não previstos no Anteprojeto de Código Penal

3.3.2.1. O acesso ilícito e a interceção ilegal

Focando-nos na adequação dos tipos penais à realidade angolana, primeiramente solta-nos à vista a não inclusão no ACP do crime de acesso ilegal, facto motivador de todos os demais crimes informáticos.

---

[284] Disponível em http://www.unitel.ao/servlet/web/A-Unitel (Acedido aos 13-01-2020).
Existem apenas duas operadoras de telefonia móvel, a Unitel e a Movicel.
[285] Disponível em https://pt.wikipedia.org/wiki/Unitel (Acedido aos 13-01-2020).
[286] Freedom on the Net 2017 – Angola. Disponível em https://www.refworld.org/docid/5a547d6e4.html (Acedido aos 13-01-2020).
[287] Disponível em https://www.menosfios.com/policia-nacional-leva-criminalidade-informatica-debate-hoje-as-19h-na-ugs/ (Acedido aos 14-01-2020).
[288] Disponível em http://www.redeangola.info/empresas-alertam-para-aumento-de-ataques-online-no-pais/ (Acedido aos 14-01-2020).

É um crime de perigo abstrato que representa "uma barreira para evitar a prática de outros ilícitos de maior gravidade"[289], acautela o "furto de informação"[290] e pressupõe uma atuação sem autorização, tendo como *ex libris* do seu cometimento o *hacking*[291].

Pela não previsão deste ilícito, podemos inferir que com base no anteprojeto, o simples ato de aceder a um sistema ou rede informática sem autorização não constitui por si só um crime. Só haverá responsabilização criminal se o acesso sem autorização for a dados que "contenham informações individualmente identificáveis" (art.º 212º nº 1 al. b)), pelo que entendemos que este diploma pune unicamente *uma forma qualificada de acesso ilegítimo*.

Por mais que legitimemos a necessidade da inclusão do crime de acesso ilegítimo e reconheçamos que se encontra parcialmente consumido no teor do crime de devassa por meio de informática, acreditamos que o tratamento dos crimes digitais num Código Penal dificultou o legislador fazer um enquadramento deste ilícito num capítulo específico.

Os crimes previstos no ACP estão repartidos por títulos, sendo respetivamente contra:

- As pessoas;
- A família;
- A fé pública;
- A segurança coletiva;
- O estado;
- A paz e a comunidade internacional;
- O património; e
- Contra o consumidor e o mercado.

Em nenhum desses títulos é enquadrável o acesso ilegal por ser um crime puramente informático.

Mas se atendermos ao bem jurídico tutelado – a segurança do sistema informático, ou seja, a proteção do designado "domicílio informático"[292] – notamos que tem alguma semelhança

[289] Acórdão do Tribunal da Relação da Guarda de 17 de Novembro de 2008, disponível no CJ, Ano XXXIII, Tomo V/2008, p. 289 e 292, sumário de António Geraldes (Refª CJ online 7922/2008).
[290] **MACEDO**, João Carlos Cruz Barbosa de, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, Coimbra Editora, 2009, p. 246.
[291] Idem.
[292] Acórdão do TRC de 15-10-2008. Disponível em http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/ae4145b5e5a62059802574f70058c7fe?OpenDocument (Acedido aos 14-01-2020).

com a violação da vida privada por via da "introdução em casa alheia", por isso essa lacuna seria suprível com a inclusão do crime de acesso ilegítimo no Título I dos crimes contra as pessoas, especificamente no Capítulo VII dos *crimes contra a reserva da vida privada.*

É neste capítulo onde se encontra prevista a "devassa por meio de informática" e outros ilícitos penais parecidos, como a já citada introdução em casa alheia e as violações de correspondência e das telecomunicações (art.ºs 209º, 212º, 213º e 214º).

Uma outra eventualidade da não inserção deste crime – e que já referimos antes – é a previsão de um ilícito similar no art.º 56º do LPDP, precisamente designado de acesso indevido. Na verdade, é enorme a similitude nas redações destes dois tipos penais, todavia diferenciam-se particularmente nos dados que são objeto de tratamento, ou seja, no crime de acesso ilegítimo "pune-se o acesso sem permissão legal ou autorização a um sistema informático, enquanto nos crimes de acesso indevido aos dados, ... se pune o acesso não autorizado a dados pessoais"[293]. Entendemos que o legislador quis, em parte, evitar a dupla incriminação da mesma ilicitude[294], isto é, o *bis in idem.*

O segundo crime não incluído no ACP e que ao nosso ver também reclama inclusão é a intecepção ilegítima, e tal como as infrações que se prendem com a violação da correspondência e de telecomunicações dos art.ºs 213º e 214º respetivamente, tem previsão constitucional no art.º 34º (CRA).

Normalmente conhecido por "espionagem informática", a interceção ilegítima "o seu maior potencial de aplicação prático é nas comunicações pela *Internet* (chats, emails, ...) "[295].

Este ilícito muito parecido com o acesso ilegítimo[296] e que "visa punir a intercepção de comunicações no interior de um sistema informático"[297], pelas afinidades que tem com os crimes de violação de correspondência e o de violação de telecomunicações referidos *supra* e

---

[293] Pedro Verdelho entende que ambos os ilícitos têm uma "relação de especialidade" visto que se dirigem à confidencialidade que se impõe no tratamento de dados pessoais. **VERDELHO**, Pedro. Comentário das Leis Penais Extravagantes. Organizado por Paulo Pinto de Albuquerque e José Branco. Vol. 1, Universidade Católica Editora, 2010, p. 492.

[294] Sobre a dupla previsão deste ilícito em dois diplomas diferentes temos o exemplo português que criminaliza o **acesso ilegítimo** no art.º 6º da Lei nº 109/2009 de 15 de Setembro do Cibercrime e também o **acesso indevido aos dados** no art.º 53º da Lei 59/2019 de 8 de Agosto que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[295] **MACEDO**, João Carlos Cruz Barbosa de, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, Coimbra Editora, 2009, p. 248.

[296] Ambos ancoram-se na ilegitimidade (falta de autorização) e inserem-se no mais amplo modo de espionagem informática. **MACEDO**, João Carlos Cruz Barbosa de. Ibidem, Idem.

[297] **VERDELHO**, Pedro. Comentário das Leis Penais Extravagantes. Op. cit, p. 517.

atendendo que o bem jurídico protegido abrange a "privacidade na comunicação de dados"[298], também o enquadraríamos nos crimes contra a reserva da vida privada.

Nos *modus operandi* que levam a concretização dessa infração temos as técnicas de interceção de comunicações eletrónicas, tais como a chamada *sniffing*[299].

3.3.2.2. A Sabotagem informática[300]

A terceira e a mais gravosa constatação – e por isso merecerá uma profunda análise da nossa parte – é a não introdução pelo legislador no texto do ACP de um delito que sancione a interferência em sistemas ou, como é designado em várias legislações, a sabotagem informática. Achamos gravosa porque os ataques informáticos mais sonantes até aqui registados em Angola enquadram-se propriamente neste ilícito penal, e tiveram repercussões muito sentidas na espera pública.

O art.º 399º do ACP que regula o crime de dano informático[301] faz uma previsão parcial do crime de sabotagem, na parte referente a causar "dano à integridade do sistema". Divisamos que entre os dois ilícitos existe uma certa "*«zona de coincidência»* ao nível de certo tipo de dados a tutelar."[302]

O primeiro ataque de grandes proporções registou-se em 30 de Março de 2016, dois dias após dezassete jovens ativistas, incluindo o rapper luso angolano Henrique Luaty da Silva Beirão, terem sido sentenciados por alegado plano de rebelião.

O ataque foi reivindicado pelo "ramo português do coletivo de *hackers* Anonymous"[303] que afirmou ter fechado "cerca de 20 *sites* do governo angolano em retaliação pelo encarceramento"[304] dos jovens, embora não tenha havido qualquer reação institucional sobre o ataque cibernético sofrido.

---

[298] Ibidem, Idem, p. 518.
[299] *Sniffing* é "a acção de capturar informações destinadas a uma máquina". **OLIVEIRA**, Wilson. Técnicas para Hackers II – Soluções para Segurança. Edições Centro Atlântico, Abril de 2003, p. 315.
[300] A sabotagem informática é o crime virtual, em regra, mais gravemente punido por ser uma autêntica arma eletrónica.
[301] Para exemplificar a proximidade entre os crimes de danos informático e sabotagem informática notemos que ambos apresentam como forma usual de perpetração a introdução de vírus. **SANTOS**, Paulo; **BESSA**, Ricardo e **PIMENTEL**, Carlos, op. cit, p. 6.
[302] **VENÂNCIO**, Pedro Dias. Lei do Cibercrime, idem, p. 49.
[303] Disponível em https://www.thestar.com.my/tech/tech-news/2016/03/31/anonymous-cyberattack-hits-angola-govt-after-activists-jailed/ (Acedido aos 14-01-2020).
[304] Idem

Em esclarecimento difundido na sua "página do Facebook no dia 29 de Março de 2016, o grupo Anonymous Portugal listou os *sites*[305] do governo que afirmou ter atacado"[306], não estando nenhum dos *sites* acessível no dia 30 de Março de 2016.

No dia 5 de Junho de 2019, a maior empresa pública de Angola – A Sociedade Nacional de Combustíveis (Sonangol) – sofreu um gravíssimo ataque informático tendo ficado completamente paralisada.[307] Este ataque coincidiu com a realização em Luanda da conferência internacional "Angola Oil & Gas" que reuniu mais de quinhentos gestores destas duas áreas, e contou com a presença do presidente angolano João Manuel Gonçalves Lourenço[308].

Atingiu os sistemas informáticos da empresa, causou a destruição e o desaparecimento de documentos internos, nomeadamente financeiros e contabilísticos e ocorreu meses após a fuga de informação da petrolífera, mas antes da divulgação pelo consórcio internacional de jornalistas do chamado "Luanda Leaks"[309].

Os *hackers* tiveram acesso a mais de sete mil computadores, conseguindo "informação privilegiada" relacionada não só à empresa como aos seus clientes tendo atingido as infraestruturas ligadas a DTI (Direção de Tecnologia de Informação), o que motivou a empresa a tomar medidas preventivas visando a proteção dos alvos mais críticos[310].

Uma dessas medidas foi a de fazer "o *shutdown* dos sistemas informáticos e da rede de comunicações"[311] da empresa e a outra foi restabelecer o software de gestão de *e-mail* (O Outlook). Os sistemas só re-estabeleceram depois da intervenção dos técnicos.

O portal Maka Angola ao fazer investigações sobre o ataque sofrido pela Sonangol, dentre as constatações que efetuou destacamos as seguintes[312]:

a) A Sonangol funcionava há mais de um ano sem um antivírus na sua rede de computadores, porque o Conselho de Administração (CA) não autorizava o

[305] A lista total dos *sites* afetados podem ser encontrada em https://www.google.pt/search?q=cyber+attack+angolan+government&client=opera&sa=N&biw=1496&bih=722&tbm=isch&source=iu&ictx=1&fir=8J8-AOPYpnmKPM%253A%252C_4JhB6R6UQNq_M%252C_&vet=1&usg=AI4_-kRQpupoKbkJWx9UPbddjSsFxiTuiQ&ved=2ahUKEwiiIPyxrLnjAhXmA2MBHSE-DYg4ChD1ATADegQIBhAE#imgrc=8J8-AOPYpnmKPM:&vet=1 (Acedido aos 14-01-2020).

[306] Disponível em https://clubofmozambique.com/news/anonymous-cyber-attack-shuts-down-20-angolan-government-websites-after-activists-jailed/ (Acedido aos 14-01-2020).

[307] Disponível em https://www.jornaldenegocios.pt/economia/mundo/africa/angola/detalhe/sonangol-foi-alvo-de-ataque-informatico (Acedido aos 14-01-2020).

[308] Disponível em http://www.novojornal.co.ao/economia/interior/sonangol-ataque-informatico-obriga-a-medidas-extraordinarias-para-processar-salarios-de-junho-73307.html (Acedido aos 14-01-2020).

[309] Disponível em http://tpa.sapo.ao/noticias/economia/inacom-alerta-para-ataques-as-redes-de-telefonia-movel (Acedido aos 22-06-2020).

[310] Disponível em https://observador.pt/2019/06/07/imprensa-angolana-da-conta-de-ataque-cibernetico-a-petrolifera-sonangol/ (Acedido aos 14-01-2020).

[311] Disponível em https://www.angop.ao/angola/en_us/noticias/economia/2019/5/23/Oil-company-Sonangol-targeted-cyber-attack,9f7b89d6-bb91-42c3-b886-93cdb3691e3a.html (Acedido aos 14-01-2020).

[312] Ataque Cibernético à Sonangol, Rafael Marques de Morais, 19 de Agosto de 2019. Disponível em https://www.makaangola.org/2019/08/ataque-cibernetico-a-sonangol/ (Acedido aos 15-01-2020).

pagamento de renovação da licença de uso do McAfee, que são menos de 200 mil dólares por ano.

b) O ataque indicava que na codificação do vírus vinha integrado o código da máquina de servidores da Sonangol. Pela complexidade do vírus, o mesmo só poderia ter sido introduzido por estrangeiros.

c) O vírus destinava-se a destruir a base de dados da Sonangol e, com isso, efectuar a "queima de arquivos" da empresa. Todavia, atingiu apenas a rede e eliminou toda a informação nela constante, nomeadamente pastas partilhadas, dados, documentos e aplicativos.

d) No mesmo dia do ataque, o CA da Sonangol solicitou de emergência os serviços da empresa angolana TIS Tech[313] para neutralizar o ataque cibernético, identificado nesse dia pelos técnicos da empresa como devastador. Essa empresa chegou ao local quatro horas depois, efetuando a instalação de um antivírus de origem israelita, o Sentinel One[314], e outros aplicativos de segurança como o Carbon Black[315]. Também procedeu a customizações nas ferramentas de segurança existentes, como o Checkpoint.

e) Especialistas apontam para o perigo que o Sentinel One representa, uma vez que está publicado numa nuvem (*cloud*). "Isto significa, em termos de segurança, que toda a informação da Sonangol fica numa nuvem, algures, sem controlo da própria empresa. Essa informação deveria estar armazenada a nível local".

f) Durante três dias ininterruptos, as equipas da TIS Tech e da Sonangol trabalharam rotativamente na recuperação do sistema e na estabilização da infraestrutura de tecnologias de informação da petrolífera. Os dois dias seguintes serviram para repor alguns serviços essenciais.

[313] Para mais informações sobre essa empresa aceda-se http://www.tistech.co.ao/home (Acedido aos 15-01-2020).
[314] Cuja página oficial localiza-se em https://www.sentinelone.com (Acedido aos 15-01-2020).
[315] Mais esclarecimentos veja-se https://en.wikipedia.org/wiki/Carbon_Black_(company) (Acedido aos 15-01-2020).

g) Foi necessário um mês inteiro para repor o sistema operacional da empresa.

Esses ataques realçam bem a necessidade do legislador angolano aprovar urgentemente o ACP bem como a necessidade da inclusão do tipo penal de sabotagem informática porque em ambos casos registou-se que a intenção dos atacantes foi a dentre outras "entravar, impedir, interromper ou perturbar gravemente o funcionamento" do sistema informático.

As avaliações feitas pelos especialistas, num e noutro caso, concluíram ainda que os ataques foram perpetrados a partir do exterior do país.

Acreditamos que o primeiro ataque despertou ainda mais o legislador ordinário e impulsionou a Assembleia Nacional angolana a aprovar um ano depois a Lei nº 7/2017 de 16 de Fevereiro (Lei de Protecção das Redes e Sistemas Informáticos)[316][317].

Não menos importante, mas também digno de menção por poder configurar o ilícito de sabotagem informática e pela sofisticação do ataque, foi o seguinte estudo:

- ✓ De acordo a CNET[318], anos atrás, o blog de notícias críticas Maka Angola, do jornalista Rafael Marques de Morais, foi alvo de ataques repetidos de DDoS, obrigando-o a receber assistência técnica do Project Shield (Google) da Jigsaw[319], que protege *sites* de poderosos ataques técnicos contra os ataques DDoS[320][321]. O mesmo jornalista investigativo também tinha sido frequentemente alvo de violência técnica via *malware*

[316] Disponível em https://animalexdominis.files.wordpress.com/2018/03/proteccc3a7c3a3o-das-redesesistemas-informc3a1ticos-2017.pdf (Acedido aos 15-01-2020). No art.º 2º relativo ao âmbito pode ler-se no nº 1 que "A presente lei aplica-se ao ciberespaço da República de Angola, contra qualquer acto de ataque, roubo informático, ciber-ataque e incidentes informáticos".

[317] Para mais considerações sobre a aprovação desta lei leia-se https://www.menosfios.com/lei-os-ciberataques-ja-esta-vigor-angola/ (Acedido aos 14-01-2020).

[318] É um *site* de mídia americano que publica críticas, notícias, artigos, blogs, podcasts e vídeos sobre tecnologia e eletrónicos de consumo em todo o mundo. Disponível em https://en.wikipedia.org/wiki/CNET (Acedido aos 14-01-2020).

[319] O *Project Shield* é um serviço anti-distribuído de negação de serviço (anti-DDoS) oferecido pela Jigsaw, uma subsidiária da empresa-mãe do Google, Alphabet Inc., para *sites* que possuem "mídia, eleições e conteúdo relacionado a direitos humanos".
Este projeto tem ajudado jornalistas, ativistas e outros de botnets de DVRs invadidos e câmaras de segurança usadas para inundar *sites* com dados. Disponível em https://en.wikipedia.org/wiki/Project_Shield (Acedido aos 14-01-2020).

[320] Alfred **NG**, "Google's Project Shield defends free speech from botnet scourge," CNET, September 29, 2016. Disponível em https://www.cnet.com/news/google-project-shield-botnet-distributed-denial-of-service-attack-ddos-brian-krebs/ (Acedido aos 13-01-2020).

[321] **Botnets IoT** são a moderna metodologia de ataques DDoS, no qual os atacantes usam como ferramentas os "DVRs, câmaras habilitadas para IP, equipamento de cabo doméstico e muitos outros dispositivos conectados à IoT". Ainda o autor alerta que "Pior, as motivações dos atacantes nem sempre afetam a disponibilidade dos serviços, mas distraem a equipe de TI para acender um incêndio ali enquanto o crime real está acontecendo aqui. Impedir a resposta a outros ataques parece ser uma tática sólida para os criminosos; Neustar disse que os clientes relataram encontrar malware, dados perdidos ou propriedade intelectual e roubo financeiro após um ataque de DDoS". IoT Botnets Are The New Normal of DDoS Attacks. **MIMOSO**, Michael. October 5, 2016. Disponível em https://threatpost.com/iot-botnets-are-the-new-normal-of-ddos-attacks/121093/ (Acedido aos 14-01-2020).

personalizado implantado em seu *laptop* pessoal[322]. Desde então, ele recebe assistência de organizações sem fins lucrativos de segurança digital para proteger suas atividades *online*.

Um ataque distribuído de negação de serviço, como o supra mencionado, pode preencher o crime de sabotagem informática. Ainda preenchem esse ilícito a introdução de vírus, o *spamming*[323][324] e a designada *mail bomb*[325].

Mas em que parte do ACP sugeríamos ao legislador enquadrar esse crime?

No Título V temos os Crimes Contra o Estado. O seu Capítulo I aborda os Crimes Contra a Segurança do Estado e contém o art.º 316º que prevê o crime de sabotagem como subparte da Secção IV dos Crimes contra a Realização do Estado.

Apesar de reconhecermos que o ideal seria mesmo ter a sabotagem informática numa lei do cibercrime, achamos que na impossibilidade de tal suceder é aconselhável ali enquadrar, aliás nota-se alguma semelhança[326] com parte do enunciado do nº 1 art.º 316º que sanciona quem "destruir, danificar, impedir o normal e eficaz funcionamento de vias de comunicação, de transmissão".

Deveras, a sabotagem informática impede o regular e o eficiente funcionamento dos sistemas informáticos assim como de toda a comunicação de dados processada à distância.

3.3.2.3. Infrações relacionadas com a violação do direito de autor e dos direitos conexos

[322] There is a detailed account of how the malware was discovered during an international conference. See: **MOYNIHAN**, Michael "Hackers are Spying on You: Inside the World of Digital Espionage," Newsweek, May 29, 2013. Disponível em https://www.newsweek.com/2013/05/29/hackers-are-spying-you-inside-world-digital-espionage-237478.html (Acedido aos 14-01-2020).

[323] *Spamming* compreende o "*envio envio intencional de um número elevado da mesma mensagem ou de diversas mensagens para um determinado endereço electrónico por forma a sobrecarregar ou entupir o servidor do sistema informático*", pode representar a sabotagem informática por interferir "no sistema de informação, actuando com a intenção de embaraçar o tráfego de dados ou perturbar o seu funcionamento informático ou de comunicação à distância". **SANTOS**, Paulo; **PIMENTEL**, Carlos e **BESSA**, Ricardo. Cyberwar. FCA. 2008, p. 13 e 14.

[324] Constitui sabotagem informática porque "*o spammer não deseja apenas "informar" sobre determinado evento; ele pretende perturbar o próprio sistema informático e, por isso, envia um número elevado da mesma mensagem ou de diversas mensagens visando entravar e perturbar os servidores*". **PEREIRA**, Joel Timóteo Ramos. Direito da Internet e Comércio Electrónico, Quid Juris, Lisboa, 2002, p. 251 e 252.

[325] **MARQUES**, Garcia e **MARTINS,** Lourenço. Direito da Informática, 2.ª Refundida e Actualizada ed., Almedina, Coimbra, 2006, p. 693.

[326] Para melhor esclarecimento sobre o paralelismo entre a sabotagem informática e a sabotagem regulada no CP confira-se Pedro Dias Venâncio, Lei do Cibercrime, p. 54.

A previsão de crimes contra os direitos de autor e direitos conexos é praticamente nula no ACP[327]. A infração de reprodução ilegítima de programa[328][329] (ou *software*) – ou de base de dados que sejam criativas – não está prevista[330].

No entanto, em 29 de Dezembro 2011, o Ministério das Telecomunicações e Tecnologias de Informação tinha apresentado a versão final do Projecto de Regulamento das Tecnologias e dos Serviços da Sociedade da Informação[331]. Nele constavam dois artigos (62º e 64º) que apresentavam a proteção jurídica que deve ser dada aos programas de computador[332] e às bases de dados[333], mas considerava apenas como contravenção a violação dos mesmos, sancionado com multas (art.º 90º e 91º).

Entretanto, para além do projeto fazer menção destes dois entes juridicamente relevantes (programas de computador e base de dados), definia também de forma pioneira expressões muito significativas no âmbito das TICs, como o documento eletrónico, assinatura eletrónica e nomes de domínio (art.º 4º al. a), p) e ee)).

Incompreensivelmente, este projeto, que apresenta uma temática tão importante, até ao momento não foi aprovado e desconhecemos as razões desse triste facto.

A título de evolução legislativa, no que diz respeito a temática, em Angola inicialmente tínhamos em vigor a lei nº 4/90, de 10 de Março, designada Lei dos Direitos de Autor. Nela as Violações do Direito do Autor[334] era o tema do Capítulo VII cujo art.º 31º referente a violação dos

---

[327] Para além dessa não previsão legal, importa frisar que não existe em Angola um Código que verse unicamente sobre os Direitos de Autor e os Direitos Conexos nem um Código de Propriedade Intelectual.

[328] A previsão deste ilícito seria de relevo, pois muitos processos que levam à responsabilização de pessoas coletivas ou equiparadas relacionam-se com o cometimento desta infração, isto é, a pessoa singular que infringe a lei age em representação e no interesse na pessoa coletiva. Pode comprovar-se por exemplo o Acórdão do Tribunal da Relação do Porto de 11-04-2007, Proc. 0616655, relator Joaquim Gomes, disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/df9b304aeb07b795802572c00049ad30?OpenDocument (Acedido aos 29-02-2020).

[329] Na lei portuguesa este delito está previsto no art.º 8º da lei 109/2009.
Embora defendamos a inclusão deste ilícito no ACP, na verdade este crime não está previsto na CB nem na Decisão-Quadro 2005/222/JAI, do Conselho da Europa de 24 de Fevereiro de 2005. *Ab initio*, a CB "não regulamenta expressamente a matéria do direito de autor e direitos conexos".
Assim, "a inspiração mais remota" desta previsão encontra-se na Recomendação nº 9(89) do Conselho da Europa e concordamos que "parece revelar uma perspectiva maximalista da abordagem penal da problemática do direito de autor sobre programas de computador". Para mais desenvolvimentos pode ler-se **VERDELHO**, Pedro. Comentário das Leis Penais Extravagantes. Idem, p. 520-523.

[330] O Decreto Presidencial nº 20/11 de 22 de Julho menciona que "os programas de computador que tiverem caráter criativo" e "as bases de dados" são protegidos pelo direito de autor (artigos 62º nº 1 e 70º nº 1).

[331] Disponível em http://www.governo.gov.ao/VerLegislacao.aspx?id=459 (Acedido aos 29-02-2020).

[332] Programa de computador é o "conjunto de instruções (*software*) usado directa ou indirectamente num computador, tendo em vista a obtenção de determinado resultado, incluindo o material de concepção" (art.º 4º al. x)).

[333] Na al. e) do art.º 4º definia Bases de Dados nos seguintes termos.

> "as colectâneas de obras, dados ou outros elementos independentes, dispostos de modo sistemático ou metódico e susceptíveis de acesso individual por meios electrónicos ou outros."

[334] A discussão dos aspetos penais dos direitos de autor e direitos conexos é realmente uma problemática, e esta dificuldade é verificada até a nível da jurisprudência. Por exemplo, o acórdão uniformizador nº 15/2013 no Tribunal Supremo português referente ao crime de usurpação, apresenta um conceito de *comunicação ao público de obra* incompatível com o apresentado na jurisprudência do Tribunal de Justiça da União Europeia. *Vide* o Acórdão da Relação de Coimbra de 28 de junho de 2017. Disponível em http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/03f18004fd3cc9f48025815200495ae7?OpenDocument (Acedido aos 11-05-2020).

direitos patrimoniais que previa os crimes de usurpação e de contrafação ou plágio nos números 1 e 2 respetivamente.

A lei nº 4/90 de 10 de Março estabelecia ainda penas de prisão e de multa bem como punia a simples negligência (art.º 32º). Para os crimes nela estatuídos o procedimento criminal não dependia de participação[335], sendo por isso crimes públicos, excetuando aqueles delitos que incidiam sobre obras que caíram no domínio público (art.º 35º), porém o procedimento criminal e a responsabilidade civil apesar de poderem ser exercidas numa "ação conjunta" eram independentes[336] (art.º 36º).

Esta lei surgiu num contexto em que as TICs quase que não se faziam sentir no país[337] e por isso não regulava os programas de computador, também por essa razão entendemos que a definição de reprodução da al. i) do art.º 4º não abrangia os *softwares*.

Com o passar dos anos foi se notando que a informática potenciava a criminalidade ligada à pirataria e por isso urgia dar cobertura e proteção penal aos direitos de propriedade intelectual relacionados com os programas de computador e bases de dados, para que se evitasse a reprodução, a divulgação ou a comunicação ao público, a venda, a transformação e a circulação dos mesmos sem a devida autorização.

Pela clara necessidade que houve de serem melhor protegidos os direitos inerentes à propriedade intelectual – destacando-se aqueles que recaem sobre os "criadores das novas tecnologias de informação e comunicação" – em substituição da lei citada *supra* aprovou-se a lei nº 15/2014 de 31 de Julho, agora com uma designação mais abrangente (Lei dos Direitos de Autor e Conexos).

Quer dizer que esta nova lei, diferentemente da anterior, já protege as obras que incidam ou sejam produzidas por meio das TICs. No leque dessas obras protegidas temos os

---

[335] O mesmo sucede na legislação portuguesa, mas excetua os crimes que dizem respeito a violação do direito moral (art.º 200º do CDADC).
[336] *Art.º 203.º do CDADC português estabelece a* Responsabilidade Civil de forma semelhante nos seguintes termos:

> "A responsabilidade civil emergente da violação dos direitos previstos neste Código é independente do procedimento criminal a que esta dê origem, podendo contudo ser exercida em conjunto com a acção criminal".

[337] Para reforçar a compreensão da evolução que se operou em Angola atente-se que o Ministério de tutela designava-se na altura *Ministério dos Correios e das Telecomunicações*, depois passou a designa-se *Ministério das Telecomunicações e Tecnologias de Informação.* Esta alteração operou-se em 2008. Disponível em http://www.mtti.gov.ao/Institucionais/Historico.aspx (Acedido aos 11-05-2020).
Recentemente esse ministério passou a integrar o da Comunicação Social e tomou a designação de *Ministério das Telecomunicações e Tecnologias de Informação e Comunicação Social.* Essa notícia consta de Jornal de Angola, é intitulada "Ministério da Comunicação Social fundido ao das Telecomunicações" e escrita por César Esteves em 3 de Abril, 2020. Disponível em http://jornaldeangola.sapo.ao/politica/ministerio-da-comunicacao-social-fundido-ao-das-telecomunicacoes (Acedido aos 20-07-2020) e cujo estatuto orgânico é consultável em https://www.governo.gov.ao/VerLegislacao.aspx?id=2430 (Acedido aos 20-07-2020).

programas de computador[338][339], ligados ou não em rede que frequentemente são objeto de reprodução[340] ilícita.

A lei nº 15/2014 de 31 de Julho é exígua no que tange a previsões penais[341]. No Capítulo IV relativo a violação, proteção e defesa dos direitos de autor e conexos notamos que as medidas judiciais daí decorrentes são, em regra, efetivadas por ações cíveis, fazendo recurso ao Código de Processo Civil (art.º 80º nº 1), ou seja, essas medidas são *grosso modo* de responsabilidade civil (art.º 81º) e por isso sancionadas com multas (art.º 89º).

O art.º 83º que versa sobre a responsabilização criminal dos infratores remete o regime sancionatório ao CP e ao CPP, todavia o ACP não prevê delito algum relacionado aos direitos de autor e conexos, constatação que nos surpreende negativamente.

Espanta-nos ainda o estranho facto da lei não considerar expressamente a usurpação[342] como sendo um crime, nem como deve ser objeto de responsabilização civil, limitando-se o art.º 84º a defini-la e a elencar as formas da sua perpetração. Na verdade, a contrafação[343] e o plágio são os únicos crimes aí previstos no art.º 85º números 1 e 2. Este artigo incompreensivelmente inclui no nº 4 o tratamento a dar aos bens usurpados mesmo não tendo na sua epígrafe *Usurpação* mas sim *Contrafacção e Plágio.*

Julgamos ser estranha a evolução legislativa processada em Angola no âmbito dos direitos de autor e conexos, pois que a lei 15/2014 de 16 de Julho, que revogou a lei 4/90 de 10 de Março, ao despenalizar a usurpação e a não prever outras medidas penais expectáveis[344], procedeu neste aspeto um retrocesso legiferante e por isso reclama por emendas ou alterações urgentes.

Dito isto, entendemos que dado ao facto dos direitos de autor e direitos conexos representarem um direito previsto constitucionalmente para os criadores intelectuais (art.º 42º da CRA), o ACP deveria prever categoricamente a criminalização de ações de usurpação, plágio,

---

[338] O programa de computador é definido no art.º 3º nº 22 desta lei da seguinte forma:

> *"O conjunto de instruções por palavras, códigos, esquemas ou por qualquer outra forma, capaz de, quando incorporado num suporte legível por máquina, fazer com que uma máquina com a capacidade de tratamento de informação consiga indicar, realizar ou completar uma função particular, uma tarefa ou um resultado".*

[339] Devem ser respeitadas as exceções à reprodução de programas de computador constantes no art.º 55º conjugado com o art.º 51º nº 1 al. d) e nº 2 al. d).

[340] Contrariamente a lei nº 4/90 de 10 de Março, a sua sucedânea (lei nº 15/2014 de 31 de Julho) na definição que apresenta de reprodução (art.º 3º nº 24) nela se incluem as feitas com recurso a meios informáticos, tal como acontece na reprodução de programas de computador.

[341] O mesmo já não acontece com o Código do Direito de Autor e dos Direitos Conexos (CDADC) português (Decreto-Lei n.º 63/85 de 03-14) que prevê para os crimes aí estabelecidos penas de prisão de até três anos e multa de 150 a 250 dias, para além de punir a negligência e não permitir a suspensão da pena nos casos de reincidência (art.º 197º).

[342] No CDADC português o crime de usurpação está previsto no art.º 195º.

[343] Consta no art.º 196º do CDADC português.

[344] Como a penalização da violação dos direitos morais e do aproveitamento de obra usurpada (art.ºs 198º e 199º do CDADC português).

contrafação de obras e violação de direitos morais que aconteçam com recurso às TICs, incluindo nestas as bases de dados protegidas.

Ademais, a não previsão deste ilícito pode ser também compreendida pelo facto de não existir em Angola diplomas que versam unicamente sobre os regimes jurídicos dos programas de computador[345] e das bases de dados[346].

No entanto, pelo crescimento do uso da informática seria aconselhável o legislador agir por antecipação, fazendo essa previsão legal ou reconsiderar o conteúdo do Projecto de Regulamento das Tecnologias e dos Serviços da Sociedade da Informação.

O local adequado para inserção dos crimes ligados aos direitos de autor e conexos é no Capítulo II dos Crimes Contra a Propriedade, por ser parte integrante do Título VII dos Crimes Contra o Património, afinal os programas de computador e as bases de dados são na verdade património dos seus legítimos produtores.

3.4. Comparação com a Convenção de Budapeste

No presente sub-tema faremos uma confrontação entre os crimes informáticos estatuídos no ACP e os previstos na CB. Dentre os conteúdos abordados na CB[347] interessa-nos apenas a Secção 1 do Capítulo II, ou seja, as medidas que devem ser adotadas a nível de cada estado no âmbito do Direito Penal Material.

Nesse aspeto preciso, a convenção pretende estabelecer modelos normativos essenciais e comuns que permitam a "melhoria dos meios para prevenir e reprimir a cibercriminalidade informática"[348].

As infrações aí constantes são um padrão de referência para os países, que podem acrescer ou suprimir certas menções em função da sua realidade.

---

[345] Em Portugal a Protecção Jurídica de Programas de Computador rege-se pela DL n.º 252/94, de 20 de Outubro (Transpôs para a ordem jurídica interna a Directiva n.º 91/250/CEE, do Conselho, de 14 de Maio) cuja 4ª versão – a mais recente – procedeu-se por via da Lei n.º 92/2019, de 04/09.

Os crimes contra a propriedade intelectual artística e de programa de computador no Brasil são punidos pelo art.º 184º do CP e pela Lei nº 9.609/1998 que dispõe sobre a proteção da propriedade intelectual de programa de computador.

[346] Em Portugal é regulado pelo Decreto-Lei n.º 122/2000 de 07-04 (Transpõe para a ordem jurídica interna a Directiva nº 96/9/CE, do Parlamento Europeu e do Conselho, de 11 de Março, relativa à protecção jurídica das bases de dados).

[347] Esses assuntos estão agrupados em quatro capítulos e tratam da terminologia, medidas a adotar a nível nacional, cooperação internacional e as disposições finais, respetivamente.

[348] **RODRIGUES**, Benjamim Silva. Idem, p. 475.

A CB surge essencialmente como resultado da Recomendação nº R (89) 9 do Conselho da Europa sobre os delitos relacionados com o computador e do trabalho empreendido por algumas organizações supranacionais como a ONU, AIDP, OCDE e CDPC.

As infrações aí constantes e a sua classificação já foram enunciadas no segundo Capítulo[349].

O crime de acesso ilegítimo[350] do art.º 2º da CB tem o seguinte teor

> **Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infracção seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático.**

A previsão desta infração tem por fito garantir a segurança dos sistemas e dados informáticos, máxime a confidencialidade, a integridade e a disponibilidade, o que quer dizer que "é interesse protegido a salvaguarda da possibilidade de gerir, operar e controlar os sistemas de forma livre e tranquila, sem perturbação"[351]. E tal se garante penalizando a simples intrusão ilegal num sistema informático, sem a exigência de uma intenção específica[352], por poder obstruir a sua utilização e também por possibilitar o acesso a dados que *a priori* devem ser confidenciais.

Importa referenciar que este crime pressupõe o acesso sem a devida autorização, excluindo-se os casos em que exista permissão para tal. Este ato de aceder abrange a penetração no todo ou em parte de qualquer sistema informático, excluindo-se "a situação na

---

[349] Ponto 2.1, p. 29.

[350] 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 (Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040&from=EN acedido aos 17-01-2020) prevê no art.º 3º o crime de *Acesso ilegal a sistemas de informação* com o seguinte teor

> *"Os Estados-Membros devem tomar as medidas necessárias para assegurar que o acesso intencional e não autorizado à totalidade ou a parte de um sistema de informação seja punível como infração penal caso a infração seja cometida mediante a violação de uma medida de segurança, pelo menos nos casos que se revistam de alguma gravidade".*

Nessa previsão, diferentemente da estabelecida na CB, estabelece unicamente a punição do acesso ilegal perpetrado com alguma gravidade.

[351] **VERDELHO**, Pedro. Comentário das Leis Penais Extravagantes. Idem, p. 516.

[352] No excerto de fundamentação de direito do Acórdão da 1ª Vara de Competência Mista de Guimarães de 26-06-2007, Proc. 11287/01.1TDLSB, a juíza relatora de Círculo Ana Cristina Clemente parece-nos ter um entendimento relativamente diferente ao referir que este "tipo legal exige a intenção de alcançar benefício ou vantagem ilegítimos que pode reconduzir-se ao desafio à segurança do visado, ao prazer da intrusão; bem como a vanglória publicitada do feito" (Ref.ªJusNet 8521/2007). Pedro Dias Venâncio discorda com autores que apontam a intenção de obter-se "benefícios ou vantagens" de natureza patrimonial. **VENÂNCIO**, Pedro Dias, idem, p. 65 e 66.

qual a pessoa acede fisicamente a um computador autónomo sem passar por outro sistema informático"[353].

O seu cometimento pode ser efetivado, dentre outras formas, pela utilização indevida de uma palavra-passe ou pela inobservância dos procedimentos e medidas de segurança.

Sobre a não inclusão do crime de acesso ilegítimo no ACP já com alguma largueza nos referimos antes, por isso aqui não mais ampliaremos muito o nosso discurso. Mas é mister notar que no ACP tem parcial correspondência com esse delito a alínea b) do art.º 212º que trata da devassa por meio da informática, onde pode ler-se que é punido quem "aceder, sem autorização, a dados informaticamente tratados que contenham informações individualmente identificáveis".

Ao nosso ver, essa previsão é insuficiente porque o acesso ilegal procedido sem autorização aí penalizado é apenas aquele que atinge "informações individualmente identificáveis", quando a convenção recomenda a punição de todo o acesso ao sistema.

Compreende o legislador angolano que os acessos que não impliquem devassa não devam ser penalizados mesmo que "quebrem as regras de segurança".

Na legislação angolana, outra correspondência com art.º 2º, e tanto já anteriormente frisada, encontra-se no art.º 56º do LPDP[354]. Embora não esteja num diploma que faça parte do nosso escopo de estudo, o aí designado "crime de acesso indevido" parece-nos ter um conteúdo que tem alguma correspondência com o que a convenção sugere, se bem que também pune somente o acesso ilegal a dados pessoais. Nele pode ler-se que

> **1. Quem, sem autorização, aceder a dados pessoais cujo acesso lhe está vedado, incorre em crime punível com pena de prisão de 6 meses a 2 anos ou multa correspondente.**
>
> **2. Sem prejuízo do número anterior, o acesso indevido ocorre quando:**
>
> **a) For conseguido através de violação de regras técnicas de segurança;**

[353] **RODRIGUES**, Benjamim Silva. Idem, p. 478.

[354] Ao confrontar o crime de acesso ilegítimo do art.º 6º da Lei do Cibercrime (Lei n.º 109/2009, de 15 de Setembro) e o crime de acesso indevido do art.º 44º da Lei nº 67/98, de 26 de Outubro, Pedro D. Venâncio chega a conclusão que entre os dois ilícitos "não existe nenhum ponto de contacto", ou seja, a similitude entre ambos é somente nominal. No acesso indevido "pune-se o acesso não autorizado a dados pessoais. No crime de acesso ilegítimo o bem jurídico protegido é o património do lesado e a segurança dos sistemas informáticos", e para reforçar a dissemelhança entre ambos culmina dizendo que "o crime de **acesso indevido** é indiferente se esses dados pessoais estão tratados em ficheiros informáticos ou manuais". **VENÂNCIO**, Pedro Dias. Idem, p. 60 e 61.
Embora a análise mencionada *supra* tenha sido feita a crimes constantes em diplomas portugueses acreditamos que se aplicam *mutatis mutandis* ao caso *subjudice*.

b) Tiver possibilitado ao agente ou a terceiros o conhecimento de dados pessoais;

c) Tiver proporcionado ao agente ou a terceiros, benefício ou vantagem patrimonial.

3. O procedimento criminal depende de queixa.

Portanto, seria de bom grado ter essa infração acolhimento no ACP por ser a "porta" dos demais crimes cibernéticos.

A infração seguinte da convenção é a intercepção ilegítima[355] do art.º 3º cujo assunto é

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a intercepção intencional e ilegítima de dados informáticos, efectuada por meios técnicos[356], em transmissões não públicas[357], para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas[358] provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infracção seja cometida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático.

Esta infração tem por objetivo defender "o direito dos dados transmitidos, à semelhança do que ocorre com a violação do direito ao respeito das comunicação"[359], punindo as interceções sucedidas no interior de um sistema informático que podem configurar ações de *espionagem*

---

[355] Igualmente prevista no art.º 6º da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de agosto de 2013, aí tem o seguinte conteúdo

> *"Os Estados-Membros devem tomar as medidas necessárias para assegurar que a interceção intencional e não autorizada, através de meios técnicos, de transmissões não públicas de dados informáticos para, a partir de ou num sistema de informação, incluindo emissões eletromagnéticas de um sistema de informação que comporte esses dados, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade"*

[356] Por meios técnicos subentendam-se "os dispositivos electrónico-digitais susceptíveis de captarem os fluxos informacionais e comunicacionais que se encontram armazenados em redes de comunicações electrónicas ou em sistemas informáticos (perspectiva estática), ou circulam por uma rede de comunicações electrónicas ou um sistema informático e automatizado de dados (perspectiva dinâmica)." **RODRIGUES**, Benjamim Silva. Idem, p. 341.

[357] A expressão "não públicas" é explicada no Relatório Explicativo da CB no seu nº 54. Disponível em https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf (Acedido aos 16-01-2020).

[358] O âmbito das "emissões electromagnéticas" constam do nº 57 do Relatório Explicativo da CB. Idem.

[359] Ainda Benjamim Rodrigues sobre o alcance dessa infração acresce o seguinte: a "intercepção ilegítima pode abranger quer a escuta, o controlo ou a vigilância do conteúdo das comunicações, bem como a obtenção do conteúdo directamente por acesso ao sistema informático e pela sua utilização, seja indirectamente por dispositivos electrónico-magnético de escuta". **RODRIGUES**, Benjamim Silva. Idem, p. 479.

informática[360]. Noutros termos, podemos dizer que nesta infração procura-se "evitar todo tipo de monitorização dos fluxos informacionais e informático-digitais «... que ocorram de um sistema ou rede informáticos, a ele destinadas ou deles provenientes ...»"[361].

O bem jurídico ali tutelado tem duplo aporte constitucional: o direito à privacidade do art.º 32º e o direito ao sigilo nas comunicações do art.º 34º, ambos da CRA.

Tem ligeiras similitudes com o crime de violação de telecomunicações do art.º 214º do ACP, na parte do nº 1 que pune a intromissão "no conteúdo de telecomunicação", divergindo na necessidade de ter conhecimento deste conteúdo. Porém, é mais com a devassa por meio informático que se parece, partilhando inclusive parte do bem jurídico protegido.

É um crime de perigo, não exigindo qualquer dano efetivo, ou seja, consuma-se pela simples ação formal de captar informações, não se exigindo que haja a efetiva obtenção de informação[362].

O texto normativo começa com a exigência de que a interceção deva ser dolosa e "não autorizada" e dá algumas opções aos estados ao regularem sobre essa temática. Por exemplo, há a possibilidade de serem penalizadas somente as interceções de transmissões "entre sistemas informáticos conectados à distância"[363].

A interceção ilegal é uma infração muito semelhante ao acesso ilegítimo e, possivelmente, pelas mesmas razões que este não tenha tido acolhimento no ACP. É presumível que o legislador tenha entendido que a infração de interceção ilegal possa ser subsumida em alguns dos delitos já previstos.

O delito subsequente é o relacionado à interferência em dados do art.º 4º[364] da CB. Nele pode ler-se que

> **1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito**

[360] A espionagem informática é também designada por "furto de dados" por consistir "na tomada de conhecimento de informações ou dados ilegitimamente e contra a vontade e conhecimento do seu titular", isto é, representa o conhecimento indevido de dados. **MACEDO**, João Carlos Cruz Barbosa de, "Algumas considerações acerca dos crimes informáticos em Portugal", *idem*, p. 232.

[361] **RODRIGUES**, Benjamim Silva. Idem, p. 337.

[362] **VERDELHO**, Pedro. Comentário das Leis Penais Extravagantes. Idem, p. 518.

[363] Ibidem, Idem.

[364] Esse delito é mencionado de novo no art.º 4º da Diretiva 2013/40/UE DO Parlamento Europeu e do Conselho de 12 de Agosto de 2013, com a designação de "Interferência ilegal nos dados" e afirma que

> *Os Estados-Membros devem tomar as medidas necessárias para assegurar que o ato intencional e não autorizado de apagar, danificar, deteriorar, alterar ou suprimir dados informáticos de um sistema de informação, ou de os tornar inacessíveis, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade.*

interno, o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos.

2. **Uma Parte pode reservar-se o direito de exigir que a conduta descrita no n.º 1 provoque danos graves.**

A penalização da interferência em dados do art.º 4º da CB visa dar guarida a sua integridade e ao regular funcionamento dos dados informáticos como também à utilização eficiente de dados ou de programas informáticos gravados. Para o efeito, pune-se a danificação, a eliminação ou a deterioração do "conteúdo informático dos dados e de programas"[365], e ainda toda a alteração que afeta negativamente os mesmos.

O que estabelece o nº 1 é praticamente o crime de dano contra os dados, pois que a supressão dos mesmos faz com que não estejam acessíveis a quem detenha um computador ou um suporte nos quais os dados se encontram armazenados.

Para que haja punição, o infrator tem de agir com dolo e sem estar autorizado ou, como se infere do texto do artigo, a atuação deve ser intencional e ilegítima.

O nº 2 prevê que cada estado possa impor que sejam apenas punidas as atuações das quais resultem a produção de um "prejuízo grave", cabendo ainda a cada estado definir o que entenda ser "prejuízo grave".

O ACP albergou essa previsão legal e tal acolhimento fê-lo no art.º 399º que criminaliza o dano informático.

A opção pela designação desse tipo penal por «dano informático» parece-nos aceitável, mas para melhor clarividência sugeríamos o acréscimo do termo dado, ficando "dano a dados informáticos". Não corroboramos com alguns diplomas que têm designado este crime como sendo de «dano relativo a dados ou outros programas informáticos», visto que no conceito de dado informático constante na al. c) do art.º 233º[366] do ACP já estão previstos os programas informáticos.

O conteúdo aí empregado vai ao encontro do tipo objetivo da modalidade sugerida pela convenção, por isso pune na primeira parte do seu nº 1 "Quem, com intenção de causar prejuízo a terceiro, alterar, deteriorar, inutilizar, apagar, suprimir, destruir ou, de qualquer forma, causar dano a sistemas ou dados informáticos".

---

[365] **RODRIGUES**, Benjamim Silva. Idem, p. 482.

[366] Ali podemos ler o seguinte: "Dado informático" é qualquer representação de factos, informações ou conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo programas que permitam a um sistema informático executar uma função; (o sublinhado é nosso).

O art.º 399º vai mais além punindo não só a interferência a dados como também em sistemas. Ademais, a segunda parte do nº 1 estatui igualmente a punição de quem causar dano de forma intencional "mediante a introdução ou transmissão de dados informáticos ou, por qualquer outra forma, interferir no funcionamento de sistema informático".

O nº 2 do art.º 4º da CB tem igualmente o consequente abrigo no ACP, uma vez que o art.º 399º pune unicamente os danos que forem relevantes (nº 4), agravando-se a punição em função da dimensão do prejuízo causado (nº 3 al. a) e b)).

Da interferência em dados segue-se a interferência em sistemas constante no art.º 5º com o texto seguinte

> **Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.**

De acordo ao nº 9 da Recomendação (89), reforçado pelo ponto 65 da Nota Explicativa, a interferência ilegal em sistemas do art.º 5º da CB corresponde a sabotagem informática.

As condutas que esta previsão pretende acautelar são aquelas sucedidas de forma dolosa e que emperram o uso legal dos sistemas informáticos, estando aqui incluídos os sistemas de telecomunicações. Outro pressuposto é que a ação do "sabotador informático" decorra "sem a devida permissão", ficando fora da discursividade jurídico-penal deste artigo as que forem autorizadas.

O seu tipo objetivo é preenchido pela ação de "transmitir, danificar, eliminar, deteriorar, causar ruína", alargando-se nas ações que consistem em "impedir, ou interromper o funcionamento de um sistema informático". Pretende-se, *grosso modo*, punir toda e qualquer ação que visa "entravar o funcionamento de um sistema informático".

Dessas ações típicas, podemos perceber que o bem jurídico aqui tutelado envolve "o interesse dos exploradores e utilizadores de um sistema informático ou de um sistema de

telecomunicações no seu bom funcionamento, sendo possível proteger um número indeterminado de outras funções"[367].

O artigo estabelece também a penalização das ações que forem consideradas "graves"[368], podendo ainda ser estabelecida a "quantidade mínima de danos" a considerar, estando a disposição dos estados elencarem as atuações passíveis dessa qualificação.

Os ataques informáticos que causam graves perturbações a nível das comunicações informáticas, como os designados ataque de negação de serviço e o ataque distribuído de negação de serviço (DoS, DDoS)[369] encaixam-se bem nesse ilícito penal, alguns deles levam mesmo aos ditos *shutdown* ou encerramento de *sites.*

A disseminação de vírus ou de qualquer outro programa malicioso também pode ser aqui compreendida. Merecem ainda enquadramento nesta previsão as façanhas ligadas ao *spam*[370]*,* desde que esses correios não solicitados entravem de forma gravosa as comunicações.

O art.º 3º da Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de Agosto de 2013, na mesma ordem de ideias, também aborda a interferência ilegal no sistema, reforçando o art.º 5º da CB enunciando o seguinte

> **Os Estados-Membros devem tomar as medidas necessárias para assegurar que o ato intencional e não autorizado de impedir ou interromper gravemente o funcionamento de um sistema de informação, introduzindo dados informáticos, transmitindo, danificando, apagando, deteriorando, alterando ou suprimindo esses dados, ou tornando-os inacessíveis, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade.**

---

[367] **RODRIGUES**, Benjamim Silva. Idem, p. 483.

[368] Leia-se, para mais subsídios, o ponto 67 da Nota Explicativa.

[369] Benjamim Siva Rodrigues fala desses ataques nos seguintes termos:

> "Trata-se de um fenómeno de paralisação dos usos das estruturas informáticas. A acção principal, com vista a "paralisação", consiste no envio massivo de informação a um computador ou terminal informático através da rede em forma de correio electrónico ("*mail-bombing*" ou "*spamming*") ou de pacotes de dados até que o equipamento, por saturação, já não suporte e bloqueie com a cessação de funcionamento. O "DDoS" surge-nos como uma técnica mais apurada já que requer programas mais complexos que permitam que o ataque se desenvolva, em paralelo, numa pluralidade de terminais computacionais, assim se obtendo o colapso de todo sistema".

RODRIGUES, Benjamim Silva. Idem, p. 327.

[370] Em Portugal a regulação do Spam foi feita inicialmente pelo Decreto-Lei n.º 7/2004 de 7 de Janeiro, que transpôs a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, no seu Capítulo IV que regula as Comunicações publicitárias em rede e marketing direto (art.º 22.º). Posteriormente, foi transposta a Diretiva n.º 2009/136/CE para a Lei 46/2012 – Dados pessoais e privacidade nas comunicações eletrónicas, que regula presentemente o envio de comunicações não solicitadas.

Como podemos notar, os dois diplomas no essencial mantêm praticamente o mesmo conteúdo, mormente no que respeita a tutela penal a dar aos ataques contra os sistemas informáticos.

A existência de um diploma que traz somente os aspetos relativos "a ataques contra os sistemas de informação" revela bem a preocupação que a União Europeia tem acerca dos mesmos, refletida na dependência da sociedade moderna aos sistemas informáticos.

Essa regulação autónoma compreende-se ainda pelo surgimento do moderno tipo de criminalidade organizada ligada à informática, ou seja, surgem cada vez mais atos ligados ao chamado ciberterrorismo, afetando inclusive a segurança dos países por impedirem que os governos assegurem as questões sociais vitais.

Esses ataques aproveitam-se das falhas de segurança e das vulnerabilidades dos sistemas e, tal como os protagonizados em Angola e retratados anteriormente, provocam "prejuízos substanciais, através da interrupção de sistemas de informação e comunicação" (no caso dos ataques contra o estado angolano em 2016); e a "perda ou alteração de informações comerciais confidenciais importantes" (os praticados contra a empresa petrolífera Sonangol em 2019).

Analisemos a relação existente entre o *corpus* do art.º 5º da CB referente a sabotagem informática e o ACP.

Como já referimos antes, não existe no ACP uma previsão totalmente correspondente a este artigo. Encontramos uma ligeira similitude com o crime de dano informático do art.º 399º na parte que pune "quem causar danos a sistemas informáticos" (nº 1) e na cláusula aberta que penaliza "qualquer interferência no funcionamento do sistema informático" (nº 2).

O crime previsto na legislação angolana difere do crime de dano relativo a dados acolhido em outras legislações lusófonas que abordam o cibercrime.

O legislador angolano ao adotar a lata designação de "dano informático", quis precisamente envolver os danos quer perpetrados contra os sistemas informáticos quer os executados contra os dados informáticos, aliás como se pode inferir da expressão "causar dano a sistemas ou dados informáticos".

Seguindo o mesmo diapasão, o nº 2 do art.º 399º pune, para além da "introdução ou transmissão de dados informáticos", a interferência "no funcionamento de sistema informático", e de acordo a CB é propriamente essa "interferência em sistemas" que representa o crime de sabotagem, coincidindo também na intencionalidade e na ilegitimidade do ato.

Falta-nos agora refletirmos se o crime de dano informático regula ou não as obstruções em sistemas informáticos consideradas "graves".

Na verdade, no art.º 399º não se vislumbra propriamente a expressão "obstrução grave" colhida no art.º 5º da CB. Ou melhor, o dispositivo da convenção sugere exatamente que somente sejam objeto de punição os atos descritos que representem uma perturbação gravosa em sistemas informáticos.

Essa exigência, ao nosso modesto ver, fica preenchida pelo nº 3 do art.º 399º que qualifica a gravidade da "interferência" em função da relevância do prejuízo causado, e mais uma vez parece-nos a "interferência em dados" ficar absorvida nos "danos informáticos"[371]. A sabotagem informática não é nada mais do que um dano informático grave que incide no sistema informático.

No tipo objetivo da CB punem-se os atos que perturbam o funcionamento de sistemas informáticos ou a comunicação de dados. O ilícito do ACP pune todo o dano relevante causado quer nos sistemas informáticos quer nos dados informáticos. O segundo é por isso mais abrangente.

Assim, sugeríamos – à guisa de outras legislações modernas sobre o cibercrime – que houvesse um tratamento diferenciado entre os dois ilícitos, urgindo, para o efeito, a feitura de alguns ajustamentos, esvaziando-se o teor do art.º 399º e substituindo-o por dois tipos penais, um relativo a dano informático a dados e outro relacionado com a sabotagem informática.

Seguidamente temos no art.º 6º da CB a extensa explanação da regulação do uso abusivo de dispositivos[372], onde lê-se que

---

[371] Seguindo o entendimento de Pedro Verdelho ao confrontar as duas previsões legais, a "perturbação do sistema", que se exige para a verificação do crime de sabotagem informática, "tem de ser resultado da prática de actos que, em si mesmos, isoladamente, poderiam consubstanciar crime de dano relativo a dados ou programas do computador".
Seguidamente e evidenciado sempre a semelhança entre os dois delitos em causa diz que "na prática, uma vez que actos típicos do crime de dano podem resultar na prática de sabotagem, não será raro enquadrar situações concretas quer num, quer noutro tipo". **VERDELHO**, Pedro. Comentário das Leis Penais Extravagantes. Idem, p. 513.

[372] Na Diretiva 2013/40/UE Do Parlamento Europeu e do Conselho de 12 de Agosto de 2013 é equivalente ao art.º 7º que fala dos "Instrumentos utilizados para cometer infrações" da seguinte forma

> *Os Estados-Membros devem tomar as medidas necessárias para assegurar que a produção, venda, aquisição para utilização, importação, distribuição ou qualquer outra forma de disponibilização de um dos seguintes instrumentos, não autorizadas e com o intuito da sua utilização para a prática de uma das infrações previstas nos artigos 3º a 6º, seja punível como infração penal, pelo menos nos casos que se revistam de alguma gravidade:*
> *a) Um programa informático, concebido ou adaptado essencialmente para cometer uma das infrações previstas nos artigos 3º a 6º;*
> *b) Uma senha, um código de acesso ou dados similares que permitam aceder à totalidade ou a parte de um sistema de informação.*

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracções penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente:

a) A produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:

i. Um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir a prática de uma das infracções definidas em conformidade com os artigos 2º a 5º;

ii. Uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam aceder a todo, ou a parte de um sistema informático com a intenção de serem utilizados para cometer qualquer uma das infracções definidas nos Artigos 2º a 5º; e

b) A posse de um elemento referido nas alíneas a), i. ou ii., com a intenção de ser utilizado com o objectivo de cometer qualquer uma das infracções referidas nos artigos 2º a 5º. As Partes podem exigir que no direito interno se reúna um certo número desses elementos para que seja determinada a responsabilidade criminal.

2. O presente artigo não deve ser interpretado como impondo responsabilidade criminal quando a produção, a venda, a aquisição para utilização, a importação, a distribuição, ou outra forma de disponibilização ou posse, mencionadas no n.º 1 do presente artigo não tenham por objectivo cometer uma infracção estabelecida em conformidade com os artigos 2º a 5º da presente Convenção, como é o caso de ensaios autorizados ou de protecção de um sistema informático.

3. Cada Parte pode reservar-se o direito de não aplicar o disposto no n.º 1 do presente artigo desde que essa reserva não diga respeito à venda, distribuição, ou a qualquer outra forma de disponibilização dos elementos referidos no n.º 1, a), ii.

Este artigo tem duas ideais centrais relacionadas com os dispositivos: o seu uso ilegítimo e o seu uso abusivo, e por isso "sanciona, em termos gerais, a produção, a difusão ou até a mera posse com esses propósitos, de *vírus informáticos* ou de *passwords* obtidas de forma ilegítima"[373]. Tem por suporte outros diplomas legais recentemente adotados a nível do Conselho da Europa e da União Europeia, bem como da longínqua Convenção de Genebra de 1929 relacionada à falsificação de moeda.

De acordo ao que estabelece este artigo, a sua finalidade é tipificar as condutas que merecem tutela penal, praticadas de forma intencional, sem autorização e que afetam dispositivos ou dados de acesso, dos quais se procedeu um uso abusivo que atente contra a confidencialidade, integridade e disponibilidade dos sistemas informáticos.

A bem dizer, as infrações aí previstas requerem ferramentas de pirataria ou dispositivos informáticos, por isso mesmo "pretende-se estabelecer uma tutela avançada, ao se conceber a criminalização da aquisição de tais ferramentas informáticas"[374], com o fito de impedir que se criem os ditos "mercados negros".

Importa notar que os dispositivos aqui referenciados são somente aqueles "concebidos, ou adaptados, essencialmente para efeitos de cometimento de uma infração".

O nº 3 do art.º 6º deixa à disposição dos estados regularem, fazendo uma avaliação do que pode ser incluído no crime de "uso indevido de equipamento", todavia o normativo aconselha que se penalizem, no mínimo, "a venda, a distribuição ou a disponibilização de uma *password* ou dados de acesso a computadores".

Compulsando os delitos informáticos do ACP não descortinamos nenhuma correspondência integral com este normativo da CB, contudo notamos que se encontra sinteticamente previsto na falsificação informática (art.º 235º) e no dano informático (art.º 399º) por serem ilícitos que resultam de "utilizações indevidas de dispositivos".

Integralmente acolhidos pelo ACP foram os crimes contra o computador. Na verdade são crimes comuns, só que no presente caso são perpetrados por intermédio de um sistema informático, ou seja, implicam a manipulação de dados ou de sistemas informáticos.

O primeiro vem consignado no art.º 7º e reporta o crime de falsidade informática, podendo nele ler-se que

---

[373] **VERDELHO**, Pedro. "A Convenção Sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa." Idem, p. 262.

[374] **RODRIGUES**, Benjamim Silva. Idem, p. 485. Este autor entende que o art.º 6º da CB, resumidamente, criminaliza "o fabrico, a produção, a importação, a distribuição, a venda ou locação, a posse, a instalação, a manutenção ou a substituição, a promoção comercial, o *marketing* ou a publicidade, com fins comerciais, de dispositivos ilícitos".

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal.

Também designada falsificação informática[375] ou falsificação relacionada com computadores[376], a regulação desta infração pelo Conselho da Europa pretendeu estabelecer uma punição, no ambiente informático, de um ilícito semelhante ao que classicamente se designa por falsificação de documentos.

A falsificação tradicional (art.º 234º do ACP) pressupõe a tangibilidade do documento, por isso com esta "nova" falsificação objetivou-se, efetivamente, fazer um alargamento punitivo para os documentos (públicos ou privados) que se encontram armazenados de forma eletrónica.

A falsificação eletrónica requer um procedimento intencional no processo de emissão de dados e a ilegitimidade na atuação. Sobre este aspeto, o ponto 83º da Nota Explicativa reforça dizendo que "a introdução não autorizada de dados correctos ou incorretos dá origem a uma situação correspondente à elaboração de um documento falso".

A delimitação do alcance da expressão "autenticidade" cabe às partes.

Pelo exposto, vemos que preenchem esse ilícito penal a criação ou modificação desautorizada de dados que adquiram relevância legal, podendo ser utilizados como se fossem genuínos, provocando deste modo engano nas relações jurídicas. Assim, o bem jurídico protegido funda-se na "segurança e na fiabilidade dos dados electrónicos que podem ter consequências nas relações jurídicas".

---

[375] Para Benjamim Rodrigues essa infração "consiste na criação ou modificação, sem autorização de quem de direito, dos dados gravados para que adquiram um valor probatório diferente e que o desenvolvimento das transacções jurídicas, que se funda sobre a autenticidade das informações fornecidas por esses dados, possa ser alvo de um engano". Quanto ao conceito de falsificação aqui evocado, o autor entende que "ele pode fundar-se sobre a autenticidade quanto ao autor do documento ou pode ter-se em linha de conta a veracidade das informações contidas no documento em questão". **RODRIGUES**, Benjamim Silva. Idem, p. 346 e 347.

[376] Leia por exemplo os pontos 80 e 81 da Nota Explicativa.

No ACP não divisamos a definição de autenticidade de um documento, mas do *corpus* do art.º 235º infere-se que documentos autênticos sejam aqueles passíveis de serem usados "como meio de prova", ou seja, de puderem ser utilizados para "finalidades juridicamente relevantes"[377].

O conteúdo da lei angolana a respeito da falsidade informática compatibiliza-se com o constante na convenção, já que pune quem "dolosamente enganar outrem introduzindo ou excluindo dados em sistema informático, originando desta atuação dados falsificados que podem ser tidos como reais, servindo mesmo como meio de prova" (art.º 235º nº 1). Não obstante, essa previsão vai um pouco além punindo igualmente "quem não sendo falsificador", aja intencionalmente, utilizando esses dados informáticos que foram falseados (art.º 235º nº 2). Traz ainda no nº 3, como circunstância agravante, o facto de o autor da ilicitude ser funcionário público.

A pretensão fraudulenta ou ilegítima na punição desta infração, sugeridas às partes no final do art.º 7º da CB, foi adotado no ACP por determinar a consideração da "intenção de enganar".

Da falsificação informática segue-se a infração de burla informática do art.º 8º da CB que tem o texto seguinte:

> **Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, o acto intencional e ilegítimo, que origine a perda de bens a terceiros através:**
>
> **a) Da introdução, da alteração, da eliminação ou da supressão de dados informáticos,**
>
> **b) De qualquer intervenção no funcionamento de um sistema informático, com a intenção de obter um benefício económico ilegítimo para si ou para terceiros.**

[377] Idem, p. 489.

Este delito, também rotulado de manipulação informática fraudulenta[378], surge precisamente devido a constatação do acréscimo de infrações económico-financeiras que se podem associar à própria Internet, nestas agregando-se os abusos de cartões de créditos.

Esta verificação levou o legislador a incriminar as manipulações registadas à entrada dos sistemas, ou melhor dizendo, as ingerências no tratamento de dados; desde que efetuadas de forma abusiva e visarem o prejuízo do património de alguém, ou seja, pretende-se com o efeito impedir que haja "transferência de propriedade ilegal".

Apesar de ter algumas especificidades próprias, o crime de burla informática "tem a mesma natureza do crime clássico de burla, sendo portanto um crime contra o património"[379].

Os elementos do tipo penal estão representados pelas ações de "introdução, modificação, extinção ou supressão" que causem degeneração ao funcionamento de um sistema informático. Isto quer dizer, que o agente atua com a finalidade de obter um benefício económico ilícito.

Para que esse tipo legal esteja previsto, além da vantagem económica já enunciada, é necessário ainda que a ação se desenrole de forma intencional (intenção fraudulenta)[380] e sem autorização. Assim, a intenção é eivada de uma fraude específica baseada na desonestidade com o intento de beneficiar-se a si ou a outrem.

O art.º 407º do ACP usa a designação de *burla informática e das telecomunicações* para essa infração, mas a sua previsão acolhe, praticamente, todo o conteúdo que a convenção expõe.

Mantém no essencial as formas de atuações previstas no art.º 8º CB, enunciando que tais práticas aplicam-se a quem pretender "obter para si ou para terceiro vantagem patrimonial".

As ligeiras diferenças notadas prendem-se com a não inserção no texto do ACP da necessidade do procedimento decorrer de "forma intencional" ou "não autorizada", mas tal achamos ser desnecessário ou irrelevante já que o meio astucioso ou enganoso que se exige para o cometimento desse crime pressupõe intencionalidade (lesar o património) e ilegitimidade (não autorização).

---

[378] Ponto 88 da Nota Explicativa.

[379] **VERDELHO**, Pedro. "A Convenção Sobre Cibercrime do Conselho da Europa – Repercussões Na Lei Portuguesa." Idem, p. 263.

[380] Sobre este aspeto, a parte final do ponto 90 da Nota Explicativa dá o exemplo seguinte: "as práticas comerciais com relação ao mercado da concorrência, que possam causar prejuízo económico a uma pessoa e beneficiar outra, mas que não sejam realizadas com intenção fraudulenta ou desonesta, não devem ser incluídas na ofensa estabelecida por este artigo". Outro exemplo tem a ver com "o uso de programas de coleta de informações para uma loja de comparação na Internet ("*bots*"), mesmo que não seja autorizada por um *site* visitado pelo "*bot*", não se destina a ser criminalizada."

As infrações relacionadas contra os conteúdos reportam propriamente as que têm a ver com a pornografia infantil prevista no art.° 9° da CB e traz o seguinte teor

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, as seguintes condutas, quando cometidas de forma intencional e ilegítima:

a) Produzir pornografia infantil com o objectivo da sua difusão através de um sistema informático;

b) Oferecer ou disponibilizar pornografia infantil através de um sistema informático;

c) Difundir ou transmitir pornografia infantil através de um sistema informático;

d) Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;

e) Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.

2. Para efeitos do n.º 1, a expressão "pornografia infantil" inclui qualquer material pornográfico que represente visualmente:

a) Um menor envolvido num comportamento sexualmente explícito;

b) Uma pessoa que aparente ser menor envolvida num comportamento sexualmente explícito;

c) Imagens realísticas que representem um menor envolvido num comportamento sexualmente explícito;

3. Para efeitos do n.º 2, a expressão "menor" inclui qualquer pessoa com idade inferior a 18 anos. Uma Parte, pode, no entanto, exigir um limite de idade inferior, que não será menos que 16 anos.

4. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto nos n.ºs 1, alínea d), e 2, alíneas b) e c).

Com este dispositivo legal pretende-se efetuar um combate cerrado ao flagelo da exploração sexual das crianças levados a cabo pelos sistemas informáticos.

Deve assinalar-se que na pornografia infantil *sub judice* não está em consideração a penalização de atos de natureza sexual envolvendo crianças, não sendo este o objeto da CB. O que importa relevar é "a posterior utilização ou difusão dessa pornografia"[381].

Muitos diplomas legais antecedentes determinaram a regulação deste ilícito[382].

Nesse artigo são incriminadas, especialmente, três ações: a produção visando a difusão, a oferta ou disponibilização e a difusão ou transmissão de material contendo conteúdo relacionado à pornografia infantil, usando para tal os sistemas informáticos.

A incriminação da produção (n.º 1 al. a)) enquadra-se na luta contra os perigos que essa realidade representa. Com a incriminação da oferta ou disponibilização (n.º 1 al. b)) o legislador tencionou abranger os conteúdos envolvendo pornografia infantil postos *online*, punindo deste modo os ditos *sites* pornográficos. Já com a penalização da difusão ou transmissão visou-se combater a "disseminação activa desse material" (n.º 1 al. c)).

Na al. d) do nº 1, a "obtenção activa" de material com pornografia infantil, tal como o conteúdo obtido fazendo *download* num sistema informático, estão abrangidos pela expressão "obter para si ou para terceiros".

A mera posse desse material[383] num sistema informático ou num suporte é igualmente criminalizada por representar uma forma de impulsionar à solicitação desses materiais muito bem descritos no n.º 1 al. e) e por estimular o comércio de pornografia em que se explorem sexualmente crianças, ou como a Nota Explicativa realça, pretende-se sancionar todos os "participantes nesta cadeia, desde a produção até à posse".

As alíneas a), b) e c) do nº 2 reportam os aspetos que envolvem a definição da pornografia infantil.

O comportamento lesivo aqui abordado deve suceder de forma ilícita e sem autorização.

Termina o artigo definindo menor como sendo uma pessoa que tenha menos de 18 anos de idade seguindo o art.º 1º da Convenção das Nações Unidas sobre os direitos da criança.

---

[381] **VERDELHO**, Pedro. "A Convenção sobre Cibercrime do Conselho da Europa - Repercussões na Lei Portuguesa." Idem, p. 264.

[382] Por exemplo, a nível mundial temos o Protocolo facultativo à Convenção das Nações Unidas relativos aos direitos da criança respeitantes à venda, à prostituição das crianças e à pornografia envolvendo crianças (disponível em https://www.unicef.pt/media/2766/unicef_convenc-a-o_dos_direitos_da_crianca.pdf acedido aos 19-01-2020) e a nível europeu realce-se a Decisão-Quadro 2004/68/JAI do Conselho da Europa de 22 de Dezembro de 2003, relativa à luta contra a exploração sexual das crianças e da pedopornografia (disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32004F0068&from=LV acedido aos 20-01-2020).

[383] Nesses "atos de posse, para além da guarda de fotografias e vídeos em meios físicos, podem ser exemplificadas com a manutenção do material pornográfico proibido no disco rígido do computador ou outro dispositivo de memória rígida, como por exemplo *pendrive*, HD externo, CD, DVD, *Blue Ray*, etc.
Igualmente, também se compreende como posse, a manutenção de arquivos contendo pornografia infantil em caixa de correio eletrónico ou nas denominadas nuvens virtuais como, por exemplo, o famoso Dropbox.". *In* **MORAIS**, Felipe Soares Tavares. Internet, Pornografia e Infância: a Criminalização da Posse de Pornografia Infantil. Revista do Ministério Público do Rio de Janeiro nº 64, Abr. – Jun. 2017, p. 120 e 121.

No ACP a pornografia infantil é regulada no art.º 184º, no entanto excetua-se o nº 1 por reportar um tipo de pornografia infantil que não envolve os sistemas informáticos.

Tal como sucede na convenção, no nº 2 são tipificadas as ações de produção com a intenção de divulgar (al. a)) e a difusão ou transmissão (al. b)). Porém, a presente estatuição não acolhe a punição da simples posse, aliás, nem sequer faz menção dessa eventualidade, entendendo-se que a posse desse tipo de material num sistema informático ou num dispositivo de armazenamento não carece de censura penal.

Outro ponto de dissemelhança é a idade adotada relativamente ao menor. Para efeitos da presente infração, no anteprojeto tem-se por menor quem tenha uma idade inferior aos 16 anos e não fica por ali, qualificando como gravosa esta infração quando lesar um menor de 14 anos (nº 3).

Uma outra especificação, a título de agravação extraordinária, acontece no caso de o agente infrator fazer dessas práticas uma profissão ou se o seu procedimento tiver por objetivo a obtenção dum lucro.

Na definição da pornografia infantil, o legislador angolano não foi muito conciso porém abrangente, considerando preencher esse ilícito meramente "qualquer material pornográfico que represente visualmente um menor de 16 anos ou pessoa aparentando ser menor de 16 anos, envolvidos em comportamentos sexualmente explícitos" (nº 5 al. a)).

No campo das infrações temos finalmente aquelas que sancionam as violações que atingem os direitos do autor e os direitos conexos do art.º 10º da CB, onde consta o seguinte

> **1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a violação do direito de autor definido pela legislação dessa Parte, em conformidade com as obrigações que a mesma assumiu em aplicação da Convenção Universal sobre o Direito de Autor, revista em Paris, em 24 de Julho de 1971, da Convenção de Berna para a Protecção das Obras Literárias e Artísticas, do Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e do Tratado da OMPI sobre o Direito de Autor, com excepção de quaisquer direitos morais conferidos por essas Convenções, quando esses actos forem praticados**

intencionalmente, a uma escala comercial e por meio de um sistema informático.

2. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a violação dos direitos conexos definidos pela legislação dessa Parte, em conformidade com as obrigações assumidas por força da Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão (Convenção de Roma) do Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, e do Tratado da OMPI sobre Interpretações, Execuções e Fonogramas, com excepção de qualquer direito moral conferido por essas Convenções, quando esses actos forem praticados intencionalmente, a uma escala comercial e por meio de um sistema informático.

3. Uma Parte pode, em circunstâncias bem delimitadas, reservar-se o direito de não determinar a responsabilidade penal nos termos dos n.ºs 1 e 2 do presente artigo, na condição de estarem disponíveis outros meios eficazes e essa reserva não prejudique as obrigações internacionais que incumbem a essa Parte, em aplicação dos instrumentos internacionais mencionados nos n.ºs 1 e 2 do presente artigo.

O uso massivo da Internet potenciou extremamente as infrações aos direitos de propriedade intelectual, máxime as que afligem os direitos autorais e os direitos conexos. Nestas violações destacam-se as ações de reprodução e difusão nas redes informáticas de obras que são objeto de proteção legal[384]. A tecnologia digital facilitou a realização de cópias desautorizadas. Tais ações decorrem inexistindo para o efeito qualquer consentimento do titular de tais direitos.

A nível global, a relevância dos direitos do autor e dos direitos conexos faz-se sentir no art.º 17º da Declaração Universal dos Direitos Humanos, ou seja, são considerados uma parte integrante dos direitos fundamentais.

O que esta regulação propõe efetivar é a criminalização das ações cometidas por meio dos sistemas informáticos e que lesem a propriedade intelectual. Neste escopo excluem-se os

[384] Nas obras protegidas incluem-se as literárias, fotográficas, musicais, audiovisuais e outras.

direitos morais e as lesões relacionadas à utilização indevida por direitos das marcas, patentes e *designs*.

O art.º 10º da CB encontra-se assim distribuído: no nº 1 temos as penalizações a serem impingidas pela violação dos direitos de autor, no nº 2 as aplicáveis pela violação dos direitos conexos e nº 3 as reservas ou "circunstâncias limitativas" dadas aos estados-membros na aplicação dos números anteriores.

Vários diplomas internacionais influenciaram o *corpus* deste artigo, nestes destacamos a Convenção de Berna de 1886, a Convenção de Roma de 1961[385], o Ato de Paris de 24 de Julho de 1971 que retificou a Convenção Universal sobre o Direito de Autor de 1952, o Acordo relativo às questões comerciais dos direitos da propriedade intelectual (ADPIC)[386][387] de 1994 e o Tratado da Organização Mundial da Propriedade Intelectual (OMPI)[388] sobre a interpretação ou execução e fonogramas de 20 de Dezembro de 1996. Na verdade, "a Convenção restringe a aplicabilidade destes tratados no ambiente digital"[389].

As infrações aqui tidas como dignas de penalização devem decorrer de forma "deliberada"[390] e efetivamente incidir na esfera comercial "e não a um simples uso privado e pessoal"[391].

Como já anteriormente assinalámos, o art.º 10º da CB não tem acolhimento no ACP, ou seja, nos crimes contra a propriedade do Capítulo II do Título VII não constam delitos relacionados à violação dos direitos de propriedade intelectual cometidos fazendo recurso a um sistema de computadores.

Em Angola os programas de computador e as bases de dados ainda carecem de tutela penal e por isso clama-se por tal regulação. Na versão final do Projecto de Regulamento das Tecnologias e dos Serviços da Sociedade da Informação de 2011[392], apresentada pelo Ministério das Telecomunicações e Tecnologias de Informação, previa a sua proteção jurídica nos art.ºs 62º e 64º respetivamente.

A violação das normas constantes neste Projeto constituem uma contravenção (art.º 90º) e logo sem relevância delituosa.

---

[385] Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão.
[386] Originalmente designado TRIPs *(Agreement on Trade-Related Aspects of Intellectual Property Rights)*.
[387] Em Angola esta Lei foi ratificada a 2 de junho de 1990, publicada no Diário da República (D.R. n.º 26, Iª série).
[388] Angola é membro da OMPI desde Janeiro de 1985, esse facto impõe ao país realizar mudanças no seu quadro legal.
[389] **VERDELHO**, Pedro. "A Convenção Sobre Cibercrime do Conselho da Europa - Repercussões Na Lei Portuguesa." Idem, p. 266.
[390] O art.º 61º do ADPIC sugere esta expressão em vez de "intencional".
[391] **RODRIGUES**, Benjamim Silva. Idem, p. 497.
[392] Infelizmente esse importante dispositivo legal até a presente data ainda não foi aprovado, e já lá vai quase uma década de espera.

No Decreto Presidencial 202/11 de 22 de Julho – Regulamento das Tecnologias e dos Serviços da Sociedade da Informação – a proteção dos programas de computador e das bases de dados é remetida à lei da proteção dos direitos de autor e conexos (Lei nº 15/2014 de 31 de Julho)[393], e esta lei apesar de albergar as obras protegidas nas TICs (art.º 2º nº 4), faz um deficiente enquadramento penal no tocante a violação dos direitos das mesmas[394].

Embora em Angola esses direitos tenham aporte constitucional no art.º 42º (Propriedade Intelectual) e no art.º 43º (Liberdade de criação cultural e artística), esses factos parecem não terem ainda despertado o legislador.

Neste diploma legal encontram-se definidos os programas informáticos (art.º 3º nº 22), e o art.º 4º al. l), ainda diz expressamente que dentre as obras protegidas temos os "programas de computador, ligados ou não em rede", porém as únicas imputações penais referentes às reproduções ilegais de programa protegido são a contrafação e o plágio.

O art.º 83º sobre responsabilidade criminal dos direitos de autor e conexos, reconhece a possibilidade de sanção penal, mas não se denota nele qualquer regulação neste aspeto quando esses direitos forem violados com recurso aos sistemas informáticos. Seguindo a exceção constante no nº 3 do art.º 9º da CB, achamos que o legislador ao erigir a LDACA preferiu "não impor a responsabilidade penal", prevendo a resolução das questões de violação dos direitos de autor e conexos por via de "acções civis" (art.º 80º nº 1 e art.º 81º) usando o CPCA[395].

3.5. Comparação com a Convenção da União Africana

Aqui traremos cada um dos crimes informáticos previstos no ACP e estabeleceremos uma comparação resumida com seu correspondente na CM.

Já acima aduzimos que as disposições penais da CM constam no art.º 29º que é parte integrante da Secção II. Neste artigo temos as ofensas específicas às TICs que são os ataques

---

[393] Essa lei revoga a Lei n.º 4/90, de 10 de Março (disponível em https://www.wipo.int/edocs/lexdocs/laws/pt/ao/ao002pt.pdf acedido aos 21-01-2020) e previa sanção penal no seu art.º 32, mas os crimes aí mencionados (usurpação, contrafação e plágio do art.º 31º) não eram cometidos por meios de sistemas informáticos.

[394] Como já tivemos o cuidado de aduzir, a punição nessa lei é muito restrita, as violações resultam na sua maioria em ações cíveis (art.º 81º) e são sancionadas por multas (art.º 89º). O art.º 83º da responsabilização criminal remete o regime jurídico sancionatório ao CP e ao CPP, porém o ACP não prevê crime algum referente a direitos de autor e conexos. A usurpação do art.º 84º não é considerada crime; os únicos crimes aí contidos são os de contrafação e de plágio (art.º 85º nº 1 e 2).
Assim, achamos que da lei 10/90 de Março para a lei 15/2014 de Julho procedeu-se uma esquisita evolução legislativa *despenalizante*.

[395] Para melhor compreensão dos meios de tutela penal dos direitos de autor e dos direitos conexos no ordenamento jurídico angolano leia-se a obra de Adriano Edgar dos Santos. Os meios de tutela do direito de autor e direito conexo no direito angolano. Dissertação de Mestrado em Ciências Jurídicas orientada pela Professora Doutora Adelaide Menezes Leitão. Universidade de Lisboa. Faculdade de Direito. Lisboa Abril/2017. Disponível em https://repositorio.ul.pt/bitstream/10451/31636/1/ulfd134164_tese.pdf (acedido aos 21-01-2020).

contra os sistemas informáticos, as violações de dados informáticos e as infrações relativas ao conteúdo, respetivamente.

Devemos realçar que, contrariamente à CB e ao ACP, a CM não cataloga a nomenclatura das infrações informáticas. Deste modo, as denominações dessas infrações que passaremos a utilizar retiramo-las do próprio enunciado de cada alínea ou ponto em análise.

Nas disposições penais, a convenção africana começa por regular o *acesso ilegítimo* e a facilitação do seu cometimento. O diploma africano dá uma atenção especial a esse delito constante no art.º 29º, reservando-lhe três alíneas – a), b) e c) – todas do nº 1.

A al. a) tem uma elaboração que se distingue da encontrada em outros diplomas. Aí criminaliza-se não só o comum "acesso não autorizado" como também o acesso que vai além do autorizado. Entretanto, em nenhuma parte deste diploma encontramos uma definição de "acesso autorizado", pelo que ficamos sem perceber em que medida um acesso pode exceder ao permitido.

Da al. d) do art.º 2º 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 infere-se que o «acesso não autorizado» representa um comportamento não consentido pelo proprietário ou por outro titular dos direitos do sistema ou de parte dele, ou não permitido pelo direito nacional. Consideramos que esta definição dada pela União Europeia é igualmente aplicável no âmbito da União Africana.

Na al. b) penaliza-se o acesso autorizado ou o que suplanta o permitido e que visa o cometimento de uma nova infração ou a facilitação da prática da mesma. Aqui nota-se implicitamente que o legislador reconhece o acesso ilegítimo como sendo "a porta de entrada" de outras infrações.

A al. c) sugere punir quem "manter-se ou tentar manter-se de forma fraudulenta, no todo ou em parte de um sistema informático". Embora essa alínea fale de "manter-se" e não propriamente do "acesso", incluímos no crime de acesso ilegítimo pois que essa ação de "manter-se" é naturalmente precedida da ação de aceder ilegitimamente.

Este crime de risco não está previsto no ACP, embora – como já elucidamos – no crime de devassa por meio da informática se faça uma ligeira menção do mesmo. Contudo, aí somente se penalizam os acessos aos dados que contenham "informações individualmente

identificáveis" (art.º 212º). Na mesma senda, o art.º 56º do LPDP referente ao crime de acesso indevido pune unicamente o acesso ilegal a dados pessoais.

A al. d) do nº 1 do art.º 29º da CM apresenta um enunciado que nos remete (parcialmente) ao crime de *sabotagem informática*, porém o ACP não dá acolhimento categórico a essa infração que procura punir "a dificultação, o entrave ou o embaraçamento do funcionamento de um sistema computacional".

A previsão da sabotagem informática na CM tem um texto muito reduzido, seria recomendável enriquecê-lo com expressões do tipo "pune-se quem perturbar ou obstruir gravemente o funcionamento de um sistema informático", e não mencionar apenas "quem dificultar ou distorcer".

Na al. e) do art.º 29º da CM sanciona-se todo aquele que "introduzir ou tentar introduzir fraudulentamente dados num sistema informático". Esta estatuição afigura-se incompleta já que uma introdução fraudulenta de dados pode preencher vários ilícitos informáticos do ACP. Por exemplo, se a intenção da introdução de dados for a de enganar, originando dados falsos que podem ter relevância jurídica então teremos a infração de falsidade informática (art.º 235º); se causar prejuízo ou interferir no funcionamento do sistema teremos um dano informático (art.º 399º) e caso cause prejuízo patrimonial para a vítima ou vantagem patrimonial para o infrator o crime seria o de burla informática e nas telecomunicações (art.º 407º).

O primeiro crime verdadeiramente acolhido conjuntamente por ambos os diplomas em análise é o *dano informático*[396]. No CM está contido no art.º 29º nº 1 al. f), punindo-se a "introdução ou a tentativa de introdução de dados a um sistema informático" assim como a "danificação, apagamento, deterioração, modificação fraudulenta de dados informáticos".

No ACP, o nº 1 do art.º 399º considera dano informático a ação de quem deliberadamente e visando causar prejuízo a outrem "deteriorar, inutilizar, apagar, suprimir, destruir ou, de qualquer forma, causar dano a sistemas ou dados informáticos". O nº 2 do mesmo artigo inclui no mesmo ilícito penal a "introdução ou transmissão de dados informáticos" ou, qualquer género de "interferência no funcionamento de sistema informático, causando intencionalmente dano a alguém".

[396] No art.º 1º da CM a definição de dano informático é dada da seguinte forma: "qualquer prejuízo à integridade ou à disponibilidade de dados, de um programa, sistema ou uma informação".

Embora usem termos aparentemente diferentes, se analisarmos bem os dois enunciados, tanto o ACP como a CM punem a danificação que afeta os dados ou os sistemas informáticos, coincidindo essencialmente nos elementos objetivos e subjetivos, no entanto somente a convenção africana pune a tentativa.

Também não previsto no ACP, porém constante na CM temos o crime de *uso abusivo de dispositivo*[397] das al. g) e h) nº 1 do art.º 29º. Este delito pune a concessão de um equipamento ou dado que favoreça o cometimento de infrações cibernéticas bem como a aquisição encoberta de senhas que possibilitem o acesso ilegal a um sistema informático. De uma forma genérica, essas atuações atentam contra a confidencialidade, a integridade e a disponibilidade de sistemas ou dados informáticos.

A inclusão deste ilícito no ACP seria aconselhável pois ações muito frequentes no mundo virtual como a dos chamados *keyloggers* em que estes programas "captam as teclas digitais no computador ou no teclado virtual, através de cliques"[398] – permitindo o furto de senhas de contas bancárias, cartões de crédito, acesso a sistemas e a outras informações confidenciais – preenchem precisamente o ilícito de uso abusivo de dispositivo.

Incluem-se dentro deste crime o uso de *spywares* ou de qualquer outro tipo de *malware* que facilite obter o acesso a dados[399]. Procura-se com esta previsão legal combater a pirataria informática.

O cometimento desta infração pressupõe um certo nível de sofisticação técnica por parte do infrator. Porém, o surgimento de mercados negros *online* onde elucidam as formas de aquisição de senhas, "disponibilizam ferramentas para testes de penetração e deteção de vulnerabilidades e Trojan de Acesso Remoto (RATs[400])"[401] potenciam a perpetração desta infração.

---

[397] É um delito muito semelhante ao ilícito de invasão de dispositivo de informática p. e p. pelo art.º 154º-A do CP brasileiro que protege a liberdade individual (inviolabilidade dos segredos, a privacidade das pessoas por via do respeito a intimidade da vida privada), ou seja, a tutela é individual e não tem a ver com a proteção da rede mundial de computadores e o seu regular funcionamento. Disponível em https://consultor-juridico.jusbrasil.com.br/noticias/100326806/o-novo-crime-de-invasao-de-dispositivo-informatico (Acedido aos 18-02-2020).

[398] **CRESPO**, Marcelo Xavier de Freitas. Crimes digitais. Saraiva. São Paulo, 2011. Disponível em https://books.google.co.ao/books?id=Px9nDwAAQBAJ&pg=PT71&lpg=PT71&dq=crime+de+Uso+abusivo+de+dispositivos&source=bl&ots=8aBtZgkdON&sig=ACfU3U2mDt6CCH_ivYVWkWVrYKIK5R95pg&hl=pt-PT&sa=X&ved=2ahUKEwiw0r-h6trnAhWPK7kGHXmqBjIQ6AEwC3oECAoQAQ#v=onepage&q=crime%20de%20Uso%20abusivo%20de%20dispositivos&f=false (Acedido aos 18-02-2020).

[399] Idem.

[400] A **Remote Access Trojan** (RAT) is a malware program that includes a back door for administrative control over the target computer. RATs are usually downloaded invisibly with a user-requested program – such as a game – or sent as an e-mail attachment. Once the host system is compromised, the intruder may use it to distribute RATs to other vulnerable computers and establish a botnet. Disponível em https://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan (Acedido aos 18-02-2020).

[401] Disponível em https://www.cambridge.org/core/books/principles-of-cybercrime/misuse-of-devices/42940535CBFE1E3834219EF14ADAACBD (Acedido aos 18-02-2020).

Por formas a ser evitada essa infração, a CM impõe aos vendedores de produtos tecnológicos a feitura, por intermédio de peritos em segurança informática, de testes para avaliar a segurança dos mesmos e divulgar aos potenciais consumidores as vulnerabilidades que forem detetadas (al. g) nº 1 do art.º 29º).

O nº 2 do art.º 29º da CM na sua al. a) acolhe o crime de *interceção ilegal* que sugere condenar quem "intercetar ou tentar intercetar fraudulentamente, através de meios técnicos, dados informatizados durante a sua transmissão não pública para, de ou dentro de um sistema informático".

Tal como o delito anterior, a interceção ilícita também não está previsto no ACP. Entretanto, por tratar-se de um crime de "violação de dados informatizados", assemelha-se a violação de telecomunicações do art.º 214º do ACP, já que ambos pressupõem uma atuação dolosa e desautorizada que resulte na "intromissão nas telecomunicações", causando deste modo a violação da privacidade das comunicações, ou seja, a violação ou a interceção enunciadas têm a ver duma forma geral com as transferências eletrónicas.

Contudo, distinguem-se ligeiramente pois no crime de violação de telecomunicações pune-se meramente a ingerência em telecomunicações que possibilite a tomada de conhecimento de conteúdos passíveis de serem divulgados, e não a simples interceção de dados transmitidos de forma não pública.

As interceções efetuadas por necessidades forenses e as realizadas por decisão judicial para servirem de evidências legais não constituem infrações. Nestas incluem-se ainda as ações dos serviços de inteligência, pois visam proteger e defender a segurança nacional.

Previsto no art.º 235º do ACP e nas al. b) e c) do nº 2 do art.º 29º da CM temos a *falsidade informática*[402]. É uma infração relacionada ao computador que atenta contra a fé pública e a sua previsão legal visa proteger não só o património do lesado como a segurança que deve existir nas relações jurídicas. As infrações ligadas a adulteração de identidades, obtenção de credenciais de usuários recorrendo aos ataques de *pharming* e do seu predecessor

[402] A falsificação relacionada a computadores envolve a representação de indivíduos, autoridades, agências e outras entidades legítimas *online* para fins fraudulentos. Os *cibercriminosos* podem passar-se por pessoas de organizações e agências legítimas, a fim de induzi-las a revelar informações pessoais e fornecer dinheiro, bens e/ou serviços. O remetente do *e-mail* finge pertencer a uma organização ou agência legítima na tentativa de fazer com que os usuários confiem no conteúdo e sigam as instruções do *e-mail*. O *e-mail* é enviado de um endereço de *e-mail* falsificado (projetado para parecer com um *e-mail* autêntico da organização ou agência) ou de um nome de domínio semelhante à organização ou agência legítima (com algumas pequenas variações). Disponível em https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html (Acedido aos 20-02-2020).

phishing[403] são ações que *grosso modo* preenchem os mais frequentes *modus operandi* desse ilícito penal.

Nos dois diplomas esse delito tem um tratamento praticamente idêntico. Tanto na convenção africana como no anteprojeto angolano criminaliza-se quem com a intenção de defraudar alguém proceder a "introdução, alteração, ou a supressão de dados informáticos", criando dados não verdadeiros com o propósito de serem usados para fins juridicamente relevantes como se de originais se tratassem.

Punem igualmente quem, mesmo não sendo o falsificador, fizer a utilização de dados que foram adquiridos de maneira enganosa (art.º 235º nº 2 do ACP e art.º 29º nº 2 al. c) da CM).

Outro crime relacionado ao computador que também decorre mediante a fraude e que está estabelecido conjuntamente no ACP e na CM é a *burla informática* (no art.º 407º ACP e nº 2 al. d) do art.º 29º CM). A burla tratada no ACP abrange não só a informática como também as telecomunicações. Algumas atuações – como os ataques de *phishing* – podem preencher concomitantemente o ilícito de burla informática e falsificação informática.

Os dois dispositivos legais sãos concordes em criminalizar a atuação que compreende "a obtenção fraudulenta, para si ou para outra pessoa, de qualquer benefício, por intermédio da introdução, alteração, eliminação ou supressão de dados informatizados".

Apesar desta parte coincidente, a CM termina utilizando uma expressão vaga ao mencionar que pune igualmente "qualquer forma de interferência no funcionamento de um sistema informático". Na mesma linha de ideia, mas com uma elaboração mais consentânea, o ACP criminaliza a "interferência no resultado de tratamento de dados". Tanto num como noutro caso exige-se que resulte numa vantagem patrimonial ilegítima ao autuante.

O nº 2 do art.º 29º da CM termina com duas alíneas. Primeiramente a al. e) que, tal como faz a al. a) do art.º 212º do ACP, pune o processamento negligente de dados pessoais. Só que a CM vai mais além, acrescendo que essa negligência, ou falta de precaução, tem a ver com a não consideração de certas "formalidades prévias de processamento". Estas formalidades constam no art.º 10º e de acordo ao nº 2, "o processamento de dados pessoais deve sujeitar-se

[403] **GONÇALVES**, Joana Margarida Andrade. *Pharming*: Análise dogmático-penal, em especial enquanto forma de lesão do património. Dissertação de Mestrado em Direito e Informática. Trabalho efetuado sob a orientação do Professor Doutor António Manuel Tavares de Almeida Costa e do Professor Doutor Victor Francisco Mendes de Freitas Gomes da Fonte. Universidade do Minho. Escola de Direito. Outubro de 2015, p. 20. Disponível em http://repositorium.sdum.uminho.pt/handle/1822/40931. (Acedido aos 20-02-2020).

a uma declaração da autoridade de protecção", que nos termos do nº 4 deliberará sobre a sua aceitação ou não quando tratarem de

a) Informações genéticas e à investigação na área de saúde;
b) Informações sobre infrações, condenações ou medidas de segurança;
c) Número nacional de identificação;
d) Informações biométricas; e
e) Dados de interesse público, nomeadamente para fins históricos, estatísticos ou científicos.

Seguidamente temos na al. f) – também sem similitude no ACP – não propriamente um crime mas a estatuição que impõe a responsabilização criminal de quem participar numa organização criminosa que tem por fim preparar ou cometer as infrações previstas na CM. A segunda parte do ponto 2 do nº 3 referente ao art.º 29º reforça esta consagração aludindo que as "infracções cometidas sob a égide de uma organização criminosa serão punidas com as penas máximas previstas para a infracção em causa." O combate à ciberguerra, ao ciberterrorismo[404] e à ciberespionagem faz parte dos objetivos dessa estatuição.

A seguir são regulados na CM os ditos delitos relacionados com conteúdos.

Nesta vertente a CM dá uma atenção especial à *pornografia infantil*. No seu art.º 1º das definições, começa precisamente por defini-la. A sua previsão consta no art.º 29º nº 3 ponto 1 al. a), b), c) e d). No ACP está previsto no art.º 184º.

Nos dois normativos prevêem-se a criminalização dos atos que consistem na produção, transmissão ou representação de pornografia infantil. Punem ainda a aquisição, a importação, a facilitação e o acesso a imagens de material desta natureza. Neste quesito só a CM pune a posse.

O ponto de dissonância reside na faixa etária correspondente à menoridade. A CM considera menor quem tenha menos de dezoito anos (art.º 1º). A pornografia infantil retratada no ACP fixa abaixo dos dezasseis anos (art.º 184º nº 5 al. b)), havendo a possibilidade de agravar-se a punição se a vítima tiver menos de catorze anos.

[404] Para uma melhor abordagem desta temática consulte-se **PINTO**, Marco Aurélio Gonçalves. Teoria relativista do ciberterrorismo. Academia Militar. Dissertação para a obtenção do grau de Mestre em Guerra da Informação. Trabalho realizado sob a supervisão: Orientador Professor Doutor Fernando Carvalho Rodrigues; Co-Orientador Professor Doutor João Pedro da Cruz Fernandes Thomaz. Lisboa 2011. Disponível em https://comum.rcaap.pt/bitstream/10400.26/6826/1/Ciberterrorismo_tese_VersFinal.pdf (Acedido aos 11-05-2020).

O delito que a seguir a CM prevê, mas o ACP não acolhe, é o de *racismo, xenofobia e outras formas de discriminação* feitas com recurso a sistemas informáticos (art.º 29º nº 3 ponto 1 al. e), f) e g)). Esta previsão parece-nos ter sido influenciada pelo Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adotado em Estrasburgo em 28 de Janeiro de 2003. Ali elencam-se várias formas de discriminação tal como racial, étnica, partidária, religiosa, política e familiar.

O art.º 29º encerra com o nº 4 que recomenda a punição das "infrações relativas às medidas de segurança das trocas comerciais electrónicas", identicamente sem correspondência no ACP, porém, de forma geral, qualquer dos crimes informáticos do ACP podem ter repercussões no âmbito do comércio eletrónico, por isso essa previsão da CM fica substancialmente consumida por qualquer dos delitos dependendo da situação em concreto, sendo irrelevante a sua não previsão.

Capítulo IV – OS CRIMES INFORMÁTICOS E AS CONDUTAS DELITUOSAS MAIS RELEVANTES LIGADAS ÀS TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO

4.1. Introdução

Os crimes informáticos são em regra cometidos por intermédio de façanhas tecnológicas também designadas por ataques informáticos, muitos dos quais ligados à engenharia social. Na sua maioria os atacantes aproveitam-se das falhas dos mecanismos de segurança e das vulnerabilidades dos próprios sistemas informáticos.

Neste capítulo apresentaremos de forma sintética algumas dessas ações específicas que têm sido utilizadas para o cometimento de algumas infrações informáticas previstas na CB ou no ACP.

Por formas a não sermos muito prolixos nem alargarmos excessivamente o âmbito do presente capítulo, trataremos somente das formas de perpetração que melhor se enquadram nos crimes informáticos, porém teremos o cuidado de selecionarmos aquela maneira que preencha significativamente o "comportamento desviante"[405] mais relevante.

Os ataques de negação de serviço e os ataques de negação de serviço distribuído já não serão objeto de estudo neste capítulo, uma vez que já foram analisados com alguma profundidade no capítulo anterior quando nos referirmos aos ataques efetuados contra o sistema informático da Sonangol, contra os *sites* oficiais de diversas instituições do Governo de Angola e contra o portal de notícias Maka Angola.

Assim, dentro das principais tecnologias usadas para a prática de crimes digitais – para além das atuações relacionadas com a pornografia infantil – estudaremos *o hacking (phishing e pharming), man-in-the-middle attack, sniffing* e *scamming.*

E por fim, para termos uma melhor panorâmica dos crimes cibernéticos mais frequentes em Angola, estudaremos a implementação e a constatação das técnicas delituosas na realidade deste país.

4.2. Principais tecnologias usadas para a prática de crimes digitais

4.2.1. Hacking

[405] Expressão utilizada pela Brigada de Investigação de Criminalidade Informática (BICI) da Polícia Judiciária. Disponível em http://www.4law.co.il/portu1.htm (Acedido aos 06-04-2020).

Hacking[406] é um termo genérico que designa uma vastidão de ações, que visam comprometer computadores e redes, perpetradas por qualquer forma de intromissão sem autorização de um dispositivo, rede ou servidor e que viole "a privacidade do seu administrador ou dos seus utilizadores e que vise danificar, ou de outro modo comprometer, propriedades como ficheiros, programas ou websites"[407].

As técnicas ligadas à engenharia social[408] têm sido igualmente utilizadas nas ações de hacking para invasão de computadores e sistemas, possibilitando mesmo o acesso a dados pessoais de usuários.

Sobre isso Ibekwe[409] faz duas observações que julgamos importantes. Na primeira entende que uma das intenções do hacking é "a obtenção de dados informáticos, acesso seguro a quaisquer programas, segredos comercial ou industrial ou informação classificada", na segunda menciona que uma prática habitual dos *hackers*[410] consiste na "utilização de um dispositivo para evitar a deteção ou identificação".

Ainda nessas atuações os *hackers* procuram a diversão, a satisfação da sua curiosidade ou a obtenção de algum benefício para si ou para outrem, explorando as vulnerabilidades que encontrem nos sistemas. Também tem sido notória a existência do hacking ligado ao ativismo político[411], tal como o registado nos ataques contra vários ministérios do governo angolano como repulsa a condenação de dezassete ativistas.

Facilmente damos conta que hacking é uma ação suscetível de afetar qualquer pessoa ou instituição que tenha um dispositivo conectado à Internet e decorre de diversas maneiras.

A sua classificação depende da intenção do *hacker*, sopesada na sua inofensividade ou lesividade.

São três os tipos fundamentais, sendo estes:

---

[406] Para mais informação sobre a evolução desse termo leia-se **PAVLIK**, Kimberly. Cybercrime, Hacking, And Legislation. Walden University, USA. Journal of Cybersecurity Research – 2017 Volume 1, Number 1, p. 14 e 15. Disponível em https://www.researchgate.net/publication/317270246_Cybercrime_Hacking_And_Legislation (Acedido aos 12-05-2020).

[407] Disponível em https://softwarelab.org/pt/hacking/ (Acedido aos 07-04-2020).

[408] A **engenharia social**, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais. Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança. Disponível em https://pt.wikipedia.org/wiki/Engenharia_social_(segurança) (Acedido aos 07-04-2020).

[409] **IBEKWE**, Chibuko Raphael. The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions. A Thesis Submitted to the School of Law, University of Stirling for the Degree of Doctor of Philosophy (PhD). July 2015, p. 97 e 99.

[410] "A computer hacker is a computer expert who uses their technical knowledge to achieve a certain goal, or overcome a certain obstacle, within a computerized system". Disponível em https://en.wikipedia.org/wiki/Hacker (Acedido aos 24-09-2020).

[411] Em inglês é designado por *hacktivism*.

1. ***White Hat Hacking (hacking de chapéu branco)*:** frequentemente chamado de "hacking ético ou cívico", é aquele utilizado para finalidades benignas.

   Geralmente são contratados por empresas no sentido de cooperarem para o melhoramento dos seus sistemas de segurança pela identificação das eventuais vulnerabilidades. Sendo assim, *grosso modo,* atuam com a autorização do administrador dos sistemas.

2. ***Black Hat Hacking (hacking de chapéu preto)*:** também designado de "hacking anti-ético", tem uma atuação contrária a anterior sendo geralmente movido por intentos financeiros, pessoais ou doutra natureza.

   Desta forma, a sua atuação decorre logicamente sem a devida permissão do administrador, usando para o efeito páginas *web* comprometidas e correios eletrónicos de *phishing* a fim de fazerem o *download* e instalarem *malware* nos computadores visados, tornando-os propensos a sofrerem furtos de informação diversa.

3. ***Gray Hat Hacking (hacking de chapéu cinzento):*** tem uma postura intermédia, situando-se entre os dois tipos supramencionados.

   Estes não são completamente maldosos, podendo normalmente aceder a uma rede sem permissão aproveitando-se das vulnerabilidades achadas e em seguida entrarem em contacto com o administrador, solicitando uma quantia monetária para poderem efetuar a correção das falhas existentes. Entretanto, importa referir que caso não sejam bem-sucedidos, podem partilhar as vulnerabilidades analisadas com os seus congéneres de chapéu preto.

São diversas as técnicas de hacking, mas genericamente têm a ver com "a distribuição de malware e campanhas de e-mail de phishing até vigilância e atividades organizadas de botnets"[412], entretanto tendo em conta a frequência estas podem ser resumidas em cinco[413]: WAP Falso, Keyloggers[414], Ataques DDoS, Phishing e Roubo de Cookies.

[412] Disponível em https://softwarelab.org/pt/hacking/ (Acedido aos 07-04-2020).
[413] Conforme enunciados no *site* anterior.
[414] São ferramentas baseadas em *hardware* ou *software* que permitem registar as teclas pressionadas no teclado das vítimas com a finalidade de roubar a sua informação pessoal.

Para nos protegermos dos ataques dos *hackers* devemos seguir as práticas recomendadas de cibersegurança, procurando sempre instalar nos nossos computadores os melhores programas de antivírus, provenientes de entidades de credibilidade reconhecida.

Nos casos de acedermos à Internet por via de uma rede pública, devemos recorrer a uma VPN (rede virtual privada) para impedir que os dados fiquem facilmente acessíveis.

Outros comportamentos que ajudam a bloquear esses ataques passam pelo não acesso a *links* anónimos, a correios eletrónicos desconhecidos nem à mensagens enviadas por pessoas estranhas. Verificar bem a originalidade da página antes de introduzir uma palavra-passe, principalmente em *sites* bancários, preferindo aqueles que sejam encriptados, recorrendo aos teclados virtuais sempre que tal seja possível, são outras condutas que devem ser tidas em conta.

De acordo com o art.º 2º da CB, o acesso a um sistema informático sem a devida autorização, tal como sucede no hacking, configura um crime de acesso ilegal[415]. Este delito cobre o essencial das ameaças perigosas que acarretam os ataques contra a segurança dos sistemas informáticos e dados[416], abrindo portas para o cometimento doutras infrações, sendo por isso um dos crimes informáticos mais antigo[417].

No ACP o hacking preenche parcialmente o ilícito penal de devassa por meio de informática por ser uma ação que pode igualmente consistir em "aceder, sem autorização a dados informaticamente tratados e que contenham informações individualmente identificáveis" (art.º 212º al. b)), tendo uma moldura penal abstrata de prisão até um ano ou de multa até 120 dias.

Para além destes dois crimes, as intrusões possibilitadas pelo hacking podem também permitir ao intruso ter acesso a informação confidencial dentro de um computador sem permissão[418], que frequentemente resultam em falsidade informática ou burla informática e nas telecomunicações previstas e punidas pelos art.ºs 235º e 407º do ACP, respetivamente.

Para melhores desenvolvimentos sobre o keylogger leia-se **NORMAN**, Alan T. Hacking: How to Make Your Own Keylogger in C++ Programming Language. Kindle Edition, 2017.

[415] O termo hacking é precisamente usado como sinónimo de "acesso não autorizado" ou "invasão informática". **MINAHIM**, Maria Auxiliadora de Almeida & **SPÍNOLA**, Luíza Moura Costa. A fraude cometida por meios informáticos sob o prisma da vitimodogmática. Revista de Direito Penal, Processo Penal e Constituição | e-ISSN: 2526-0200 | Maranhão | v. 3 | n. 2 | p. 144 - 160 | Jul/Dez. 2017. Double Blind Review pelo SEER/OJS. Recebido em: 29.11.2017. Aprovado em: 30.12.2017. Disponível em https://www.researchgate.net/publication/324086263_A_FRAUDE_COMETIDA_POR_MEIOS_INFORMATICOS_SOB_O_PRISMA_DA_VITIMODOGMATICA (Acedido aos 12-05-2020).

[416] **WALDEN**, Ian. Computer crimes and digital investigations. Second Edition. Oxford University Press. 2007, Chapter 3, p. 250.

[417] **TAYLOR**, Paul. 'Hacktivism: in search of lost ethics?' Crime and the Internet. Edited by David S. Wall, 2001, 59-73, p. 61.

[418] A título exemplar, em 2012, 117 milhões de contas do LinkedIn foram hackeadas e senhas e credenciais individuais foram roubadas por um cidadão russo preso em Praga em 2016. **KOTTASOVA**, Ivana. Arrested Russian linked to theft of 117 million LinkedIn passwords. CNN Tech. Disponível em http://money.cnn.com/2016/10/20/technology/russian-hacker-arrested-linkedin-password/ (Acedido aos 11-05-2020).

4.2.2. Phishing e pharming

Falaremos agora de uma das técnicas mais conhecidas de hacking, o phishing[419], bem como de um ataque avançado de phishing: o pharming.

Phishing[420] "é a tentativa fraudulenta de obter informações confidenciais como nomes de usuário, senhas e detalhes de cartão de crédito, por meio de disfarce de entidade confiável em uma comunicação eletrónica. Geralmente, é realizado por falsificação de e-mail ou mensagem instantânea, e muitas vezes direciona os usuários a inserir informações pessoais em um *site* falso, que corresponde à aparência do *site* legítimo"[421][422].

Atraem os *phishers* informações que contenham senhas, números de cartão de crédito e outros números de identificação do cidadão[423]; mas dentro destas as senhas de contas bancárias têm sido as preferenciais. As informações obtidas os atacantes usam-nas para perpetrar uma vastidão de ações criminosas em que se destacam a fraude, o roubo de identidade[424] e a espionagem corporativa.

Pelo exposto, fica claro que as fraudes engendradas pelo phishing visam frequentemente uma vantagem pecuniária, o que significa que "o principal efeito do *site* de phishing é o abuso de informações através do comprometimento dos dados do usuário que podem prejudicar as vítimas em forma de perdas financeiras ou valores"[425].

Os ataques de phishing devem ser encarados com elevada preocupação porque comparativamente a outras formas de ameaças da Internet, como *hackers* e vírus, é a que mais cresce rapidamente[426].

O phishing pode ser implementado de diversas maneiras nas quais destacamos como principais as seguintes[427]:

---

[419] É também uma técnica de "engenharia social".
Para Jakobsson o *Phishing representa* um casamento entre a tecnologia e a engenharia social, pelo que nós concordamos. Disponível em http://www.markus-jakobsson.com/ (Acedido aos 17-04-2020).

[420] Provém do vocábulo inglês *fishing*. É escrito com as letras ph em vez de f por ser a forma de escrita que os *hackers* frequentemente usam em suas linguagens quando interagem em ambientes próprios. O seu surgimento deve-se ao facto dos utilizadores, também designados *phish*, serem por esta via atraídos por uma comunicação imitada, caindo numa armadilha ou gancho que irá recuperar as suas informações confidenciais.

[421] Disponível em https://pt.wikipedia.org/wiki/Phishing (Acedido aos 24-09-2020).

[422] O que sucede é que o *phisher* tenta buscar fraudulentamente informações confidenciais ou sensíveis de usuários legítimos imitando comunicações eletrónicas de uma organização pública ou confiável de maneira automatizada. **JAKOBSSON** Markus & **MYERS**, Steven. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley-Interscience. 2006, p. 1.

[423] Idem.

[424] Topkara et. al. na sua definição de phishing consideram-no como sendo "an online identity theft", ou seja, uma forma de roubo de identidade online. **TOPKARA**, Mercan; **KAMRA**, Ashish; **ATALLAH**, Mikhail J. e **NITA-ROTARU**, Cristina. Viwid: Visible watermarking based defense against phishing. Digital Watermarking. Springer Link. 2005, p. 470. Disponível em https://link.springer.com/chapter/10.1007%2F11551492_36 (Acedido aos 17-04-2020).

[425] **JAKOBSSON** Markus; **MYERS**, Steven. Idem, p. 1 e 2.

[426] Idem.

1. *E-mail para e-mail*: quando alguém recebe um *e-mail* solicitando informações confidenciais a serem enviadas ao remetente.
2. *E-mail para website*: quando alguém recebe um *e-mail* incorporado ao endereço da *web* de phishing.
3. *Website a website*: quando alguém clica no *website* de phishing através de um mecanismo de pesquisa ou um anúncio *online*.
4. *Browser para website*: quando alguém digitou incorretamente um endereço de *website* legítimo em um navegador e depois se referiu a um *site* de phishing que tem uma semelhança semântica com o endereço da *web* legítimo.

A título de exemplo, o WannaCry[428] foi um tipo de phishing que teve repercussões mundiais alarmantes tendo o Eternal Blue por *exploit*; o Server Block Messenger é o vetor de ataque e as vulnerabilidades se prendem com as falhas da sua implementação.

Não obstante a perigosidade que o phishing representa, existem algumas medidas que podem ser tomadas para mitigar o seu potencial malévolo. Essas também são denominadas de "medidas anti-phishing"[429] e muitas delas já têm sido tomadas.

Por exemplo, a nível da indústria existe desde 2003 o Grupo de Trabalho Anti-Phishing (APWG da designação original inglesa, Anti-Phishing Working Group[430]) que é um consórcio internacional que reúne empresas afetadas por ataques de phishing, empresas de produtos e serviços de segurança, agências de aplicação da lei, agências governamentais, associações comerciais, organizações regionais de tratados internacionais e empresas de comunicação. Possui mais de 3200 membros de mais de 1700 empresas e agências em todo o mundo.

Dentre algumas das medidas a serem implementadas para a prevenção ou mesmo a deteção de phishing temos a colocação de extensões ou barras de ferramentas adicionais para navegadores, como recursos incorporados em navegadores e como parte da operação de *login*

---

[427] Utilizaremos as formas adotadas por Alnajim e Munro. **ALNAJIM**, Abdullah e **MUNRO**, Malcolm. An Approach to the Implementation of the Anti-Phishing Tool for Phishing Websites Detection. Intelligent Networking and Collaborative Systems. INCOS'09. International Conference. December 2009. IEEE, 105-112.

[428] O WannaCry é um *worm ransom ware* que se espalhou rapidamente através de várias redes de computadores em 12 de Maio de 2017. Para mais desenvolvimentos aceda-se o *link* https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (Acedido aos 20-04-2020).

[429] **BUTLER**, Rika. A framework of anti-phishing measures aimed at protecting the online consumer's identity. Stellenbosch University. October 2007. Disponível em https://www.researchgate.net/publication/220677176_A_framework_of_anti-phishing_measures_aimed_at_protecting_the_online_consumer's_identity (Acedido aos 20-04-2020).

[430] Disponível em https://en.wikipedia.org/wiki/Anti-Phishing_Working_Group (Acedido aos 20-04-2020).

do *site*. Tem utilidade semelhante a ferramenta Spoof Guard[431] que utiliza URL, imagens, nome de domínio e *link* para avaliar a probabilidade de falsificação.

O **Lucent Personalized Web Assistant** (LPWA)[432] é outra ferramenta que protege contra roubo de identidade e de informações pessoais do usuário e, para o feito, usa uma função para definir variáveis do usuário, como endereço de *e-mail*, nome de usuário e senha para cada servidor visitado pelo usuário, tal como faz o PwdHash[433].

Dynamic Security Skins[434] é outro tipo de anti-phishing baseado em navegador e garante a verificação de identidade de um servidor remoto por humanos, mas é difícil de ser falsificado por atacantes. Essa solução foi implementada com base no trabalho anterior sobre Provas Interativas Humanas[435], que emprega recursos distintos entre *sites* legítimos e falsificados por humanos.

O **Trust Bar**[436] é outra solução de certificação contra phishing. Os autores desta ferramenta propuseram a criação de uma Área de Credenciais Confiáveis (TCA, Trusted Credentials Area) que controla uma área significativa, localizada na parte superior de todas as janelas do navegador e é grande o suficiente para conter logotipos altamente visíveis e outros ícones gráficos para credenciais identificando uma página legítima. Embora a sua solução não dependa de fatores de segurança complexos, não evita os ataques de falsificação.

O phishing – quer tenha uma factualidade típica que consista na utilização indevida de senhas bancárias, no furto ou na usurpação da ciberidentidade[437] de outrem ou ainda noutra

---

[431] **CHOU**, N.; **LEDESMA**, R.; **TERAGUCHI**, Y.; **BONEH**, D. & **MITCHELL**, J. C. Client-side defense against web-based identity theft. 11th Annual Network and Distributed System Security Symposium (NDSS'04), San Diego, USA, 2004. Disponível em https://crypto.stanford.edu/SpoofGuard/webspoof.pdf (Acedido aos 20-04-2020).

[432] **GABBER**, E.; **GIBBONS**, P.B.; **KRISTOL**, D.M.; **MATIAS**, Y. & **MAYER**, A. Consistent, yet anonymous, Web access with LPWA. Commun. 1999. ACM 42, 42–47. Disponível em http://theory.stanford.edu/~matias/papers/lpwa-cacm.pdf (Acedido aos 20-04-2020).

[433] **ROSS**, B.; **JACKSON**, C.; **MIYAKE**, N.; **BONEH**, D. & **MITCHELL**, J. C. A browser plug-in solution to the unique password problem. Proceedings of the 14th USENIX Security Symposium. 2005.

[434] **DHAMIJA**, R. & **TYGAR**, J. D. The battle against phishing: dynamic security skins. ACM International Conference Proceeding Series, 77–88, 2005. Disponível em https://dl.acm.org/doi/10.1145/1073001.1073009 (Acedido aos 20-04-2020).

[435] **DHAMIJA**, R. & **TYGAR**, J. Phish and hips: human interactive proofs to detect phishing attacks. HIP, 69–83, 2005. Disponível em https://www.researchgate.net/publication/221342044_Phish_and_HIPs_Human_Interactive_Proofs_to_Detect_Phishing_Attacks (Acedido aos 20-04-2020).

[436] **GABBER**, E. et al. Idem.

[437] Para mais desenvolvimentos da temática relativa a usurpação da ciberidentidade consulte-se **SILVA,** Flávio Manuel Carneiro da. A usurpação da ciberidentidade. *Dissertação de Mestrado em Direito Criminal, realizada sob a orientação do Exmo. Senhor Professor Doutor José M. Damião da Cunha.* Porto, 2014.

forma de atuação – pode preencher diversos ilícitos penais. Aqui iremos referenciar alguns destes tipos legais que podem estar associados ao phishing.

No caso da criação de páginas *web* ou de nomes de domínio totalmente análogas aos de determinadas instituições bancárias, visando induzir o cliente a aceder à páginas defraudadas crendo serem as originais, estaremos na presença do crime de falsidade informática[438] (art.º 235º do ACP e art.º 7º da CB), pois que o *phisher* provoca engano nas relações jurídicas atingindo especificamente "a segurança das transações bancárias"[439], ludibriando o utilizador pela interferência no tratamento de dados.

O envio massivo de *e-mails* pode "infetar" o computador do usuário tão logo ele os abra, e após esse ato o "atacante" poderá aceder ilegitimamente de forma remota o computador, incorrendo no cometimento do ilícito de acesso ilegal (art.º 2º da CB) que é uma ameaça à segurança (confidencialidade, integridade e disponibilidade) dos sistemas informáticos[440]. Se esse acesso incidir sobre informações individualmente identificáveis então preencherá a infração de devassa por meio de informática (art.º 212 al. b) do ACP).

Registando-se o processo de contaminação do computador da vítima perpetrado por agentes do crime através do uso de tecnologia[441], mormente programas informáticos, em que se manipula de certa forma o sistema operativo, afetando o *browser* (Internet Explorer) de navegação, por representar uma interferência em dados estaremos na presença do delito de dano informático (art.º 399º do ACP e art.º 3º da CB), ademais afeta a capacidade de uso.

Se por exemplo – da ação supramencionada – depois da infeção do computador da vítima houver a tomada de credenciais bancárias da mesma e o acesso à sua conta bancária por via da Internet, e destas ações resultar em prejuízo patrimonial a vítima então teremos no caso o crime de burla informática[442] (art.º 407º do ACP e art.º 8º do CB).

---

[438] **TEIXEIRA**, Paulo Alexandre Gonçalves. Dissertação para obtenção do grau de Mestre em Direito, especialidade em Ciências Jurídico-Criminais. Universidade do Minho. Orientado pelo Prof. Doutor Fernando Conde Monteiro. Fevereiro, Lisboa, 2013, p. 19.

[439] Com base no nº 2 *in fine* do Acórdão do Tribunal da Relação de Lisboa de 09-01-2007, Proc. 5940/2006-5, "no crime de falsidade informática o bem jurídico protegido é o da segurança nas transacções bancárias". Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/ac54d66fd7a768ff80257287003f73d8?OpenDocument (Acedido aos 15-07-2020).

[440] **VENÂNCIO**, Pedro Dias. Idem, p. 59.

[441] **TEIXEIRA**, Paulo Alexandre Gonçalves. O fenómeno do *phishing* enquadramento jurídico-penal. Idem, p. 40.

[442] Paulo Teixeira acha que a burla informática assenta nos seguintes passos:

- envio das mensagens enganosas, com o intuito de induzir a vítima a abrir o e-mail e a descarregar/executar um programa (a pretexto de segurança acrescida), ou a aceder a um sítio onde descarrega esse mesmo programa;
- instalação do programa no computador, no qual irá alterar o *browser* para redirecionar a vítima para o sítio falso;
- utilização de dados sem autorização (a utilização indevida de *username* e *password*) para aceder à conta bancária da vítima através do serviço de homebanking;
- execução da(s) transferência(s) bancária(s) para conta(s) de destino.

TEIXEIRA, Paulo Alexandre Gonçalves. O fenómeno do *phishing* enquadramento jurídico-penal. Idem, p. 46.

Pharming[443] é um "ataque avançado de phishing"[444] baseado na técnica de envenenamento do cache do servidor DNS que consiste em corromper o DNS em uma rede de computadores fazendo com que a URL de um *site* passe a apontar para um servidor diferente do original[445][446].

É também utilizado para o furto de identidade *online* e de informações confidenciais (nomes de usuário e senhas), podendo ser realizado no lado do cliente ou na Internet, usando técnicas complexas e bem projetadas que tornam o ataque geralmente impercetível ao usuário[447].

O que sucede praticamente é a manipulação do tráfego de um *site*, já que o usuário pretendendo ter acesso a um *site* legal, o seu navegador é redirecionado para uma página defraudada, ou seja, a URL aponta para um servidor diferente do legítimo.

Neste tipo de ataque cibernético o *hacker* geralmente comporta-se de duas maneiras[448]:

1- Instala no computador do usuário um vírus ou cavalo de Tróia que altera o arquivo *host*[449] do computador para desviar o tráfego de seu destino para um *site* falso.

2- "Envenena" um servidor DNS, fazendo com que vários usuários acedam ao *site* falso sem querer. Os *sites* falsos podem ser usados para instalar vírus ou cavalos de Tróia no computador do usuário, ou podem tentar coletar informações pessoais e financeiras para roubar identidades.

Quanto ao enquadramento penal[450], o pharming por representar a manipulação de dados informáticos pode configurar o ilícito de falsidade informática (art.º 235º do ACP e 7º da CB) e tem sido muito utilizado para fraude de identidades, obtenção de credenciais de usuários bem

---

[443] O vocábulo "pharming" é um neologismo baseado na aglutinação das palavras "farming" e "phishing".

[444] **PATEL**, Jayshree & **PANCHAL**, S. D. A survey on Pharming attack Detection and prevention Methodology. IOSR Journal of Computer Engineering (IOSR-JCE). e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 1 (Jan. - Feb. 2013), p. 66.

[445] Disponível em https://pt.wikipedia.org/wiki/Pharming (Acedido aos 24-09-2020).

[446] Por outras palavras podemos dizer que "corresponde a um tipo específico de phishing, cujo intuito é corromper o Domain Name System (DNS), responsável, em linhas gerais, por localizar e traduzir os endereços dos *sites* digitados nos navegadores". Disponível em http://netspeed.com.br/mais/blog/empreendedorismo/empresarial/qual-a-diferenca-entre-phishing-e-pharming-2/ (Acedido aos 30-04-2020).

[447] **GASTELLIER-PREVOST**, Sophie; **GRANADILLO**, Gustavo Gonzalez & **LAURENT**, Maryline. A Dual Approach to Detect Pharming Attacks at the Client-Side · DOI: 10.1109/NTMS.2011.5721063 · Source: IEEE Xplore Conference: New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference March 2011.

[448] Conforme descrito em https://www.kaspersky.com.br/resource-center/definitions/pharming (Acedido aos 30-04-2020).

[449] Mais preocupante do que os ataques de arquivos *host* é o comprometimento de um roteador de rede local.
Como a maioria dos roteadores especifica um DNS confiável para os clientes quando eles ingressam na rede, as informações erradas aqui prejudicarão as pesquisas para toda a LAN.
Ao contrário das reescritas de arquivos *host*, é difícil detetar o comprometimento do roteador local.
Os roteadores podem transmitir informações incorretas de DNS de duas maneiras: configuração incorreta das definições existentes ou *firmware*. Disponível em https://pt.wikipedia.org/wiki/Pharming (Acedido aos 30-04-2020).

[450] Para melhores desenvolvimentos sobre o enquadramento penal do pharming leia-se **GONÇALVES**, Joana Margarida Andrade. *Pharming*: Análise dogmático-penal, em especial enquanto forma de lesão do património. Dissertação de Mestrado em Direito e Informática. Trabalho efetuado sob a orientação do Professor Doutor António Manuel Tavares de Almeida Costa e do Professor Doutor Victor Francisco Mendes de Freitas Gomes da Fonte. Universidade do Minho. Escola de Direito. Outubro de 2015. Disponível em http://repositorium.sdum.uminho.pt/handle/1822/40931 (20-02-2020).

como para aceder a redes de pagamentos e de transferências monetárias como indica o Acórdão do STJ de 18/12/2013[451].

4.2.3. Man-In-The-Middle Attack

Em criptografia, e segurança de computadores, o *man-in-the-middle attack* (MITM[452]) – em tradução livre para português "ataque homem no meio" (em alusão ao atacante que vai intercetando os dados) – é uma das práticas mais frequentes de ataque perpetrada contra as redes de computadores e, em regra, atingem não só pessoas como também empresas e grandes organizações.

Verifica-se quando o atacante transfere ou altera a correspondência entre duas pessoas que julgam estar em comunicação direta, com o objetivo de adquirir informações individuais tais como certificações de *login*, pontos de interesse da conta e números de cartão de cobrança. Os alvos são normalmente clientes de aplicativos financeiros, negócios de SaaS, locais de negócios baseados na Web e outros *sites* que exigem *login*.[453]

Um exemplo de ataque do MITM é a espionagem ativa, na qual o invasor faz conexões independentes com as vítimas e transmite mensagens entre elas para fazê-las acreditar que estão conversando diretamente entre si por uma conexão privada, quando na verdade toda a conversa é controlada por ele. Neste caso, o atacante deve ser capaz de intercetar todas as mensagens relevantes que passam entre as duas vítimas e injetar novas[454].

O que acima referimos sucede de forma imediata em muitas circunstâncias. Por exemplo, um invasor que se insere no ponto de acesso dentro do alcance da receção de uma rede Wi-Fi não criptografada[455].

Visto ter por fito burlar a autenticação mútua, um ataque MITM será bem-sucedido somente se o atacante personificar cada ponto de extremidade suficientemente bem para satisfazer suas expectativas, por isso é recomendável o uso de protocolos criptográficos com

---

[451] Disponível em www.dgsi.pt (Acedido em 03.01.2020).

[452] São igualmente usadas outras abreviações como MitM, MiMor e MIM. Veja-se **WALLACE**, Brian Michael, and **MILLER**, Jonathan Wesley. "End point-based man in the middle attack detection using multiple types of detection tests." U.S. Patent 9,680,860, issued June 13, 2017.Ouainda Khader, A. S., & Lai, D. (2015). Preventing man-in-the-middle attack in Diffie-Hellman key exchange protocol. In 22nd International Conference on Telecommunications: ICT 2015 (p. 204). Engineers Australia.

[453] Avijit **MALLIK**, Abid **AHSAN**, Mhia Md. Zaglul **SHAHADAT** and Jia-Chi **TSOU**. Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science. January 2019, p. 77. Disponível em https://www.researchgate.net/publication/330249434_Man-in-the-middle-attack_Understanding_in_simple_words (Acedido aos 23-04-2020).

[454] Disponível em https://pt.wikipedia.org/wiki/Ataque_man-in-the-middle (Acedido aos 23-04-2020).

[455] **CALLEGATI**, Franco; **CERRONI**, Walter & **RAMILLI**, Marco (2009). "Man-in-the-Middle Attack to the HTTPS Protocol". *IEEE Security & Privacy Magazine*. **7**: 78 – 81.

autenticação de terminal, como sucede com o TLS (Transport Layer Security) que autentica ambas as partes usando uma autoridade de certificação mutuamente confiável[456].

Para controlarem os dispositivos os cibercriminosos podem usar vários tipos de ataques MITM, nestes destacamos os seguintes[457]:

1. IP spoofing ou *IP address spoofing*[458] *(Falsificação de IP* ou *falsificação de endereço IP)* – Todo dispositivo capaz de se conectar à Internet possui um endereço IP (Protocolo de Internet), que é semelhante ao endereço da sua casa. Ao falsificar um endereço IP, um invasor pode induzir a vítima a pensar que está interagindo com um *site* ou com alguém que não é, pode ainda dar ao invasor acesso à informações que de outra forma não seria compartilhada.

2. DNS spoofing ou *DNS cache poisoning*[459] *(Falsificação de DNS* ou *envenenamento de cache DNS)* – O spoofing do DNS (Domain Name Server) é uma técnica que força o usuário a um *site* falso, em vez do *site* real que ele pretende visitar. A vítima pode pensar que está visitando um *site* seguro e confiável quando na verdade está interagindo com um fraudador. O objetivo do autor é desviar o tráfego do *site* real ou capturar credenciais de *login* do usuário.

3. HTTPS spoofing (Falsificação de HTTPS) – Ao fazer negócios na Internet, visualizar "HTTPS" no URL, em vez de "HTTP", é um sinal de que o *site* é seguro e confiável. De fato, o "S" significa "seguro"[460]. Um invasor pode enganar seu navegador, fazendo-o crer que está visitando um *site* confiável quando não está. Ao redirecionar seu navegador para um *site* não seguro, o invasor pode monitorar suas interações com esse *site* e possivelmente roubar informações pessoais que está compartilhando.

4. SSL hijacking (Sequestro de SSL) – Quando o dispositivo se conecta a um servidor não seguro – indicado por "HTTP" – o servidor geralmente pode redirecioná-lo automaticamente para a versão segura do servidor, indicada por "HTTPS". Uma conexão com um servidor seguro significa que existem protocolos de segurança padrão, protegendo os dados compartilhados com

---

[456] Idem.

[457] Seguimos os tipos constantes em https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html (Acedido aos 23-04-2020) por serem mais abrangentes. Noutros estudos encontramos uma quantidade inferior de tipos pelo que preterimos.

[458] Designação adotada na p. 185 de **JOHN**, Emil Kuriakose e **THASEEN**, Sumaiya. Efficient defense system for ip spoofing in networks vit. University, Chennai, Tamil Nadu, India. October 2012. Disponível em https://www.researchgate.net/publication/268585450_Efficient_Defense_System_for_IP_Spoofing_in_Networks (Acedido aos 23-04-2020).

[459] Disponível em https://en.wikipedia.org/wiki/DNS_spoofing (Acedido aos 23-04-2020).

[460] Ou "*secure*" do original em inglês.

esse servidor. SSL significa Secure Sockets Layer, um protocolo que estabelece *links* criptografados entre o navegador e o servidor da *web*.

Em um SSL hijacking, o invasor usa outro computador e servidor seguro e intercepta todas as informações que passam entre o servidor e o computador do usuário.

5. E-mail hijacking (Sequestro de e-mail) – Às vezes, os cibercriminosos têm como alvo contas de e-mail de bancos e outras instituições financeiras. Depois de obterem o acesso, eles podem monitorar as transações entre a instituição e seus clientes. Os atacantes podem falsificar o endereço de *e-mail* do banco e enviar suas próprias instruções aos clientes, isso convence o cliente a seguir as instruções dos destes e não as do banco. Como resultado, um cliente inconscientemente pode acabar colocando dinheiro nas mãos dos meliantes.

6. Wi-Fi eavesdropping (espionagem de Wi-Fi) – Os criminosos cibernéticos podem configurar conexões Wi-Fi com nomes aparentemente legítimos, semelhantes a uma empresa próxima. Depois que um usuário se conectar ao Wi-Fi do fraudador, este poderá monitorar a atividade *online* daquele e intercetar credenciais de *login*, informações de cartão de pagamento e muito mais. Esse é apenas um dos vários riscos associados ao uso de Wi-Fi público.

7. Stealing browser cookies (Furto de cookies do navegador) – Para entender o risco de *cookies* roubados do navegador, precisa-se entender o que é. Um *cookie* do navegador é uma pequena informação que um *site* armazena no seu computador. Por exemplo, um retalhista *online* pode armazenar as informações pessoais inseridas e os itens do carrinho de compras que selecionamos em um *cookie*, para que não precisemos digitar novamente essas informações ao retornar.

Um cibercriminoso pode sequestrar esses *cookies* do navegador. Como os *cookies* armazenam informações da sua sessão de navegação, os atacantes podem obter acesso às senhas, endereço e outras informações confidenciais.

A autenticação e a deteção ou verificação de violação são os dois principais meios que podemos recorrer para nos prevenirmos dos ataques MITM. A primeira fornece um certo grau de certeza de que uma determinada mensagem veio de uma fonte legítima; a segunda somente apresenta evidências de que uma mensagem pode ter sido alterada.

Nos métodos de autenticação temos a exigência de troca de informações tal como ocorre nas chaves públicas (PK) e o uso de um canal que seja seguro. São igualmente recomendáveis: o uso de uma infraestrutura de chave pública (como TLS) e o método da autenticação mútua.

Na detecção de violação realça-se o uso do exame de latência (*e.g.* funções de *hash*) principalmente em situações que envolvem transações. Também os protocolos baseados na criptografia quântica são de elevada utilidade.

A criptografia quântica, em teoria, fornece evidência de violação para transações através do teorema da não-clonagem[461].

Os protocolos baseados na criptografia quântica tipicamente autenticam parte ou toda a sua comunicação clássica com um esquema de autenticação incondicionalmente seguro, por exemplo Autenticação Wegman – Carter[462].

A análise forense de rede[463] é outro recurso relevante que nos pode facultar evidências[464] importantes em caso de suspeita de ataque principalmente quando envolve a captura de tráfego de rede.

Outras ações que podem impedir os ataques MITM envolvem[465]:

---

[461] Igualmente utilizado nas transações por Bitcoin como se pode ler em **JOGENFORS**, Jonathan. Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics. Information Coding Group, Department of Electrical Engineering. Linköping University. April 2016.
Disponível em https://www.researchgate.net/publication/299749136_Quantum_Bitcoin_An_Anonymous_and_Distributed_Currency_Secured_by_the_No-Cloning_Theorem_of_Quantum_Mechanics (Acedido em 24-04-2020).

[462] Para mais desenvolvimentos sobre essa forma de autenticação e da necessidade que a QKD (Quantum Key Distribution) precisa de autenticação ITS (Information-theoretically secure) para impedir ataques man-in-the-middle leia-se **ABIDIN**, Aysajane **LARSSON**, Jan-Ake. Direct Proof of Security of Wegman-Carter Authentication with Partially Known Key. Department of Electrical Engineering, Linköping University, SE-581 83 Linköping, Sweden. 2013.
Disponível em https://eprint.iacr.org/2013/126.pdf (Acedido em 24-04-2020).

[463] Nesta obra os autores apresentam o método que designam por ***Live Forensic*** na p. 67. **SAPUTRA**, Dedy e **RIADI**, Imam. Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method· International Journal of Cyber-Security and Digital Forensics (IJCSDF) 8(1): 66-73. The Society of Digital Information and Wireless Communications (SDIWC), 2019 ISSN: 2305-001. May 2019.
Disponível em https://www.researchgate.net/publication/333198147_Network_Forensics_Analysis_of_Man_in_the_Middle_Attack_Using_Live_Forensics_Method (Acedido em 24-04-2020).

[464] E estas evidências compreendem:

Endereço IP do servidor
Nome DNS do servidor
Certificado X.509 do servidor
O certificado é autoassinado?
O certificado é assinado por uma CA confiável?
O certificado foi revogado?
O certificado foi alterado recentemente?
Outros clientes, em outras partes da Internet, também obtêm o mesmo certificado?

Consultado em https://pt.wikipedia.org/wiki/Ataque_man-in-the-middle (Acedido em 24-04-2020).

[465] Com base nas formas constantes em https://www.forcepoint.com/cyber-edu/man-in-the-middle-attack (Acedido em 24-04-2020).

- Implementar uma solução abrangente de segurança de e-mail.
- Implementar uma solução de segurança da Web.
- Educar os utilizadores.
- Manter as credenciais seguras.

Em termos de enquadramento legal, os ataques MITM podem preencher vários tipos penais de acordo ao caso específico e os danos emergentes. Por exemplo, no caso de resultar na obtenção de códigos de acesso a senhas e outras informações confidenciais, estamos na presença do crime de acesso ilegal; no caso de espionagem para além do acesso ilegal teremos a interceção ilegítima; ademais, se a espionagem possibilitar ao defraudador intercetar credenciais de *login* bancários e depois efetuar pagamentos *online* então o crime será o de burla informática; quando registamos alterações na correspondência ou a falsificação de endereço IP o crime é de falsificação informática.

4.2.4. Sniffing (Farejador ou analisador de pacotes)

O ataque de sniffing representa um furto ou interceção de dados, capturando o tráfego de rede e utilizando um sniffer[466], ou seja, é o processo que consiste em monitorar e capturar os pacotes que trafegam por uma determinada rede fazendo recurso a ferramentas de sniffing[467].

Pode ser utilizado para diversas finalidades, muitas das quais benignas tais como o "gerenciamento de rede, monitoramento e diagnóstico de ambientes computacionais"[468]. As empresas usam-no igualmente para controlar o uso de redes pelos funcionários, prevenir que vírus infetem computadores bem como limitar a disseminação de *malware*.

Também nas utilizações benignas devemos referenciar a utilização da técnica[469] denominada por sniffing de rede[470] no âmbito da análise forense.

---

[466] É um aplicativo destinado a capturar pacotes de rede. Permite ao invasor examinar a rede e adquirir informações que lhe possibilitam entravar ou corromper a rede, ou ainda fazer a leitura das comunicações que ocorrem nela.

[467] Algumas das ferramentas mais sonantes usadas no sniffing são: Wireshark, Tcpdump, Dsniff, Network Miner e Kismet. Mas para além destes temos outros de menor expressão como Ether Ape, Fiddler, Omni Peek, PRTG Network monitor. Disponível em https://intellipaat.com/blog/tutorial/ethical-hacking-cyber-security-tutorial/sniffing-attacks/ (Acedido aos 15-04-2020).

[468] Disponível em https://pt.wikipedia.org/wiki/Analisador_de_pacotes (Acedido aos 15-04-2020).

[469] Algumas técnicas mais sonantes de sniffing são: MAC Flooding, DHCP Attacks, DNS Poisoning, Spoofing Attacks e ARP Poisoning. Disponível em https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing.htm (Acedido aos 15-04-2020).
Para mais desenvolvimentos sobre essa temática leia-se **CASAGRANDE**, Rogério Antônio. Técnicas de detecção de sniffers. Dissertação submetida à avaliação, como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação. Sob orientação do Prof. Doutor Raúl Fernando Weber. Porto Alegre, Outubro de 2003. Disponível em https://www.lume.ufrgs.br/bitstream/handle/10183/3423/000400345.pdf (Acedido aos 16-04-2020).

[470] O sniffing de rede, ou sniffing de pacotes, é uma técnica usada por investigadores para capturar pacotes de dados sendo transferidos através de uma rede. Esses pacotes são então registrados e analisados.

No entanto esse ataque destaca-se mais pela sua utilização maliciosa, uma vez que a captura de tráfego de rede permite: a obtenção de cópias de arquivo importantes durante a transmissão, a aquisição de senhas que facilitam alargar o âmbito da penetração de um ambiente invadido e a visualização de conversações em tempo real[471]. Tem ainda servido para permitir ter informações respeitantes a contas bancárias alheias.

Para evitar um ataque desta natureza é imperioso criptografar os pacotes de dados que são transmitidos.

Este tipo de ataque tem semelhança com o toque em fios telefónicos com o objetivo de saber o que se conversa e, por esta razão, podemos dizer que configura uma forma de escuta telefónica aplicada à rede de computadores[472].

Existem dois tipos diferentes de sniffing[473]:

1- *Sniffing ativo:* É o processo de Sniffing no switch. Um switch é um dispositivo de rede ponto a ponto. O switch regula o fluxo de dados entre suas portas, monitorando ativamente o endereço MAC em cada porta, o que ajuda a transmitir dados apenas para o alvo pretendido. Para capturar o tráfego entre os sniffers alvo, é necessário injetar ativamente o tráfego na LAN para permitir o sniffing do tráfego. Isso pode ser feito de várias maneiras.

Por exemplo, pode envolver o lançamento de um ataque de spoofing ARP (Address Resolution Protocol) ou um ataque de inundação de tráfego contra um switch para capturar o tráfego[474].

2- *Sniffing passivo:* Esse é o processo de Sniffing através do hub[475]. Qualquer tráfego que esteja passando pelo segmento de rede não comutado ou não-híbrido pode ser visto por todas as máquinas desse segmento. Sniffers operam na camada de enlace de dados da rede. Todos os dados enviados pela LAN são realmente enviados para cada máquina conectada

---

Um dos mais populares sniffers de rede é o Wireshark que está disponível gratuitamente e os seus desenvolvedores disponibilizaram o seu código-fonte. O Wireshark permite a captura de pacotes, o registro de tráfego e a análise individual de pacotes. Publicado no Portal GSTI, escrito por André Rodrigues, disponível em https://www.portalgsti.com.br/2018/11/sniffing-de-rede.html (Acedido aos 16-04-2020).

[471] Idem com a referência 12.

[472] Disponível em https://en.wikipedia.org/wiki/Sniffing_attack (Acedido aos 15-04-2020).

[473] Usamos as definições disponíveis em https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types (Acedido aos 16-04-2020).

[474] Disponível em https://www.skillset.com/questions/how-is-sniffing-usually-categorized (Acedido aos 16-04-2020).

[475] A boa notícia é que os *hubs* estão quase obsoletos hoje em dia. A maioria das redes modernas usa comutadores. Portanto, sniffing passivo não é mais eficaz. Disponível em https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing.htm (Acedido aos 15-04-2020).

à LAN. É chamado de passivo, pois os sniffers colocados pelos atacantes esperam passivamente que os dados sejam enviados e então os capturam.

Sniffing passivo envolve ouvir e capturar tráfego, mas não interagir com ele[476].

Tal como os próprios nomes indicam – o sniffing ativo é facilmente detectável; o passivo não é[477].

Fazendo recurso a ferramentas de deteção, os invasores podem aceder à informações classificadas, abarcando o tráfego de correio eletrónico (SMTP, POP, tráfego IMAP), tráfego da Web (HTTP), tráfego FTP[478], etc.

O Packet Sniffer[479] usualmente fareja os dados da rede sem efetuar qualquer alteração nos pacotes; estes podem simplesmente observar, exibir e registrar o tráfego, e essas informações podem ser acedidas pelo atacante. Outrossim é possível configurá-los de duas formas[480]:

- ✓ O **sniffer "não filtrado"** em que capturam todos os pacotes possíveis e os gravam em um disco rígido local para posterior exame.
- ✓ O **sniffer "filtrado"**, no qual os analisadores capturam apenas pacotes que contêm elementos de dados específicos.

Para além da forma de prevenção anteriormente mencionada, recomenda-se às organizações, bem como aos utilizadores, a absterem-se de aplicativos que utilizem protocolos que não se revelem seguros, como aqueles que tenham ainda a forma de autenticação básica do tipo HTTP, FTP (File Transfer Protocol) e Telnet. No lugar destes deve preferir-se fazer recurso dos chamados protocolos seguros, como HTTPS, SFTP (Secure File Transfer Protocol) e SSH (Secure Shell).

Uma outra contramedida de relevo é a utilização de switches no lugar de hubs, o que dificulta os sniffers e melhora o desempenho da rede[481].

---

[476] Idem.
[477] Idem.
[478] Idem com a referência 15.
[479] Também designado Packet Analyzer, Protocol Analyzer ou Network Analyzer. Vide https://usa.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer (Acedido aos 15-04-2020).
[480] Idem.
[481] Disponível em http://index-of.es/Sniffers/Sniffers_pdf/Cap6-Sniffers.pdf (Acedido aos 16-04-2020).

Em situações que obriguem o uso de protocolos inseguros, em quaisquer aplicativos, aconselha-se encriptar toda a transmissão de dados efetuada, ou ainda utilizar uma VPN (redes privadas virtuais).

Nos termos da Convenção de Budapeste, um ataque de sniffing sendo uma forma de intercetar ilícita e intencionalmente dados informáticos, "comprometendo a confidencialidade dos dados em tráfego e a segurança das redes"[482], configura por excelência uma infração de interceção ilegítima[483] prevista e punida pelo art.º 3º, ademais preenche também o crime de acesso ilegítimo estabelecido no art.º 2º.

No ACP esse ataque pode preencher o ilícito penal de violação de telecomunicações do art.º 214º (ou o crime comum de violação de correspondência[484] do art.º 213º), desde que a intromissão possibilite ter conhecimento do conteúdo que trafega na rede. Além disso, se do sniffing suceder a interceção de informações que sejam individualmente identificáveis então representará a infração de devassa por meio de informática, constante na al. b) do art.º 212º.

4.2.5. Scamming

O termo scamming provém do verbo inglês *scam*, que representa a ação de defraudar, sendo que a mesma palavra pode significar um esquema fraudulento[485].

Este tipo de ataque ligado a engenharia social representa na verdade um "ato de valer-se de meio informático para atuar com o intuito de obter alguma vantagem sobre o usuário"[486].

Trata-se geralmente de golpes ou armadilhas que são concebidos pelos scammers para que os utilizadores que tenham conhecimentos deficientes sobre o meio informático acabem por atuar de acordo com o desiderato do *cibercriminoso*.

Um dos tipos mais conhecidos de scamming é a designada **fraude nigeriana**[487] ou **advance-fee scam** (golpe de taxa antecipada). "É um truque de confiança no qual as vítimas

---

[482] **HORA**, Evandro Curvelo. Sobre a detecção remota de sniffers para detectores de intrusão em redes TCP/IP: Dissertação de Mestrado em Ciência da Computação. Orientado por Fábio Bueno Queda da Silva. Universidade de Pernambuco. Recife, Dezembro de 1999. Disponível em https://repositorio.ufpe.br/bitstream/123456789/2550/1/arquivo4949_1.pdf (Acedido aos 15-04-2020).

[483] Nuno de Carvalho considera mesmo o sniffing como sendo sinónimo de intecepção ilegítima. **CARVALHO**, Nuno. Organizações e segurança informática. Editora Lugar da Palavra. Setembro de 2009, p. 24.
Na mesma senda, o parecer do Conselho Superior da Magistratura do Ministério Público de 9 de Abril de 2009 sobre o Anteprojecto de Proposta de Lei do Cibercrime, cujo relator foi Joel Timóteo Ramos Pereira, diz que o sniffing enquadra-se totalmente no crime de interceptação. Disponível em https://www.csm.org.pt/ficheiros/pareceres/2009/parecer09_05.pdf (Acedido aos 16-04-2020).

[484] **SOTTO-MAYOR**, Belmiro; **FERREIRA**, Paulo e **LESSA** André. Aspectos sociais da informática, criminalidade informática – desafios de uma nova geração. Faculdade de Engenharia da Universidade do Porto. Trabalho realizado no âmbito da disciplina de Aspectos Sociais da Informática, leccionada por Manuel Veiga de Faria. Maio de 2006, p. 11. Disponível em https://egov.ufsc.br/portal/sites/default/files/aspectos_sociais_da_0.pdf (Acedido aos 16-04-2020).

[485] **SYDOW**, Spencer Toth. Crimes informáticos e suas vítimas. São Paulo: Saraiva, 2015, p. 125.

[486] **MINAHIM**, Maria Auxiliadora de Almeida & **SPÍNOLA**, Luíza Moura Costa. Op. cit, p. 150.

são persuadidas a avançar somas relativamente pequenas de dinheiro na esperança de obterem um ganho muito maior"[488]. No caso de a vítima fazer o pagamento, o atacante inventa uma série de taxas adicionais ou simplesmente desaparece[489].

Esses golpes são frequentemente muito bem elaborados e assim parecem muito convincentes, por isso na generalidade os atacantes têm sido bem-sucedidos, resultando em prejuízos avultados para as vítimas.

Os fraudadores visam as potenciais vítimas enviando *e-mails* ou interagindo em painéis de discussão e sistemas de mensagens instantâneas (tais como Yahoo messenger, MSN messenger) enquanto na verdade ocultam as suas reais identidades.

Para além da fraude nigeriana existem outros tipos de scamming e os mais comuns são employment scams, lottery scams, online sales and rentals, e romance scams. A seguir passaremos a estudar cada um deles.

Employment scams[490] ou *golpes de emprego*: direciona-se a pessoas que apresentam os seus currículos *online* para efeitos de obtenção de emprego. Numa das formas de atuação o atacante envia uma carta com o logotipo adulterado da empresa, a oferta de emprego comummente indica salários e outros bonos adicionais e solicita a vítima que dê autorização para trabalhar num dado país e inclui nesta oferta o endereço de um falso funcionário do governo para entrar em contato. Este falso funcionário do governo passa a forçar a vítima, extraindo taxas pela promessa de trabalho e outros serviços na verdade inexistentes.

Lottery scams ou *golpe da lotaria*: envolve falsos anúncios de vitórias na loteria, nos quais solicita-se que o pretenso vencedor envie suas informações confidenciais para uma determinada conta de *e-mail* que assim coleta essas informações e notifica a vítima exigindo uma pequena taxa para que os seus fundos sejam liberados. Uma vez essa taxa enviada o

---

[487] Tem essa designação por ter surgido na Nigéria na década de 1970. **THOMPSON**, N. 'You've got fraud!' Foreign Policy, Washington: May/Jun. 2003, p. 93.

[488] **CHANG**, Joshua. An analysis of advance fee fraud on the internet. Article (PDF Available) in Journal of Financial Crime 15(1):71-81. DOI: 10.1108/13590790810841716. The University of Sydney. January 2008. Disponível em https://www.researchgate.net/publication/241280377_An_analysis_of_advance_fee_fraud_on_the_internet (Acedido aos 12-05-2020).

[489] Disponível em https://en.wikipedia.org/wiki/Advance-fee_scam (Acedido aos 12-05-2020).

[490] Melhores desenvolvimentos encontram-se na obra de **VIDROS**, Sokratis; **KOLIAS**, Constantinos & **KAMBOURAKIS**, Georgios. Online recruitment services: Another playground for fraudsters. George Mason University. Article (PDF Available) in Computer Fraud & Security2016(3):8-13. March 2016. DOI: 10.1016/S1361-3723(16)30025-2. Disponível em https://www.researchgate.net/publication/299346771_Online_recruitment_services_Another_playground_for_fraudsters (Acedido aos 12-05-2020).

atacante vai inventando outras taxas até não mais ser possível contactá-lo. Os valores envolvidos nesse tipo de scamming são geralmente muito elevados[491].

Online sales and rentals scam ou *golpe de vendas e alugueres online*: sucede no processo de compra de bens e serviços por meio de anúncios classificados, particularmente em *sites* em que o atacante contacta o vendedor de um determinado bem ou serviço por telefone ou *e-mail*, manifestando interesse no item, depois envia um cheque falso por um valor superior ao preço fixado, solicitando ao vendedor que envie a diferença para um endereço alternativo, geralmente por ordem de pagamento ou Western Union.

Na ânsia de vender, o vendedor não espera verificar o cheque e, quando o cheque sem fundo é devolvido, a fraude já foi efetivada. Dado o facto de essa fraude depender de pagamentos com cartão de crédito, para impedi-la sugerimos o pagamento em numerário[492].

O romance scam[493] ou *dating scam* (fraude de romance ou fraude de namoro): é um tipo relativamente novo que se tornou observável por volta de 2008 em que os criminosos fingem iniciar um relacionamento por meio de *sites* de namoro *online* e depois defraudam suas vítimas em grandes somas de dinheiro[494]. Por norma, o vigarista aborda a vítima em um serviço de encontros *online*, em mensagens instantâneas ou em um *site* de rede social e alega ter interesse nela, em seguida publica fotos de uma pessoa atraente, usa essa comunicação para ganhar confiança e depois pede dinheiro[495].

Para nos protegermos do scamming muitas medidas podem ser tomadas como evitar fazer pagamentos antecipados. Algumas destas medidas são institucionais como a registada na

---

[491] **PURAM**, Pradeep Kumar; **KAPARTHI**, Mukesh; **RAYAPROLU**, Haas & **KRISHNA**, Aditya. Online scams: taking the fun out of the internet. Article (PDF Available)· September 2011, p. 561. Disponível em https://www.researchgate.net/publication/267218231_ONLINE_SCAMS_TAKING_THE_FUN_OUT_OF_THE_INTERNET (Acedido 12-05-2020).

[492] O mesmo sugerem os autores da obra **PARK**, Youngsam; **MCCOY**, Damon & **SHI**, Elaine. Understanding Craigslist Rental Scams. Conference Paper. DOI: 10.1007/978-3-662-54970-4_1. Issn: 0302-9743. May 2017, p. 3. https://www.researchgate.net/publication/317234064_Understanding_Craigslist_Rental_Scams (Acedido 12-05-2020).

[493] É ainda denominada catfish scam ou simplesmente catfishing. Para melhor compreensão consulte-se **SMITH**, Lauren Reichart; **SMITH**, Kenny D. & **BLAZKAINDIANA**, Matthew. Follow Me, What's the Harm? Considerations of Catfishing and Utilizing Fake Online Personas on Social Media. 2017 Human Kinetics, Inc. Journal of Legal Aspects of Sport, 2017, Vol. 27, p. 32-45. Disponível em https://doi.org/10.1123/jlas.2016-0020 (Acedido aos 13-05-2020).

[494] **WHITTY**, Monica T. & **BUCHANAN**, Tom. (2012). The Online Dating Romance. Scam: A Serious Crime. Cyber Psychology, Behavior, and Social. Networking, 15(3), 181-183. Disponível em https://www.researchgate.net/publication/221805037_The_Online_Romance_Scam_A_Serious_Cybercrime (Acedido 12-05-2020).

[495] O Wikipedia apresenta outras formas de atuação da seguinte maneira: "O vigarista pode alegar estar interessado em conhecer a vítima, mas precisa de dinheiro para reservar um avião, comprar uma passagem de ônibus, alugar um quarto de hotel, pagar custos de viagens pessoais, como gasolina ou aluguel de veículos, ou para cobrir outras despesas. Em outros casos, eles alegam que estão presos em um país estrangeiro e precisam de assistência para retornar, para escapar da prisão por funcionários locais corruptos, para pagar despesas médicas devido a uma doença contraída no exterior e assim por diante. O golpista também pode usar a confiança adquirida pelo ângulo do romance para introduzir alguma variante do scamming nigeriano feito por cartas, como dizer que eles precisam obter dinheiro ou objetos de valor fora do país e pretendem compartilhar a riqueza, fazendo a solicitação por ajuda para poderem deixar o país tornando ainda mais atraente o cenário para a vítima".
Disponível em https://en.wikipedia.org/wiki/Advance-fee_scam (Acedido aos 12-05-2020).

Nigéria onde o governo criou em 2004 a Comissão de Crimes Económicos e Financeiros (EFCC, Economic and Financial Crimes Commission) para combater esses crimes, incluindo a fraude nigeriana[496] e adotou em 2009 uma tecnologia inteligente denominada "Eagle Claw" desenvolvida pela Microsoft para rastrear *e-mails* fraudulentos.

Essas medidas recomendadas podem ser resumidas em cinco[497]:

a) **Verifique o endereço da Web (ou URL)**: as comunicações de *sites* sociais populares, processadores de pagamento *online* ou administradores de TI são geralmente usadas para atrair o público inocente. O endereço da *web* do *site* fraudulento pode parecer-se muito com o *site* autêntico. Pode até conter o endereço do *site* autêntico, mas também inclui código para redirecionar o tráfego para um *site* falso.

b) **Fique atento e cético** em relação a pessoas que inesperadamente entrem em contato contigo por *e-mail* ou telefone e perguntando sobre informações pessoais. Abra apenas *e-mails*, *links* e anexos de fontes confiáveis.

c) **Saiba quem são seus provedores** para o teu hosting, *e-mail* e Internet. Saiba também como esses provedores entrarão em contato contigo.

d) **Proteja o seu computador** com filtros de *spam*, *software* antivírus e firewalls. Para uma proteção ideal, mantenha esses programas atualizados.

e) **Aja imediatamente** se achas que foste vítima de um golpe *online*. Se forneceste números de conta, PINs ou senhas a uma fonte não identificada, notifique imediatamente as empresas com as quais tens contas.

Quanto ao enquadramento jurídico-penal, o scamming por configurar uma fraude insere-se propriamente nos crimes contra o computador e contra o património, ou seja, preenche os

[496] Disponível em https://en.m.wikipedia.org/wiki/Economic_and_Financial_Crimes_Commission (Acedido aos 12-05-2020).

[497] Seguimos as medidas bem apresentadas pelo *site* Global Reach. Apesar de fazer menção de seis medidas, na verdade o *site* apresenta apenas cinco. Disponível em https://www.globalreach.com/about/newsletters/grip-newsletter/6-ways-to-avoid-internet-scams/6-scam-savvy-tips/ (Acedido aos 12-05-2020).

ilícitos penais de falsidade informática ou de burla informática (art.ºs 7º e 8º da CB e 235º e 407º do ACP)[498] conforme o caso em concreto.

4.3. Atuações relacionadas com a pornografia infantil

A exploração sexual de crianças no espaço cibernético tem a sua efetivação no abuso sexual de crianças, na posse, na partilha bem como na disseminação de conteúdos relacionados com a pornografia de menores.

A concretização desses ilícitos, que devem ser cometidos de forma deliberada e intencional na rede, é levada a cabo de diversas maneiras e aqui descreveremos algumas delas.

Nas práticas mais frequentes é notória a realização de filmagens com computadores ligados à rede e equipados com *webcam*[499] ou de outro software de comunicação como o *Skype* ou o *Zoom,* em que o infrator vai projetando as filmagens e transmitindo em tempo real para que qualquer pessoa que esteja *online* aceda; pode ainda proceder a filmagens para efeitos de posterior comercialização como sucedeu na primeira e na mais relevante operação policial internacional contra os ciberpedófilos – a operação Starburst[500][501].

As novas tecnologias de informação e comunicação possibilitam que múltiplas imagens de abuso de menores sejam produzidas a partir de uma gravação digital e a consequente transferência para outros meios de comunicação.

E para agravar o cenário os atacantes têm concebido cada vez mais novas maneiras de produzir e distribuir imagens de abuso infantil. A título exemplificativo, os *scanners* são usados para carregar e distribuir imagens em formato digital e, juntamente com as câmaras *web* e digitais, fornecem aos colecionadores desse material de abuso infantil ferramentas de produção muito aprimoradas.

---

[498] No Brasil o scamming é previsto e punível pelo art.º 171º do CP como crime de estelionato. No CP nigeriano é designado de "obtenção de bens sob falsas pretensões" e consta no art.º 419º.

[499] Sem nos esquecermos dos telemóveis que têm videochamadas.

[500] **MARTELLOZZO**, Elena. Online Child Sexual Abuse: Grooming, Policing and Child Protection in a Multi-Media World. Routledge. ISBN 9780415732727. November 11, 2013.

[501] As investigações policiais internacionais mais importantes e que envolveram 19 países, incluindo os Estados Unidos são, para além da Operação Starburst de 1995, as seguintes:

- ✓ Operação Cathedral (1998);
- ✓ Operação Candyman (2001);
- ✓ Operação Landmark (2001);
- ✓ Operação Twins (2002); e
- ✓ Operação Ore (2002).

HARRISON, Christine. Cyberspace and Child Abuse Images: A Feminist Perspective. Affilia: Journal of Women and Social Work. Volume 21 Number 4. Winter 2006 365-379. © 2006 Sage Publications 10.1177/0086109906292313. http://aff.sagepub.com hosted at http://online.sagepub.com p. 368.

Noutra forma de atuação os *cibercriminosos* contactam outros infratores usando uma arquitetura de rede de computadores (*e.g.* peer-to-peer)[502] ou mesmo as redes sociais, o que tem levado à criação e o reforço da "comunidade pedófila"[503].

Para efeitos de anonimização tem sido recorrente nesta "comunidade" a utilização de software encriptados para dificultar ou impedir a deteção e a consequente identificação dos infratores, tornando quase impossível a tão desejada responsabilização penal.[504]

As técnicas desses predadores estão cada vez mais sofisticadas e incluem os mecanismos de compressão de dados, as mais recentes formas de acesso à Internet por via Wi-Fi em portáteis ou telemóveis, os pagamentos por Internet banking ou cartões pré-pagos, etc. Todos esses mecanismos reduzem a possibilidade de rastrear os delinquentes, tornando-os quase que intocáveis[505].

A sala de conversação *online* ou *chat*[506] é outro local recorrente de prática destes delitos. Os agressores ali surgem usando nomes de utilizadores falsos, os ditos *nicknames*, marcam encontro com as crianças ou as aliciam de outras maneiras.

Já que as crianças têm menos maturidade e são mais susceptíveis de serem aliciadas ou enganadas, devem ser aconselhadas a não publicarem fotografias ou vídeos íntimos porque estes podem ser objeto de utilização ilícita. Por isso urge a formação de investigadores, magistrados, pais, educadores e agentes de autoridade em geral, em matéria relacionadas à computação forense.

A formação dessas entidades possibilitaria a vigilância preventiva e facilitaria a prossecução processual dos delinquentes por via da obtenção da prova digital, como sucede nas técnicas de determinação do endereço IP[507] ou endereço MAC[508] do *modem* e placa de rede do computador associado a uma determinada comunicação de pornografia de menores.

---

[502] "Com a utilização de conexões P2P em que o servidor não é mais necessário, novas ferramentas de investigação foram desenvolvidas, como o programa CPS (Child Protection System), o qual realiza uma identificação automática e é utilizado em 77 países", p. 19. In **CAIADO**, Felipe B. & **CAIADO**, Marcelo. Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. Crimes cibernéticos. Coletânea de artigos. Volume 3. Brasília - MPF 2018.

[503] **TAYLOR**, M. The nature and dimensions of child pornography on the Internet. Paper prepared for the conference Combating Child Pornography on the Internet, Vienna. (1999, September 29 - October 1). Disponível em http://www.ipce.info/library/_3/files/nat_dims_kp.htm, p. 4. (Acedido aos 25-05-2020).

[504] **CARR**, J. Child pornography. Paper presented at the Second World Congress Against Commercial Sexual Exploitation of Children, Yokohama, Japan. (2001, December 17-20). Disponível em http://www.csecworldcongress.org/PDF/en/Yokohama/Background_reading/Theme_papers/Theme%20paper%20Child%20Pornography.pdf (Acedido aos 25-05-2020).

[506] Na linguagem brasileira diz-se "bate-papo".

[507] O endereço IP pode também ser fornecido pelas empresas Fornecedoras de Acesso à Internet (Internet Service Provider - ISP) ou pelas operadoras de telecomunicações.
Na mesma linha de pensamento está o III° ponto do Acórdão do Tribunal da Relação de Lisboa de 18-01-2011 nos seguintes termos:

> *"A identificação completa, morada e endereço de correio electrónico do titular de determinado blog, bem como o IP de criação desse blog e o IP onde foi efectuado determinado "post", constituem dados de base, que embora cobertos pelo sistema de*

Portanto, de uma forma resumida, todas as ações acima descritas preenchem o ilícito penal de pornografia infantil previsto no art.º 9º da CB e 184º do ACP[509] e no universo das TICs podem resumir-se no manuseamento de conteúdo (uma imagem ou um vídeo) pornográfico de menores numa das seguintes maneiras:

- Abrir um anexo em um correio eletrónico[510].
- Fazer o *download* em um endereço eletrónico na tela do computador ou do telemóvel.
- Armazenar em um diretório de um computador.
- Aceder a uma página *web* ou hiperligação pornográfica na qual esses conteúdos indecentes aparecem por meio do mecanismo automático de "*pop-up*".

4.4. Implementação e constatação das técnicas delituosas na realidade de Angola

4.4.1. Generalidades sobre as TICs na realidade angolana

Sobre essa temática, já avançamos alguns factos tidos como os mais pertinentes, mormente o ataque sofrido pela empresa Sonangol, o ataque que atingiu as instituições governamentais e o ataque ao *site* Maka Angola.

Antes de tocarmos noutros aspetos atinentes à frequência *cibercriminosa* em Angola devemos fazer uma descrição panorâmica sobre o ministério que tutela as TICS e outros organismos afins, os diplomas legais envolventes, os aspetos relacionados com o uso e a prestação dos serviços de Internet, as empresas públicas e privadas do setor, o uso da criptografia, as questões concernentes a cibersegurança e outras.

Em termos políticos, a principal estratégia para a implementação e desenvolvimento das TICs em Angola registou-se com a criação do Ministério das Telecomunicações e Tecnologias de Informação (MTTI) em 2008, substituindo o antigo Ministério dos Correios e Telecomunicações, o que denotou o reconhecimento estratégico deste setor para o crescimento do país.

---

confidencialidade, podem ser comunicados a pedido de uma autoridade judiciária, aplicando-se o regime do art.º 135, do CPP, quando tenha sido deduzida escusa".

Disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/0e870e9e27822433802578390057 85c2?OpenDocument (Acedido aos 27-05-2020).

[508] Disponível https://en.wikipedia.org/wiki/MAC_address (Acedido aos 27-05-2020).

[509] A pornografia infantil pode estar em concurso real com o crime de perturbação e devassa da vida privada assim como a devassa por meio de informática, previstos e puníveis nos art.ºs 211º e 212º do ACP, principalmente nos casos de divulgação de conteúdos filmados, gravados ou obtidos por uma técnica informática como o *phishing*.

[510] Não deve ser punida a simples receção de material pornográfico infantil que não tenha sido precedida de solicitação de remessa pelo recetor. Isto sucede, por exemplo, com o *spam*. *In* **ROXIN**, Claus, Crimes de Posse. Tradução de José Danilo Tavares Lobato. Revista Liberdades, IBCCRIM, nº 12, Jan. – Abr. 2013, p. 51.

Um ano depois da sua institucionalização, o MTTI criou um organismo público especializado nos serviços de telecomunicações por satélite denominado Infrasat[511] que em junho de 2017 transformou-se em Sociedade Comercial, numa altura em que se colocava em órbita o primeiro satélite angolano – o Angosat. O objetivo dessa transformação foi precisamente rentabilizar o Angosat[512].

No mesmo ano surgiu o Centro Nacional das Tecnologias de Informação (CNTI)[513] que contribuiu imenso para implementação do Plano Nacional da Sociedade de Informação (PNSI) e do Plano Estratégico da Sociedade de Informação (PAGE)[514], ambos envolvendo o quatriénio 2013/2017.

No âmbito do melhoramento da governação eletrónica, no início deste ano de 2020 foi disponibilizado o Portal dos Serviços Públicos Eletrócnicos (SEPE), "ferramenta integradora para a disponibilização de serviços públicos *online*, que foi criado com o objectivo de alcançar a modernização administrativa e identificar soluções que visam desburocratizar o acesso aos serviços públicos"[515].

As autoridades angolanas demonstram, principalmente nos últimos cinco anos, uma preocupação imensa em legislar sobre matérias relacionadas às TICs. Neste sentido, foram sendo sucessivamente aprovados alguns diplomas legais nesta segunda década do século XXI, dos quais destacamos:

- A Lei nº 22/11 de 17 de Junho – Lei da Protecção de Dados Pessoais;
- A Lei nº 23/11 de 20 de Junho – a Lei das Comunicações Electrónicas e dos Serviços da Informação;
- Regulamento das Tecnologias e dos Serviços da Sociedade da Informação (Decreto Presidencial n.º 202/11 de 22 de Julho);
- O Estatuto Orgânico da Agência Nacional de Protecção de Dados Pessoais (Decreto Presidencial nº 214/16 de 10 de Outubro);

[511] Quanto a sua missão, na página oficial pode ler-se o seguinte "Fornecer produtos e serviços que proporcionam comunicação entre empresas e pessoas, encurtando distâncias, minimizando a infoexclusão e contribuindo activamente para o desenvolvimento sócio-económico de Angola." Disponível em https://infrasat.net (Acedido aos 14-05-2020).

[512] Infrasat torna-se sociedade comercial e tratará de rentabilizar o AngoSat. Notícia escrita por Jorge Cognitivo, aos 11/06/2017. Disponível em https://www.menosfios.com/infrasat-torna-sociedade-comercial-tratara-rentabilizar-angosat/ (Acedido aos 14-05-2020).

[513] Substituindo a anterior Comissão Nacional das Tecnologias de Informação.

[514] **JÚNIOR**, Matondo Otequele. As Políticas das Tecnologias de Informação e Comunicação em Angola e a sua Implementação para o Desenvolvimento Socioeconómico. Departamento de Sociologia. Dissertação submetida como requisito parcial para obtenção do grau de Mestre em Estudos Sociais da Ciência. Orientadora Professora Doutora Maria Teresa de Morais S. Patrício Professora Associada do Instituto Universitário de Lisboa – ISCTE-IUL. Janeiro de 2013, p. 12.

[515] Disponível em http://www.angop.ao/angola/pt_pt/noticias/economia/2019/11/51/Angola-tem-mais-seis-milhoes-utilizadores-internet,1b1c3cee-23d4-4bea-9a7f-8395923810f1.html (Acedido aos 14-05-2020).

- A Lei de Protecção de Redes e Sistemas Informáticos (Lei nº 7/17 de 16 de Fevereiro);
- Resolução nº 33/19 de 9 de Julho, publicada no Diário da República – Iª Série nº 91 (Aprova para ratificação a Carta Africana Sobre a Cibersegurança e Protecção de Dados);
- A Carta Africana Sobre a Cibersegurança e Proteção de Dados (Carta de Ratificação nº 1/20 que é parte integrante do Diário da República – Iª Série nº 23 de 3 de Março de 2020); e
- A Lei da Identificação ou Localização Celular e da Vigilância Electrónica (Lei nº 11/20 de 23 de Abril).

No tocante aos serviços de telefonia móvel existem três empresas que prestam esses serviços de telecomunicações: a Unitel que é a maior, com uma quota de mercado de 80%; Movicel com os outros 20% e a Angola Telecom com uma posição "praticamente insignificante"[516]. Por isso o Despacho Presidencial de 4 de Novembro de 2019 procedeu a sub-concessão deste serviço a Angorascom Telecomunicações SA[517], substituindo a Angola Telecom como terceira operadora móvel de Angola[518].

Em 30 de Setembro de 2019 abriu-se um concurso público para admissão da quarta operadora ao abrigo do Despacho Presidencial nº 61/19, de 30 de Abril. Inicialmente foi dada como vencedora a empresa Telstar, entretanto este concurso público foi anulado porque esta empresa "não apresentou resultados operacionais dos últimos três anos, como impunha o caderno de encargos".

No segundo concurso público – de 2 de Março de 2020 – foi dada como vencedora a empresa libanesa Africell Holding SAL[519], mas ainda não começou a operar.

De acordo com o INACOM (Instituto Angolano das Comunicações) a taxa de utilização de telefonia móvel é de 50%, isto é, numa população nacional estimada em 28 milhões de habitantes, 14 milhões utilizam a comunicação por telemóveis[520].

---

[516] Idem.

[517] Disponível em https://opais.co.ao/index.php/2019/11/08/angorascom-telecomunicacoes-s-a-e-a-quarta-operadora-de-telefonia-movel/ (Acedido aos 14-05-2020).

[518] Disponível em https://angola24horas.com/index.php/politica/item/15036-angorascom-s-a-substitui-angola-telecom-com-a-terceira-operadora-de-telefonia-movel (Acedido aos 14-05-2020).

[519] Disponível em https://www.plataformamedia.com/pt-pt/noticias/economia/libanesa-africell-selecionada-para-4-operadora-de-telecomunicacoes-em-angola-11877296.html (Acedido aos 14-05-2020).

[520] Noticiado na MACAUHUB com o Título "Angola tem 14 milhões de utilizadores de telefonia móvel". Disponível em https://macauhub.com.mo/pt/2019/12/18/pt-angola-tem-14-milhoes-de-utilizadores-de-telefonia-movel/ (Acedido aos 14-05-2020).

No que concerne ao mercado de acesso à Internet, em Angola existem vários operadores ou provedores desse tipo serviço[521], no entanto a posição dominante é ocupada pela Unitel.

Segundo o Presidente do Conselho de Administração (PCA) do INACOM, em 19 de Dezembro de 2019 existiam em Angola 6.173.466 utilizadores da Internet[522], o que representava cerca de um quarto da população.

Tendo em conta o salário mínimo nacional fixado em 21.454 kwanzas (doravante kz) por mês[523] – equivalente a 29 euros[524] – os preços de acesso à Internet até agora praticados afiguram-se elevados.

Nas empresas de telefonia móvel os preços dos planos mensais de dados variam de 1.500kz a 38.564,57kz como comprovam as tabelas abaixo:

PLANO MENSAL DE DADOS DA UNITEL[525]					
Consumo	1 GB	1,5 GB	3 GB	6 GB	12 GB
Preço	1.500kz	2.000kz	3.000kz	5.000kz	10.000kz

PLANO MENSAL DE DADOS DA MOVICEL[526]			
Consumo	2 GB	6 GB	10 GB
Preço	2.000kz	5.000kz	8.000kz

PLANO MENSAL DE DADOS DA ANGOLA TELECOM[527]						
Internet download	1 Mbps	2 Mbps	4 Mbps	8 Mbps	12 Mbps	16 Mbps
Internet upload	256 Kbps	512 Kbps	768 Kbps	1 Mbps	1 Mbps	1 Mbps
Preço em kwanzas	7.165,71	10.422,85	16.676,57	26.024,57	33.288,00	38.564,57

[521] O nome de cada um desses provedores é consultável em https://www.aapsi.og.ao/associados (Acedido aos 21-09-2020).
[522] Notícia da ANGOP com o título "Angola tem mais de seis milhões de utilizadores de internet" de 19 Dezembro de 2019. Disponível em http://www.angop.ao/angola/pt_pt/noticias/economia/2019/11/51/Angola-tem-mais-seis-milhoes-utilizadores-internet,1b1c3cee-23d4-4bea-9a7f-8395923810f1.html (Acedido aos 14-05-2020).
[523] Disponível em https://meusalario.org/angola/salario/salario-minimo (Acedido aos 21-09-2020).
[524] Disponível em https://www1.oanda.com/lang/pt/currency/converter/ (Acedido aos 21-09-2020).
[525] Disponível em https://www.unitel.ao/particulares/tarifarios/#tab-171 (Acedido aos 21-09-2020).
[526] Disponível em https://movicel.co.ao/plano/movinet.html (Acedido aos 21-09-2020).
[527] Disponível em http://www.angolatelecom.ao/TARI_LOJA_DADOS.aspx (Acedido aos 21-09-2020).

Nas principais empresas de TV por Satélite que disponibilizam os Pacotes de Televisão e Internet os preçários mensais vão de 12.000kz a 204.000kz, como atestam as tabelas seguintes:

PLANO MENSAL DE DADOS DA TV CABO[528]				
Consumo	2 GB	6 GB	12 GB	20 GB
Preço	18.050kz	36.550kz	58.450kz	91.150kz

PLANO MENSAL DE DADOS DA NET ONE[529]						
Consumo	5 GB	10 GB	20 GB	30 GB	50 GB	100 GB
Preço	12.000kz	22.500kz	41.000kz	61.500kz	102.000kz	204.000kz

PLANO MENSAL DE DADOS DA ZAP[530]					
Internet download	2MB	6MB	20MB	50MB	50MB
Internet upload	512KB	1MB	2MB	10MB	10MB
Preço em kwanzas	21.350kz	32.050kz	39.250kz	98.300kz	125.100kz

Pelos preçários acima expostos verificamos claramente que as classes sociais de baixos rendimentos têm muita dificuldade em adquirir os serviços de acesso à rede.

Apesar disso é notório o crescimento de usuários das redes sociais e as preocupações do governo angolano em regular a sua utilização. De acordo com uma investigação feita pela empresa MF Press Global, as redes sociais mais utilizadas são o Facebook com 83%, o Youtube com 4,62%, e o Instagram com 2,5%[531].

Sobre o uso de *sites* com HTTP ou HTTPS é-nos difícil apreciar o seu grau de utilização por não haverem estudos sobre essa temática nem informações nos *sites* oficiais.

[528] Disponível em https://www.tvcabo.ao/residencial/pacotes/net (Acedido aos 21-09-2020).
[529] Disponível em https://www.netone.co.ao/?p=satelite (Acedido aos 21-09-2020).
[530] Disponível em http://www.zap.co.ao/zap-fibra/pacotes-tv-net (Acedido aos 21-09-2020).
[531] Notícia do portal ANGOP com o título "Angola ensaia regulação das redes sociais". Disponível em https://m.portalangop.co.ao/angola/pt_pt/mobile/noticias/ciencia-e-tecnologia/2019/2/13/Angola-ensaia-regulacao-das-redes-sociais,c8a21f25-86e9-4aa4-917a-f350cd107ec6.html?version=mobile (Acedido aos 14-05-2020).

No entanto pasmou-nos notar que o *site* oficial do governo angolano[532] não faz recurso ao protocolo seguro e nem mesmo o *site* do ministério que tutela (MTTI)[533] as TICs tem página segura.

Relativamente aos servidores de nome de domínio, em Angola existe a Associação Angolana de Provedores de Serviços de Internet (AAPSI) que congrega "todos os operadores e prestadores de serviços de Comunicações Electrónicas, nomeadamente, provedores de acesso dos serviços e de informações, operadores de rede e empresas que desenvolvam a sua actividade no âmbito dos serviços de provedoria de Internet e Tecnologia"[534].

Com base em um acordo com a AFRINIC e a Internet Systems Consortium (ISC), esta associação concluiu em 17 de Fevereiro de 2015 a instalação da primeira réplica de um servidor raiz em Angola e aderiu o projeto Anycast Root Server que visa aumentar o número de réplica de servidores raiz na região Africana[535].

Quanto as opções para hospedar um *site* na *web*, em Angola existem poucas empresas públicas vocacionadas para o efeito, mas as privadas estão em número considerável. Temos novamente a lamentar a inexistência de registo de todas essas entidades o que dificulta a nossa investigação e impossibilita aferirmos a percentagem de empresas abrangidas.

Nos serviços que prestam incluem-se a criação de domínios e subdomínios, o redimensionamento de *e-mails* e URLs, a gestão de DNS, a alteração de contactos, etc.

O primeiro agente de registo oficial é a DNS Angola[536]. Para além desta empresa pública destacamos a SEPE cujos nomes de domínio podem ser registados na sua e-loja[537].

Nas prestadoras privadas temos a Ango Web Servers[538], a Ango Sites[539], AngoHost[540] e a Iber Web[541].

Surpreendeu-nos negativamente a existência de prestadores privados que não utilizam o protocolo HTTPS, o que quer dizer que esses prestadores têm os seus próprios *sites* inseguros, o que *a priori* macula a idoneidade do serviço que prestam. Como exemplo das visadas temos a Hosting Angola que já existe desde 2008[542], a Braincom[543] e a Emersoft Computer Consulting[544].

---

[532] Disponível em http://www.governo.gov.ao (Acedido aos 14-05-2020).
[533] Disponível em http://www.mtti.gov.ao (Acedido aos 14-05-2020).
[534] Disponível em https://www.aapsi.og.ao/sobre-nos#mission (Acedido aos 19-05-2020).
[535] Disponível em https://www.aapsi.og.ao/noticia/angola-instala-primeira-replica-de-um-servidor-raiz-de-internet (Acedido aos 19-05-2020).
[536] Disponível em https://www.reg.it.ao/support?who_is_regitao (Acedido aos 19-05-2020).
[537] Disponível em https://www.sepe.gov.ao/ao/catalogo/eloja/dominios/registo-de-dominio-ao/ (Acedido aos 19-05-2020).
[538] Disponível em https://angoweb.net/quem-somos/ (Acedido aos 19-05-2020).
[539] Disponível em https://angolasites.com (Acedido aos 19-05-2020).
[540] Disponível em https://www.angohost.ao (Acedido aos 19-05-2020).
[541] Disponível em https://www.iberweb.co.ao/alojamento/ (Acedido aos 19-05-2020).
[542] Disponível em http://www.hostingangola.com/dominios.html (Acedido aos 19-05-2020).
[543] Disponível em http://dominios.co.ao (Acedido aos 19-05-2020).
[544] Disponível em http://emersoft.co.ao/servicos.php (Acedido aos 19-05-2020).

Sobre o uso da criptografia de chave pública existe um largo trabalho que deve ser feito uma vez que ainda não existem Bilhetes de Identidade ou Cartões de Cidadão que façam recurso à essa tecnologia, daí a não existência plena da assinatura eletrónica[545].

Todavia, o executivo demonstra preocupação com as questões que envolvem a criptografia, por isso em 6 de Março de 2019 aprovou o Decreto Executivo 74/19[546] relativo as *regras e requisitos para validação de sistemas de processamento eletrónico de faturação de contribuintes*, que prevê a incorporação de mecanismos que permitam a identificação e a gravação de documentos, através de um algoritmo de chave assimétrica e de uma chave privada do conhecimento exclusivo dos contribuintes (anexo I, nº 2).

Nos requisitos de assinatura prevê a sua geração por via do algoritmo RSA, considerando, em regra, o Hash do último documento assinado (nº 5 al. a) e e) do anexo I).

Reconhece-se a não existência da cultura de cibersegurança em Angola[547]. As suas estruturas ainda são "embrionárias"[548], os testes realizados decorrem "ainda de forma bastante tímida"[549], embora já surjam algumas melhorias graças a cooperação que tem tido com Portugal e já exista a lei 7/17 de 16 de Fevereiro sobre a proteção das redes e sistemas informáticos.

As preocupações com a cibersegurança são mais evidentes no sistema financeiro e de acordo com o Diretor-Geral do Instituto Nacional de Fomento da Sociedade de Informação (INFOSI), só para garanti-la o país gasta anualmente 11 milhões de dólares[550].

---

[545] No quadro legal angolano, o Regulamento das Tecnologias e dos Serviços da Sociedade da Informação (Decreto Presidencial n.º 202/11 de 22 de Julho) apresenta as definições de assinatura electrónica, assinatura electrónica avançada e assinatura electrónica qualificada (art.º 4º al. a), b) e c) e a Lei nº 23/11 de 20 de Junho (Lei das Comunicações eletrónicas e dos Serviços da Sociedade da Informação) reconhece a validade da assinatura eletrónica e a equipara às assinaturas autógrafas (art.º 28.º nº 1).
Entretanto, apesar deste reconhecimento, volvido quase uma década desde a aprovação deste diploma, o Titular do Poder Executivo ainda não regulou esta tal "equiparação" nem instituiu entidades públicas credenciadoras ou certificadoras dessas assinaturas, o que é bastante preocupante, principalmente com a disseminação do Covid-19 que tornou as compras *online* mais frequentes.
"Actualmente a nível da contratação pública, transitoriamente as assinaturas eletrónicas são substituídas pela confirmação eletrónica ou assinatura em papel enquanto não estiver em pleno funcionamento as soluções para as assinaturas electrónicas (art.º 35º nº 5 do Decreto Presidencial nº 202/17 de 6 de Setembro – Regulamento sobre o Funcionamento do Sistema Nacional da Contratação Electrónica)". *In* Angola News: *A hora da assinatura eletrónica*. Matéria escrita por Nilton Caetano Advogado (Docente na Universidade Gregório Semedo e Mestrando na Faculdade de Direito da Universidade de Lisboa) e disponível em https://angola.shafaqna.com/PT/AL/296358 (Acedido aos 16-07-2020).
Para mais desenvolvimentos sobre essa temática pode consultar-se também a opinião do Dr. Moses Caiaia sobre *O Direito angolano aplicável ao comércio electrónico.* Disponível em https://angolaforex.com/2019/05/19/specialist-ao-dr-moses-caiaia-o-direito-angolano-aplicavel-ao-comercio-electronico-ii/ (Acedido aos 16-07-2020).

[546] Este diploma faz menção a muitos aspetos que têm que ver com o uso da criptografia.
Disponível em https://www2.deloitte.com/content/dam/Deloitte/ao/Documents/tax/Tax%20News%20Flash/2018/NF_8_Decreto%20Executivo%2074_19_%20Aprova%20as%20regras%20e%20requisitos%20para%20Validação%20de%20Sistemas%20de%20Processamento%20Electrónico%20de%20Facturação%20dos%20Contribuintes..pdf (Acedido aos 19-05-2020).

[547] Disponível em https://mercado.co.ao/mercados/nao-ha-cultura-de-ciberseguranca-em-angola-LA772692 (Acedido aos 19-05-2020).

[548] Expressão usada pelo então ministro da Defesa de Angola Salviano Sequeira quando visitou a Escola Naval de Lisboa. Notícia do Jornal de Angola de 18 de Dezembro de 2019 intitulada "Estrutura embrionária de cibersegurança no país". Disponível em http://jornaldeangola.sapo.ao/politica/estrutura-embrionaria-de-ciberseguranca-no-pais (Acedido aos 19-05-2020).

[549] Idem.

[550] Disponível em https://www.angop.ao/angola/pt_pt/noticias/economia/2019/6/30/Estado-vai-gastar-USD-milhoes-ano-ciberseguranca,142a1a76-2b39-4c25-836e-7900260c5774.html (Acedido aos 19-05-2020).

4.4.2. Crimes cibernéticos mais frequentes em Angola

Falando propriamente da implantação dos crimes informáticos na realidade angolana[551] devemos começar por assinalar que ao investigarmos essa problemática ficamos imensamente limitados devido a escassez de bibliografia e de outros estudos que abordam este assunto. Por esse motivo, ao fazermos esse trabalho, recorremos com muita frequência às notícias de vários jornais oficiais bem como de alguns *sites* e *blogs*.

Para termos uma ideia dessa "raridade bibliográfica", o primeiro Manual do Direito da Informática e das TICs de Angola, somente foi lançado em Luanda no dia 21 de Fevereiro de 2020. O seu autor – João Francisco – é jurista e investigador colaborador do Centro de Investigação do Direito da Universidade Católica de Angola[552].

Da constatação que se faz denota-se que felizmente a realidade *cibercriminosa* angolana ainda não é alarmante uma vez que Angola figura "entre os países menos afetados pelos crimes cibernéticos"[553]. Não obstante, têm surgido alguns episódios que indiciam algum agravamento.

Fruto desta confirmação, e visando combater tais ilícitos, no ano de 2016 o SIC (Serviço de Investigação Criminal de Angola)[554] criou o Gabinete de Combate aos Crimes Cibernéticos que regista, em média, duas a cinco denúncias[555][556] mensalmente, destacando-se os crimes de burla[557] e difamação[558].

Para melhorar o combate à criminalidade informatizada o governo de Angola tem estabelecido intercâmbios com diversos países, tendo maior pendor os países da CPLP. Prova disso foi o seminário internacional[559] sobre "cibercrime e prova eletrónica: harmonização de

---

[551] Para mais desenvolvimentos leia-se **MENEZES**, Umbelina Teresa João, Op. cit precisamente o Capítulo 4 sobre Criminalidade Informática em Angola p. 47-60.

[552] Notícia do Jornal de Angola com o título "Leis do país respondem aos crimes informáticos" de autoria é Fonseca Bengui. Disponível em http://jornaldeangola.sapo.ao/politica/leis-do-pais-respondem-aos-crimes-informaticos (Acedido aos 19-05-2020).
Lamentavelmente, pelo isolamento imposto à capital do país – Luanda – devido a pandemia do coronavírus não nos foi possível adquirir essa tão desejada obra e a sua venda ainda não está disponibilizada digitalmente.

[553] Notícia do jornal O país, escrito por Brenda Cufuna, com o título "Angola figura entre países menos afetados pelos crimes cibernéticos". Disponível em https://opais.co.ao/index.php/2019/07/26/angola-entre-os-paises-menos-afectados-por-crimes-ciberneticos/ (Acedido aos 19-05-2020).

[554] Organismo com atribuições funcionais semelhantes a Polícia Judiciária portuguesa, vulgo PJ.

[555] Jornal de Angola. "Crimes cibernéticos carecem de legislação" por Edivaldo Cristóvão, escrito em 6 de Fevereiro de 2018. Disponível em http://jornaldeangola.sapo.ao/reportagem/crimes_ciberneticos_carecem_de_legislacao (Acedido aos 19-05-2020).

[556] É um número muitíssimo reduzido quando comparado com os factos que ocorrem em Portugal que do início de 2020 até "16 de abril já foram recebidas 162 queixas e reencaminhadas para abertura de inquérito 28" no Ministério Público (MP). Disponível em https://observador.pt/2020/04/21/cibercrimes-aumentam-de-forma-exponencial-durante-a-pandemia/ (Acedido aos 19-05-2020).

[557] Na maior parte dos casos as burlas ocorrem nos *sites* da OLX e se reportam a vendas de viaturas e de mobiliário.

[558] A difamação que se tem constatado decorre por via das redes sociais. Não é propriamente um crime informático e por isso encontra enquadramento no art.° 407 Código Penal ainda vigente em Angola, que atesta que "se alguém difamar publicamente por viva voz, escrita, desenho ou por qualquer meio de publicação, imputando-lhe um facto ofensivo da sua honra e consideração, ou reproduzindo a imputação, será condenado a prisão até quatro meses e multa até um mês".

[559] Este seminário antecedeu a XVI Conferência de Ministros da Justiça dos Países de Língua Oficial Portuguesa (CMJPLOP) e as suas conclusões e recomendações podem ser encontradas em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/decl_santa_maria_final.pdf (Acedido aos 22-05-2020).

legislação e a convenção de Budapeste na CPLP"[560] realizado na Ilha do Sal em Cabo Verde nos dias 19 e 20 de Novembro de 2019 e contou com a participação do eminente especialista na matéria, o Doutor Pedro Verdelho[561].

Neste aspeto, visando a melhoria do seu quadro funcional, o Ministério do Interior de Angola (MININT)[562] estabeleceu recentemente uma cooperação com a Hungria com objetivo de apetrechar melhor os instrumentos de combate aos crimes digitais, destacando-se nesta área a vigilância e segurança eletrónicas[563][564].

A Procuradoria-Geral da República de Angola também tem abordado este tipo de criminalidade em suas palestras[565] e na sua estrutura orgânica prevê a criação de um gabinete específico para o combate desses delitos virtuais[566].

Oficialmente não existem registos de crimes dessa natureza, porém entre os crimes informáticos mais frequentes realçam-se a clonagem de cartões Visa e multibanco, a venda simulada de produtos via Internet, as transferências ilícitas via Internet banking, difamação e calúnia[567]. Para além destas infrações constatam-se igualmente outras ações passíveis de cominação penal tais como "os furtos, a injúria, ameaças, violações de direitos autorais, a inserção de falsos dados no sistema informático, divulgação de segredos, incitamento à violência, entre outros"[568].

Recentemente, em 21 de Junho de 2020, registou-se talvez o ataque informático mais publicamente divulgado em Angola, tendo sido inclusive alertado pelo INACOM. O ataque conhecido como "toque e foge" foi desferido contra as operadoras de telefonia móvel de Angola

---

[560] Disponível em http://www.dgpj.cv/index.php/news/171-seminario-internacional-sobre-cibercrime-e-prova-eletronica-harmonizacao-de-legislacao-e-a-convencao-de-budapest-na-cplp (Acedido aos 22-05-2020).

[561] ***Pedro Verdelho*** é Procurador da República e Coordenador do Gabinete de Coordenação da Atividade do Ministério Público na área da Cibercriminalidade (Gabinete Cibercrime) que tem sede na Procuradoria-Geral da República. Disponível em http://cibercrime.ministeriopublico.pt/pagina/quem-somos (Acedido aos 22-05-2020).

[562] Pelas suas competências em Portugal equivale ao Ministério da Administração Interna.

[563] Disponível em https://opais.co.ao/index.php/2020/02/26/angola-e-hungria-cooperam-no-combate-ao-crime-cibernetico-e-transfronteirico/ (Acedido aos 22-05-2020).

[564] Em Angola aprovou-se recentemente aos 23 de Abril de 2020 Lei nº 11/20 da Identificação e ou Localização Celular e da Vigilância Electrónica.

[565] Como exemplo desta prática foi a realização no Lubango da palestra sobre "Os desafios da cibercriminalidade e a prova digital" enquadrada nas comemorações do 40º aniversário da institucionalização da PGR de Angola, proferida pelo Subprocurador **Gilberto Mizalaque Balanga Vunge** (por curiosidade antigo estudante do Mestrado em Direito e Informática da Universidade do Minho) o qual reconheceu que "O combate aos crimes cibernéticos em Angola passa por dotar a Procuradoria-Geral da República de meios tecnológicos e a consequente capacitação dos magistrados, que eventualmente possam trabalhar na matéria".

Noticiado pela Angop aos 24 Abril de 2019 sobre a epígrafe "Huíla: Magistrado aborda combate aos crimes cibernéticos". Disponível em http://m.portalangop.co.ao/angola/pt_pt/noticias/politica/2019/3/17/Huila-Magistrado-aborda-combate-aos-crimes-ciberneticos,3aa95b82-5744-4c8f-a136-be9b9023b16b.html (Acedido aos 21-05-2020).

[566] A criação deste importante gabinete, que contará com colaboração de especialistas do SIC, foi prenunciada pelo então Procurador-Geral da República de Angola João Maria Moreira de Sousa.
Noticiado pela Lusa aos 26 de Abril de 2017 com o dístico "PGR angolana vai criar gabinete para combate de crimes informáticos". Disponível em https://www.dn.pt/lusa/pgr-angolana-vai-criar-gabinete-para-combate-de-crimes-informaticos-6246264.html (Acedido aos 21-05-2020).

[567] Notícia do Jornal Valor Económico de 27 de Fevereiro de 2017 escrita por Isabel Dinis. Disponível em https://valoreconomico.co.ao/artigo/lei-contra-crimes-informaticos-ja-em-vigor (Acedido aos 21-05-2020).

[568] Idem.

– com destaque para a Unitel[569] – a partir do estrangeiro. Os atacantes utilizavam indicativos telefónicos da Sérvia e do Zimbabwe[570].

Entretanto, em comunicado oficial o INACOM tranquilizou os utilizadores das redes móveis, sobre a não existência do risco de roubo de informações ou dados pessoais, e apelou a não atenderem, nem retornarem chamadas internacionais para números desconhecidos[571].

Logo, para combater esse fenómeno, além das ações que têm sido protagonizadas pela PGR, o SIC e outras instituições governamentais, urge fazer-se um maior investimento no ramo das TICs, especificamente na área da computação forense e também preparar melhor os técnicos que são formados nas instituições angolanas, pois muitas delas encontram-se limitadas em termos de laboratórios[572].

[569] Disponível em https://angorussia.com/tech/rede-da-operadora-unitel-sofre-ataque-cibernetico/ (Acedido aos 22-06-2020).
[570] Disponível em http://tpa.sapo.ao/noticias/economia/inacom-alerta-para-ataques-as-redes-de-telefonia-movel (Acedido aos 22-06-2020).
[571] Disponível em https://informativoangolano.com/tecnologia/angola-sofre-ataque-nas-redes-das-operadoras-moveis-nas-ultimas-horas/ (Acedido aos 22-06-2020).
[572] Informação da Agência VOA (Voz da América) de 14 de Dezembro de 2014. Disponível em https://pt.wikinews.org/wiki/Crime_cibernético_chega_a_Angola (Acedido aos 23-05-2020).

Capítulo V – CONCLUSÕES E RECOMENDAÇÕES FINAIS

Neste último capítulo faremos a apresentação das conclusões da presente dissertação e as recomendações ou sugestões consideradas oportunas para o prosseguimento dos trabalhos nesta área de pesquisa.

As conclusões foram lavradas de maneira ordenada procurando obedecer a sequência de apresentação dos resultados alcançados em cada um dos capítulos e tendo em consideração que o presente trabalho teve como objetivo examinar o Anteprojeto de Código Penal da República de Angola no sentido de averiguar se os crimes informáticos ali abordados estão ou não em correspondência com a Convenção de Budapeste sobre o Cibercrime.

5.1. Conclusões do Capítulo I

No capítulo inicial referente a apresentação geral do tema fizemos uma incursão aos precedentes históricos, introduzimos o conceito jurídico de criminalidade informática e o conceito de sociedade da informação e riscos que a apresenta para o cometimento de delitos. Com base nas investigações feitas concluímos o seguinte:

- ✓ Depois do surgimento da informática, na segunda metade do século XX, a existência humana e das distintas instituições tornaram-se praticamente impossíveis sem a sua utilização.
- ✓ O avanço tecnológico, sobretudo o uso da Internet, simplificou as relações entre as pessoas e potenciou o intercâmbio entre empresas, governos e instituições internacionais. Apesar desses aspetos positivos, o recurso a essa ferramenta digital também facilitou o cometimento dos crimes clássicos e possibilitou o surgimento de novos tipos penais, fazendo emergir os designados crimes informáticos.
- ✓ O crime informático é "qualquer acção ilícita perpetrada com a ajuda de uma operação electrónica contra a segurança de um sistema informático ou de dados que ele contém, qualquer que seja o fim visado"[573].

[573] **RODRIGUES**, Benjamim Silva. Idem, p. 78, 79.

- ✓ Classificam-se em próprios ou puros e impróprios ou impuros. A distinção fundamental entre eles reside no bem jurídico que se pretende tutelar: os primeiros protegem bens jurídicos informáticos; os segundos, bens jurídicos habituais.
- ✓ A sociedade de informação representa "o modo de desenvolvimento económico e social baseado na aquisição, tratamento e difusão da informação por via de redes de comunicações digitais"[574], que infestou o quotidiano das pessoas e instituições e colocou a informação à disposição de todos de forma livre e aberta.
- ✓ Atualmente África está entre os continentes em que mais se regista um crescimento das atividades ligadas aos crimes cibernéticos e Angola não foge à regra.
- ✓ Como forma de combatê-los surgiu em 2001 a Convenção de Budapeste – instrumento jurídico do Conselho Europeu mas com vocação universal – tendo sido ratificado por vários países fora da Europa.
- ✓ Desde a edificação deste normativo, de uma forma geral, todas legislações penais nacionais que regulam este tipo de ilícitos têm-no como modelo a seguir.
- ✓ O continente africano, embora tenha igualmente uma convenção análoga, ainda debate-se com a problemática da regulação desses ilícitos. Em Novembro de 2016, dos 54 países da África, 30 careciam de disposições legais específicas para combater o cibercrime, representando mais de metade dos países.
- ✓ Dentre os países que carecem de normalização penal temos Angola que para colmatar essa falta elaborou um ACP no qual incluiu a previsão dessas infrações modernas.

5.2. Conclusões do Capítulo II

No segundo Capítulo nos debruçamos sobre o enquadramento internacional da criminalidade informática e analisámos propriamente a Convenção de Budapeste e a Convenção de Malabo, estudámos a regulação dos delitos informáticos em alguns países africanos (Ilhas Maurícias, Nigéria e Cabo Verde), comparámos as convenções europeia e africana e concluímos que:

[574] **VERDELHO**, Pedro. "Cibercrime." Direito da Sociedade da Informação, Vol. IV, Coimbra Editora, Junho de 2003, p. 348.

- ✓ A Convenção de Budapeste sobre o Cibercrime aprovada em 23 de Novembro de 2001 pelo Conselho da Europa visou "a protecção da sociedade da cibercriminalidade" e desde os seus primórdios manifestou ter "vocação universal" sendo ratificada por vários países não europeus, dentre os quais alguns africanos e é considerado o mais significativo e abrangente tratado internacional nessa temática.
- ✓ A Convenção da União Africana sobre a Cibersegurança e Proteção de Dados Pessoais adotada em 27 de Junho de 2014 tem uma ampla abrangência porque além de referir-se à criminalidade cibernética trata igualmente das transações eletrónicas e da proteção de dados pessoais.
- ✓ A CM dá uma maior liberdade aos estados-membros na determinação da tipologia criminal no momento de elaborar a sua lei nacional e embora seja mais generalista que a CB não prevê as infrações que reportam a violação dos direitos de autor e dos direitos conexos, como sucede na CB (art.º 10º).
- ✓ A lista dos países assinantes e aderentes da CM ainda não é satisfatória porque não atingiu sequer metade dos países do continente, ou seja, d*os 54 membros da União Africana 14 países assinaram* (Benim, Guiné-Bissau, Mauritânia, Chade, República do Congo, Serra Leoa, São Tomé, Zâmbia, Gana, Camarões, Moçambique, Togo, Ruanda e Tunísia) *e somente 5 a ratificaram* (Senegal, Guine Conacri, Ilhas Maurícias, Namíbia e o Gana).
- ✓ Poucos países africanos ratificaram a CB, fizeram-no unicamente cinco países, nomeadamente África do Sul, Ilhas Maurícias, Senegal, Cabo-Verde, Marrocos e o Ghana. Cabo-Verde é o único país lusófono a fazê-lo e a sua posição é de extrema relevância e achamos que deve servir de exemplo para os demais países da CPLP.
- ✓ As Ilhas Maurícias foi o primeiro país africano a elaborar uma lei de combate ao cibercrime, dois anos após a implementação da Convenção de Budapeste.
- ✓ Angola não é ainda signatária da CB, porém aprovou para ratificação a CM em 3 de Março de 2020, mediante a Carta de Ratificação nº 1/20 que é parte integrante do Diário da República nº 23 – Iª Série.

5.3. Conclusões do Capítulo III

Esse é o Capítulo fundamental da nossa dissertação. Nele examinamos de maneira profunda os delitos informáticos constantes no anteprojeto de código penal angolano. Para o efeito fizemos uma abordagem histórica dos normativos que o antecederam, estudámos os seus tipos legais e a sua adequação à realidade angolana. Terminámos o capítulo comparando esses delitos com os constantes na CB e na CM.

5.3.1. Crimes informáticos previstos no ACP

Sobre este sub-tema concluímos que

- ✓ No ACP só estão estabelecidas algumas disposições materiais. Os aspetos processuais continuam em falta, pelo que a regulação dos mesmos afigura-se premente e recomendável.
- ✓ Os tipos legais de crimes informáticos albergados pelo ACP são a devassa por meio de informática, a violação de telecomunicações, o dano informático, a falsidade informática, a burla informática e nas telecomunicações e a pornografia infantil.
- ✓ O *nominem juris* do crime de dano informático adotado no ACP é aceitável porque a expressão *dano relativo a dados ou programas informáticos* usada em outros diplomas legais afigura-se "incoerente e redundante" visto que na definição de dado informático (al. c) do art.º 233º do ACP) já estão subentendidos os programas informáticos.
- ✓ O *corpus* do art.º 399º precisa de ser enriquecido com a inserção de novas matérias e ajustamentos na redação, tais como a punição diferenciada de quem insere vírus a um computador desconectado ou "*stand alone* e daquele que realiza essa conduta em rede de computadores, com resultado lesivo muito mais grave"[575].
- ✓ No art.º 235º da falsidade informática ao invés de sancionar de forma análoga quem falsifica e quem se aproveita dos dados informáticos adulterados (nº 2), deveria prever-se uma moldura penal mais suave aos segundos.
- ✓ No ACP, e tal como sucede na CB, prevê-se unicamente – nas infrações contra o conteúdo – a punição da pornografia infantil, mas não se criminaliza os "atos de natureza racista ou xenófoba", cometidos por intermédio de sistemas informáticos.

[575] **CAPANEMA**, Walter Aranha. Op. cit., pág. 11. Disponível em https://www.academia.edu/2515494/Crime_de_dano_e_o_vírus_de_computador (Acedido em 26-12-2019).

- ✓ Na pornografia infantil, diferentemente da CB, o ACP não pune a posse deste material quando apenas se destina ao uso pessoal e concordamos. No caso de mera posse, apesar de ser uma postura moralmente censurável, não há produção nem divulgação de conteúdo lascivo, logo não há bem jurídico lesado e afasta-se a censura penal.
- ✓ Os crimes não previstos no ACP são o acesso ilegal, a intercepção ilegítima, a sabotagem informática e os relacionados com a violação dos direitos de autor e direitos conexos.
- ✓ Com base no anteprojeto, o simples ato de aceder a um sistema ou rede informática sem autorização não constitui por si só crime, por isso apenas criminaliza o acesso sem autorização a dados que "contenham informações individualmente identificáveis" (art.º 212º nº 1 al. b))[576], ou seja, pune-se unicamente *uma forma qualificada de acesso ilegítimo*, *ipso facto*, podemos dizer que o crime de acesso ilegal está parcialmente consumido no teor do crime de devassa por meio de informática.
- ✓ A não previsão da interceção ilegítima presumimos que seja pelas mesmas razões da não inclusão do acesso ilegítimo. São ilícitos muito semelhantes e ambos aportam-se na ilegitimidade, ou seja, na falta de autorização. Outro eventual motivo desta não previsão encontra-se nas conexões que tem com os crimes de violação de correspondência (art.º 212º) e o de violação de telecomunicações (art.º 214º), constantes no ACP, pois que o bem jurídico protegido – "a privacidade na comunicação de dados" – é comum a todos eles.
- ✓ A sabotagem informática tem uma "previsão parcial" no art.º 399º que regula o crime de dano informático, especificamente na parte relativa a causar "dano à integridade do sistema". Entre os dois ilícitos existe uma certa "*«zona de coincidência»* ao nível de certo tipo de dados a tutelar" e ambos apresentam como forma usual de perpetração a introdução de vírus.
- ✓ Essa previsão "subentendida" da sabotagem informática dentro do dano informático afigura-se insuficiente por não incluir a possibilidade de "entravar, impedir, interromper ou perturbar gravemente o funcionamento" do sistema informático. E dado ao facto dos ataques informáticos mais relevantes registrados em Angola preencherem esse ilícito seria mais exequível a sua previsão autónoma.

[576] O art.º 55º do ALPDP referente ao crime de acesso indevido pune unicamente o acesso ilegal a dados pessoais.

- ✓ Além do ACP não aludir os crimes relacionados com a violação dos direitos de autor e direitos conexos, também nem sequer pune "Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado ..." como acontece com o nº 4 do art.º 3º da lei portuguesa do cibercrime.
- ✓ A exclusão dos delitos contra os direitos de autor e direitos conexos foi extensiva à infração de reprodução ilegítima de programa ou de base de dados que sejam criativas, ou seja, no ACP não há previsão categórica da criminalização de ações de usurpação, plágio, contrafação de obras e violação de direitos morais que aconteçam com recurso às TICs, incluindo nestas as bases de dados protegidas[577].
- ✓ A evolução legislativa processada em Angola no âmbito dos direitos de autor e conexos é estranha, pois que a lei 15/2014 de 16 de Julho, que revogou a lei 4/90 de 10 de Março, ao despenalizar a usurpação e ao não prever outras medidas penais expectáveis (como a violação dos direitos morais ou o aproveitamento de obra usurpada do art.ºs 198º e 199º do CDADC português), procedeu neste aspeto um retrocesso legiferante e por isso reclama por alterações urgentes.

5.3.2. Comparação do ACP com a CB

Confrontando os crimes do ACP e os da CB concluímos que

- ✓ O ACP não estabelece o acesso ilegítimo como propõe o art.º 2º da CB. A previsão parcial constante na alínea b) do art.º 212º do ACP que trata da devassa por meio da informática, consubstanciada em punir quem "aceder, sem autorização, a dados informaticamente tratados que contenham informações individualmente identificáveis" afigura-se insuficiente por punir somente o acesso ilegal qualificado, quando a convenção recomenda a punição de todo e qualquer acesso ao sistema.
- ✓ Ademais, as ligeiras similitudes que o acesso ilegítimo também tem com o crime de violação de telecomunicações do art.º 214º do ACP, na parte do nº 1 que pune a

[577] Apesar desses direitos terem respaldo constitucional nos art.º 37.º (Direito de propriedade), 42º (Propriedade Intelectual) e 43º (Liberdade de criação cultural e artística).

intromissão "no conteúdo de telecomunicação", são igualmente exíguas por não envolverem o essencial do art.º 2º do CB.

- ✓ A interceção ilegal do art.º 3º da CB por ser uma infração muito semelhante ao acesso ilegítimo, provavelmente, pelas mesmas razões não tenha tido acolhimento no ACP. É presumível que o legislador entendeu que esta infração pode ser subsumida em alguns dos delitos já previstos (violação da correspondência e de telecomunicações dos art.ºs 213º e 214º), no entanto tendo dignidade constitucional (art.º 34º da CRA) e por ter como objetivo "proteger o direito à privacidade na comunicação de dados" a sua previsão independente é igualmente premente.
- ✓ A penalização da interferência em dados do art.º 4º da CB está em consonância com o art.º 399º que criminaliza o dano informático, nos termos dos quais pune-se quem de forma intencional e ilegítima proceder a danificação, a eliminação ou a deterioração do "conteúdo informático dos dados e de programas" e toda alteração que afeta a utilização eficiente dos dados ou de programas informáticos gravados.
- ✓ O crime previsto no ACP difere-se do dano relativo a dados acolhido em outras legislações lusófonas que abordam o cibercrime. O legislador angolano ao adotar a lata designação de "dano informático" visou envolver os danos quer perpetrados contra os sistemas informáticos quer os executados contra os dados informáticos, aliás, tal se infere da expressão "causar dano a sistemas ou dados informáticos".
- ✓ O *corpus* do art.º 5º da CB referente a sabotagem informática não tem no ACP uma previsão totalmente correspondente. Achamos uma ligeira parecença com o crime de dano informático do art.º 399º no tocante a punição de "quem causar danos a sistemas informáticos" (nº 1) e na cláusula aberta que penaliza "qualquer interferência no funcionamento do sistema informático" (nº 2).
- ✓ De forma geral, no tipo objetivo do art.º 5º da CB punem-se os atos que perturbam o funcionamento de sistemas informáticos ou a comunicação de dados enquanto no ilícito do ACP penaliza-se todo o dano relevante causado quer nos sistemas informáticos quer nos dados informáticos. O segundo é por isso mais abrangente.
- ✓ Quanto ao uso abusivo de dipositivos ou de equipamentos[578], nos delitos informáticos do ACP não descortinamos nenhuma correspondência integral com este normativo do art.º 6º da CB, contudo encontra-se sinteticamente previsto na falsificação informática (art.º

[578] O termo dispositivos aparece na CB, o termo equipamento figura na Nota Explicativa da CB.

235º) e no dano informático (art.º 399º) por serem ilícitos que resultam igualmente de "utilizações indevidas de dispositivos".

- ✓ As infrações relacionadas com computadores da CB foram integralmente acolhidas no ACP.
- ✓ O assunto do ACP a respeito da falsidade informática compatibiliza-se com o art.º 7º da CB pois ambos penalizam quem "dolosamente enganar outrem introduzindo ou excluindo dados em sistema informático, originando desta atuação dados falsificados que podem ser tidos como reais, servindo mesmo como meio de prova" (art.º 235º nº 1). O ACP vai um pouco além sancionando também "quem não sendo falsificador", aja intencionalmente, utilizando esses dados informáticos que foram falseados (art.º 235º nº 2), trazendo no nº 3 como circunstância agravante o facto de o autor da ilicitude ser funcionário público.
- ✓ O art.º 407º do ACP mantém, no essencial, as formas de atuações previstas no art.º 8º CB, embora use uma designação mais extensa – *burla informática e nas telecomunicações* – a sua previsão acolhe, praticamente, todo o conteúdo que a convenção expõe. Convergem essencialmente nas formas de atuações previstas, enunciando que tais práticas se aplicam a quem pretender "obter para si ou para terceiro vantagem patrimonial".
- ✓ As ligeiras dissemelhanças notadas entre ambas burlas informáticas prendem-se com a não inserção no texto do ACP da necessidade da infração decorrer de "forma intencional" ou "não autorizada", no entanto tal é desnecessário ou irrelevante uma vez que o meio astucioso ou enganoso que se exige para o cometimento desse crime pressupõe intencionalidade (lesar o património) e ilegitimidade (não autorização).
- ✓ Na CB a pornografia infantil é preceituada no art.º 9º. No ACP consta no art.º 184º, excetuando-se o nº 1 que retrata um tipo de pornografia infantil que não envolve os sistemas informáticos.
- ✓ Tal como sucede na CB, no nº 2 são tipificadas as ações de produção com a intenção de divulgar (al. a)) e difundir ou transmitir (al. b)). Contrariamente a CB, o ACP não acolhe a punição da simples posse, ou melhor, nem sequer menciona essa eventualidade. Outra dissemelhança reside na idade adotada para o menor; no anteprojeto considera-se menor a partir dos 16 anos e, de resto, qualifica como gravosa esta infração se lesar um menor de 14 anos (nº 3).

- ✓ O art.º 10º da CB não tem acolhimento no ACP, ou seja, nos crimes contra a propriedade do Capítulo II do Título VII não constam delitos relacionados à violação dos direitos de propriedade intelectual cometidos fazendo recurso a um sistema de computadores.
- ✓ O ACP não prevê a possibilidade de responsabilização das pessoas coletivas tal como preceitua o art.º 12º CB e o art.º 8º da DQ 2005/222/JAI.

5.3.3. Comparação do ACP com a CM

Comparando o ACP com a CM temos a concluir que

- ✓ Se bem que o ACP não o preveja, na CM a regulação do acesso ilegítimo do art.º 29º tem uma atenção especial, reservando-se-lhe três alíneas – a), b) e c) – todas do nº 1. A elaboração da al. a) distingue-se da encontrada em outros normativos porque criminaliza não só o comum "acesso não autorizado" como também o acesso que vai além do autorizado. Entretanto, nele não figura a definição de "acesso autorizado", e assim fica-se sem perceber em que medida um acesso pode exceder ao permitido.
- ✓ A sabotagem informática está parcialmente prevista na al. d) do nº 1 do art.º 29º da CM, porém, como já aflorámos, o ACP não dá um acolhimento pleno a essa infração. Além disso, a sua previsão na CM tem um texto muito reduzido e por isso carece de enriquecimento.
- ✓ A al. e) do art.º 29º da CM que sanciona todo aquele que "introduzir ou tentar introduzir fraudulentamente dados num sistema informático" tem uma estatuição incompleta já que uma introdução fraudulenta de dados pode preencher diversos ilícitos informáticos. Por exemplo, no ACP se a intenção da introdução de dados for a de enganar, originando dados falsos que podem ter relevância jurídica então teremos a falsidade informática (art.º 235º); se causar prejuízo ou interferir no funcionamento do sistema teremos um dano informático (art.º 399º) e caso cause prejuízo patrimonial para a vítima ou vantagem patrimonial para o infrator o crime seria o de burla informática e nas telecomunicações (art.º 407º).
- ✓ O dano informático é acolhido conjuntamente por ambos os diplomas em análise e, embora usem termos aparentemente diferentes, no essencial punem a danificação que

afeta os dados ou os sistemas informáticos e coincidem basicamente nos elementos objetivos e subjetivos, no entanto somente a convenção africana pune a tentativa.

- ✓ Não previsto no ACP, porém constante na CM temos o uso abusivo de dispositivo das al. g) e h) nº 1 do art.º 29º que criminaliza a concessão de um equipamento ou dado que favoreça o cometimento de infrações cibernéticas bem como a aquisição encoberta de senhas que possibilitem o acesso ilegal a um sistema informático, atuações que atentam contra a confidencialidade, a integridade e a disponibilidade de sistemas ou de dados informáticos.
- ✓ O nº 2 do art.º 29º da CM na sua al. a) que prevê a interceção ilegal propõe condenar quem "intercetar ou tentar intercetar fraudulentamente, através de meios técnicos, dados informatizados durante a sua transmissão não pública para, de ou dentro de um sistema informático". Este delito não está previsto no ACP, mas por abranger a "violação de dados informatizados", aparenta-se com a violação de telecomunicações do art.º 214º do ACP, uma vez que um e outro pressupõem uma atuação dolosa e desautorizada que resulte na "intromissão nas telecomunicações", causando a violação da privacidade das comunicações e afetando também a lisura das transferências eletrónicas.
- ✓ Todavia o crime de violação de telecomunicações distingue-se ligeiramente da interceção ilegal porque condena tão-somente a ingerência em telecomunicações que possibilite a tomada de conhecimento de conteúdos passíveis de serem divulgados, e não a simples interceção de dados transmitidos de forma não pública.
- ✓ A falsidade informática do art.º 235º do ACP e das al. b) e c) do nº 2 do art.º 29º da CM têm um tratamento praticamente idêntico. Protegem o património do lesado e a segurança nas relações jurídicas, ou seja, salvaguardam as infrações ligadas a adulteração de identidades, obtenção de credenciais de usuários recorrendo aos ataques de *pharming* e de *phishing*. Concordam igualmente na punição de quem, mesmo não sendo o falsificador, utilize os dados que forem adquiridos de maneira enganosa.
- ✓ Ainda estabelecido conjuntamente no ACP e na CM está a burla informática (art.º 407º ACP e nº 2 al. d) do art.º 29º CM) que no ACP abrange também as telecomunicações. Os dois dispositivos legais são concordes em criminalizar "a obtenção fraudulenta, para si ou para outra pessoa, de qualquer benefício, por intermédio da introdução, alteração, eliminação ou supressão de dados informatizados".

- ✓ O nº 2 do art.º 29º da CM na al. e), tal como a al. a) do art.º 212º do ACP, criminaliza o processamento negligente de dados pessoais, mas a CM vai mais além requerendo que a falta de precaução tenha a ver com a não consideração de algumas "formalidades prévias de processamento" do art.º 10º, ou seja, "o processamento de dados pessoais deve sujeitar-se a uma declaração da autoridade de protecção" (art.º 10º nº 2).
- ✓ No nº 2 al. f) do art.º 29º da CM – sem similitude no ACP – aparece não rigorosamente um crime mas uma estatuição que impõe a responsabilização criminal de quem participar numa organização criminosa que tem por fim preparar ou cometer as infrações previstas na CM. Nesse aspeto e visando o combate à ciberguerra, ao ciberterrorismo e à ciberespionagem a 2ª parte do ponto 2 do nº 3 do art.º 29º reforça mencionando que as "infracções cometidas sob a égide de uma organização criminosa serão punidas com as penas máximas previstas para a infracção em causa."
- ✓ Tal como o faz no acesso ilegal, a CM dá uma atenção especial à pornografia infantil e no art.º 1º das definições, começa justamente por defini-la. A sua previsão consta no art.º 29º nº 3 ponto 1 al. a), b), c) e d) e no ACP figura no art.º 184º. Os dois normativos criminalizam os atos que consistem na produção, transmissão ou representação de pornografia infantil e criminalizam ainda a aquisição, a importação, a facilitação e o acesso a imagens de material desta natureza. Apenas a CM pune a posse.
- ✓ Os diplomas têm dissonância na categorização da menoridade; para a CM menor é quem tenha menos de 18 anos (art.º 1º), já o ACP fixa a menoridade abaixo dos 16 anos (art.º 184º nº 5 al. b)).
- ✓ O penúltimo delito da CM (art.º 29º nº 3 ponto 1 al. e), f) e g)) é o que pune o racismo, xenofobia e outras formas de discriminação feitas com recurso a sistemas informáticos[579], mas sem acolhimento no ACP.
- ✓ O art.º 29º da CM encerra com o nº 4 que sanciona as "infrações relativas às medidas de segurança das trocas comerciais electrónicas". Apesar de ser um conteúdo não exposto no ACP qualquer dos crimes informáticos podem ter repercussões no comércio eletrónico, por isso essa previsão afigura-se implícita nas previsões do ACP.

5.4. Conclusões do Capítulo IV

[579] Influenciada pelo Protocolo Adicional à Convenção sobre o Cibercrime Relativo à Incriminação de Actos de Natureza Racista e Xenófoba Praticados através de Sistemas Informáticos, adotado em Estrasburgo em 28 de Janeiro de 2003.

No quarto capítulo estudámos de forma geral os delitos informáticos e os comportamentos delituosos mais significativos ligados às tecnologias de informação e comunicação. De maneira particular analisámos as principais tecnologias utilizadas para o cometimento das infrações digitais, algumas falhas de segurança e vulnerabilidades dos sistemas que os atacantes informáticos aproveitam, a situação das TICs na realidadede Angola e os crimes cibernéticos mais comuns neste país.

As conclusões a que chegamos foram as seguintes

- ✓ Nas tecnologias usadas para a prática de crimes digitais destacam-se Hacking, Phishing, Man-In-The-Middle Attack, Sniffing e Scamming.
- ✓ Os ataques de phishing – podem preencher concomitantemente o ilícito de burla informática e falsificação informática.
- ✓ Politicamente falando, a principal estratégia para a implementação e desenvolvimento das TICs em Angola registou-se com a criação do Ministério das Telecomunicações e Tecnologias de Informação[580] no ano de 2008 em substituição do Ministério dos Correios e Telecomunicações, o que revelou o reconhecimento estratégico deste setor para o crescimento do país.
- ✓ Tendo em conta o salário mínimo nacional, de uma forma geral, os preços de acesso à Internet praticados pelas diversas operadoras no mercado angolano afiguram-se elevados.
- ✓ Em Angola reconhece-se a não existência da cultura de cibersegurança e nesse quesito destacam-se as preocupações ligadas ao sistema financeiro, já que neste sector o país gasta anualmente 11 milhões de dólares só para garantir a cibersegurança.
- ✓ Não obstante terem surgido alguns episódios que indiciam algum agravamento, a realidade *cibercriminosa* angolana ainda não é alarmante uma vez que Angola figura "entre os países menos afetados pelos crimes cibernéticos"[581].
- ✓ A escassez de bibliografia que trata da criminalidade informática na realidade angolana dificultou e limitou a nossa pesquisa.

[580] A partir de 06 Abril de 2020, passou a vigorar uma fusão dos então Ministérios das Telecomunicações e Tecnologias de Informação, e o da Comunicação Social. Disponível em http://cdn1.portalangop.co.ao/angola/pt_pt/noticias/sociedade/2020/3/15/Telecomunicacoes-Comunicacao-Social-fundem,d8b6c453-06e7-49e8-b00e-b9065c56a98a.html (Acedidos aos 13-06-2020)

[581] Notícia do jornal O país, escrito por Brenda Cufuna, com o título "Angola figura entre países menos afetados pelos crimes cibernéticos". Disponível em https://opais.co.ao/index.php/2019/07/26/angola-entre-os-paises-menos-afectados-por-crimes-ciberneticos/ (Acedido aos 19-05-2020).

- ✓ Apesar de apontarmos a necessidade de serem feitas algumas alterações e de procederem certos ajustamentos nos conteúdos, reconhecemos que de forma genérica os crimes previstos no ACP, no essencial, adequam-se à realidade angolana.

5.5. Recomendações finais

Com o presente trabalho de investigação almejamos contribuir para o enriquecimento do debate sobre a urgência da previsão legal da cibercriminalidade. Esperamos sensibilizar a comunidade jurídica, assim como as autoridades judiciais e legislativas para a necessária aproximação da legislação angolana aos padrões internacionais de combate à criminalidade informática. E, com isso, contribuir para a introdução de melhoramento da previsão dos ilícitos digitais tipificados no Anteprojecto de Código Penal.

Auguramos auxiliar nas investigações e nos trabalhos de pesquisa no domínio da criminalidade informática – principalmente os aplicados à realidade angolana – mitigar a

profunda escassez bibliográfica que infelizmente hoje em dia se regista, despertar a sociedade angolana da necessidade da realização colóquios, debates ou seminários sobre o uso correto das TICs e da importância da inclusão de conteúdos que desenvolvam nos cidadãos a cultura de cibersegurança nos manuais escolares.

No prosseguimento das conclusões que apresentamos antes e no sentido de contribuirmos para o debate legislativo, recomendamos:

- A revisão urgente da legislação processual penal no sentido de integrar os meios de obtenção e conservação de prova digital, essenciais ao combate à criminalidade praticada por meios informáticos.
- O enriquecimento do *corpus* do art.º 399º, relativo ao crime de dano informático, com ajustamentos na redação e a inserção de novas matérias, diferenciando-se os tipos de danos causados por vírus de computador, assim como punir de forma desigual quem insere vírus a um computador desconectado ou *"stand alone* e aquele que realiza essa conduta em rede de computadores, com resultado lesivo muito mais grave"[582].
- A punição de forma diferente do falsificador e de quem somente se aproveita desses dados informáticos adulterados (art.º 235º nº 2 do ACP), ou seja, ao infrator que apenas se beneficia dos dados previamente defraudados deve incidir uma moldura penal inferior.
- A alteração do teor do art.º 410º e nele consignar a punição da tentativa – nos crimes de burla informática e nas telecomunicações do art.º 407º ACP – mesmo nos casos em que a lesão representar um valor ínfimo, para funcionar como uma forma de persuadir as pessoas ao não cometimento dessa infração.
- A previsão na lei de outros crimes relativos ao conteúdo, especificamente os "atos de natureza racista ou xenófoba" cometidos por intermédio de sistemas informáticos, por reclamarem igualmente por censura penal.
- A inclusão dos crimes de acesso ilegítimo e de interceção ilegítima no Título I dos crimes contra as pessoas, especificamente no Capítulo VII dos crimes contra a reserva da vida privada, por causa das semelhanças que têm uma vez que ambos punem a

[582] **CAPANEMA**, Walter Aranha. OP. cit., pág. 11. Disponível em https://www.academia.edu/2515494/Crime_de_dano_e_o_vírus_de_computador (Acedido em 26-12-2019).

"intercepção de comunicações no interior de um sistema informático" e assim garantem a "privacidade na comunicação de dados".

- A introdução da sabotagem informática no Título V dos Crimes Contra o Estado, especificamente no Capítulo I dos Crimes Contra a Segurança do Estado por acolher o crime de sabotagem (art.º 316º), justificando-se pelas correspondências que têm, mormente na parte que sanciona quem "destruir, danificar, impedir o normal e eficaz funcionamento de vias de comunicação, de transmissão". Evidentemente a sabotagem informática impede o regular e o eficiente funcionamento dos sistemas informáticos assim como de toda a comunicação de dados processada à distância.
- A consignação no Capítulo II dos Crimes Contra a Propriedade, parte integrante do Título VII dos Crimes Contra o Património do ACP, os crimes contra os direitos de autor e direitos conexos e a reprodução ilegítima de programa ou de base de dados que sejam criativas, para garantir-se a sã concorrência e a transparência nos mercados bem como a proteção das produções da classe artística.
- O reconhecimento da necessidade da aprovação do Projecto de Regulamento das Tecnologias e dos Serviços da Sociedade da Informação, diploma do Ministério das Telecomunicações e Tecnologias de Informação de 29 de Dezembro 2011, por nele constarem artigos (62º e 64º) que dão proteção jurídico-penal aos programas de computador e às bases de dados e por definir expressões relevantes no universo das TICs, como o *documento eletrónico*, *assinatura eletrónica* e *nomes de domínio* (art.º 4º al. a), p) e ee)).
- A modificação da denominação de *dano informático* do art.º 399º do ACP para *"dano a dados informáticos"*, embora concordemos que é preferível o *nomen iuris* adotado no ACP ao dano relativo a dados ou outros programas informáticos (art.º 4º das leis do cibercrime de Portugal e de Cabo Verde).
- O tratamento de maneira distinta – à guisa de outras legislações modernas sobre o cibercrime – a interferência em dados e a interferência em sistemas, urgindo para o efeito a feitura de alguns ajustamentos, esvaziando-se o teor do art.º 399º e substituindo-o por dois tipos penais, um relativo a dano informático a dados e outro relacionado com a sabotagem informática.

- A instituição no ACP da possibilidade de responsabilização das pessoas coletivas – principalmente os provedores de serviço de Internet – tal como procede o art.º 12º CB e o art.º 8º da DQ 2005/222/JAI.

- O melhoramento do texto da al. d) do nº 1 do art.º 29º da CM da sabotagem informática com expressões do tipo "pune-se quem perturbar ou obstruir gravemente o funcionamento de um sistema informático", e não mencionar apenas "quem dificultar ou distorcer".
- O estabelecimento na futura lei angolana do delito de uso abusivo de dispositivo das al. g) e h) nº 1 do art.º 29º do CM para combater-se a pirataria informática, pois ações muito frequentes no mundo virtual como a dos *keyloggers* que "captam as teclas digitais no computador ou no teclado virtual, através de cliques" – permitindo o furto de senhas de contas bancárias, cartões de crédito, acesso a sistemas e a outras informações confidenciais – preenchem esse ilícito. Aqui incluem-se ainda o uso de *spywares* ou de qualquer outro tipo de *malware* que facilite obter o acesso a dados.
- A colocação dos crimes informáticos do ACP numa legislação extravagante por ser mais suscetível a alterações motivadas pelo persistente avanço tecnológico e não em um Código Penal que, por ser a compilação essencial do Direito Penal de um ordenamento jurídico, não é desejável que seja objeto de permanentes modificações ou constantes revisões, que prejudicam a sua estabilidade, necessária à segurança jurídica.

Bibliografia

- ✓ **ALBUQUERQUE**, Roberto Chaconde. A criminalidade informática. São Paulo, SP: Juarez de Oliveira, 2006.
- ✓ **ALNAJIM**, Abdullah & **MUNRO**, Malcolm. An Approach to the Implementation of the Anti-Phishing Tool for Phishing Websites Detection. Intelligent Networking and Collaborative Systems. INCOS'09. International Conference. December 2009. IEEE, 105–112.
- ✓ **ALVES**, Ana Abigail Costa Vasconcelos; **MUNIZ**, Antônio Walber Matias & **CIDRÃO**, Taís Vasconcelos. A oportuna e necessária aplicação do direito internacional nos ciberespaços: uma avaliação sobre a Convenção de Budapeste. Disponível em http://www.congresso2017.fomerco.com.br/resources/anais/8/1507930824_ARQUIVO_FOMERCO;AOPORTUNAENECESSARIAAPLICACAODODIREITOINTERNACIONALNOSCIBERESPACOS.pdf (Acedido aos 19-07-2019).
- ✓ **AMIRI**, I. S; **AKANBI**. O. A & **FAZELDEHKORDI**, E. A Machine-Learning Approach to Phishing Detection and Defense. Syngress, 2014.
- ✓ **ASCENSÃO,** José de Oliveira – "Criminalidade informática", *in* Direito da Sociedade da Informação, Vol. II, Coimbra Editora, Coimbra, 2001.
- ✓ **BALKIN**, J. M.; **BALKIN**, Jack; **GRIMMELMANN**, James; **KATZ**, Eddan; **KOZLOVSKI**, Nimrod; **WAGMAN,** Shlomit & **ZARSKY**, Tal. Cybercrime digital cop in a Networked Environment. New York University Press, 2007.
- ✓ **BRAVO,** Manuel Lopes Rogério & **VERDELHO**, Pedro. Leis do Cibercrime - Volume 1. Edições Centro Atlântico, Abril de 2003.
- ✓ **BUTLER**, Rika. A framework of anti-phishing measures aimed at protecting the online consumer's identity. Stellenbosch University. October 2007.
- ✓ **CAMPOS**, Hélio Samuel Farinha. A Luta Contra o Cibercrime: Os Casos da União Europeia e da NATO. Dissertação de Mestrado em Relações Internacionais, 2018. Disponível em https://repositorium.sdum.uminho.pt/bitstream/1822/59396/1/Dissertac_a_o%2BHe_lio%2BCampos.pdf (Acedido aos 19-07-2019).
- ✓ **CAPANEMA**, Walter Aranha. Crime de dano e o vírus de computador. Disponível em https://www.academia.edu/2515494/Crime_de_dano_e_o_vírus_de_computador (Acedido aos 26-12-2019).
- ✓ **CARVALHO**, Nuno. Organizações e segurança informática. Editora Lugar da Palavra. Setembro de 2009.
- ✓ **CARR**, J. Child pornography. Paper presented at the Second World Congress Against Commercial Sexual Exploitation of Children, Yokohama, Japan. (2001, December 17 - 20).
- ✓ **CASAGRANDE**, Rogério Antônio. Técnicas de detecção de sniffers. Dissertação submetida à avaliação, como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação. Sob orientação do Prof. Doutor Raúl Fernando Weber. Porto Alegre, Outubro de 2003.
- ✓ **CASTRO**, Carla Rodrigues Araújo de. Crimes de informática e seus aspectos processuais. 2 ed. Rio de Janeiro: Lumen Juris, 2003.

- ✓ **CHANG**, Joshua. An analysis of advance fee fraud on the internet. Article (PDF Available) in Journal of Financial Crime 15(1):71-81. DOI: 10.1108/13590790810841716. The University of Sydney. January 2008.
- ✓ **CHOU**, N; **LEDESMA**, R.; **TERAGUCHI**, Y; **BONEH**, D. & **MITCHELL**, J. C. Client-side defense against web-based identity theft. 11th Annual Network and Distributed System Security Symposium (NDSS'04), San Diego, USA, 2004.
- ✓ **CLOUGH**, Jonathan. A world of difference: the Budapest Convention on cybercrime and the challenges of harmonisation. Article is based on a presentation given at the 2nd International Serious and Organised Crime Conference, Brisbane, 29–30 July 2013. Disponível em http://classic.austlii.edu.au/au/journals/MonashULawRw/2014/28.pdf (Acedido aos 19-07-2019).
- ✓ **CORREIA**, Pedro Miguel Alves Ribeiro & **JESUS**, Inês Oliveira Andrade de. Combate às transferências bancárias ilegítimas pela Internet no direito português: entre as experiências domésticas e políticas globais concertadas. Artigo Científico. Recebido: 10 de Março de 2015; Aceito: 04 de Abril de 2016. Online Version ISSN 2317-6172. Rev. Direito GV Vol.12 no.2. São Paulo May/Aug. 2016. Disponível em https://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322016000200542 (Acedido aos 21-07-2020).

- ✓ **COSTA,** José de Faria & **MONIZ**, Helena: Algumas reflexões sobre a criminalidade informática em Portugal, Boletim da Faculdade de Direito, Coimbra, Vol.73, 1997.
- ✓ **CRESPO**, Marcelo Xavier de Freitas. Crimes digitais. Saraiva. São Paulo, 2011. Disponível em https://books.google.co.ao/books?id=Px9nDwAAQBAJ&pg=PT71&lpg=PT71&dq=crime+de+Uso+abusivo+de+dispositivos&source=bl&ots=8aBtZgkdON&sig=ACfU3U2mDt6CCH_ivYVWkWVrYKIK5R95pg&hl=pt-PT&sa=X&ved=2ahUKEwiw0r-h6trnAhWPK7kGHXmqBjIQ6AEwC3oECAoQAQ#v=onepage&q=crime%20de%20Uso%20abusivo%20de%20dispositivos&f=false (Acedido aos 18-02-2020).
- ✓ **DHAMIJA**, R. & **TYGAR**, J. D. The battle against phishing: dynamic security skins. ACM International Conference Proceeding Series, 77 – 88, 2005.
- ✓ **DHAMIJA**, R. & **TYGAR**, J. Phish and hips: human interactive proofs to detect phishing attacks. HIP, 69 – 83, 2005.
- ✓ **DELGADO**, Vladimir Chaves. Cooperação internacional em matéria penal na convenção sobre o cibercrime. Dissertação apresentada como requisito parcial para conclusão do Programa de Mestrado em Direito das Relações Internacionais do Centro Universitário de Brasília, Brasília 2007. Disponível em https://repositorio.uniceub.br/jspui/bitstream/123456789/3562/3/vladimir.pdf (acedido aos 19-07-2019).
- ✓ **DIAS**, Vera Marques. A problemática da investigação do cibercrime. Data Venia – Revista Jurídica Digital. Ano 1. N.º 01. Julho-Dezembro, 2012.

- ✓ **EUFRASIO**, Emília Teixeira Lima. O cibercrime e a violação dos direitos fundamentais de natureza pessoal dos menores – o caso da CPLP. Dissertação apresentada à Faculdade de Ciências Sociais e Humanas da Universidade Fernando Pessoa, como parte dos requisitos para obtenção do grau de Mestre em Criminologia. Porto, 2015. Disponível em https://bdigital.ufp.pt/bitstream/10284/4932/1/DM_EmíliaEufrásio.pdf (Acedido aos 19-07-2019).

- ✓ **GABBER**, E.; **GIBBONS**, P. B.; **KRISTOL**, D. M.; **MATIAS**, Y. & **MAYER**, A. Consistent, yet anonymous, Web access with LPWA. Commun. 1999. ACM 42, 42 – 47.
- ✓ **GASTELLIER-PREVOST**, Sophie; **GRANADILLO**, Gustavo Gonzalez & **LAURENT**, Maryline. A Dual Approach to Detect Pharming Attacks at the Client-Side · DOI: 10.1109/NTMS.2011.5721063 · Source: IEEE Xplore Conference: New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference March 2011.
- ✓ **GERCKE**, Marco. Understanding cybercrime: Phenomena, challenges and legal response. ITU (International Telecommunication Union). September, 2012. Disponível em https://www.itu.int/ITU-/cyb/cybersecurity/docs/Cybercrime_legislation_EV6.pdf (Acedido aos 28-01-2020).
- ✓ **GONÇALVES**, Joana Margarida Andrade. *Pharming*: Análise dogmático-penal, em especial enquanto forma de lesão do património. Dissertação de Mestrado em Direito e Informática. Trabalho efetuado sob a orientação do Professor Doutor António Manuel Tavares de Almeida Costa e do Professor Doutor Victor Francisco Mendes de Freitas Gomes da Fonte. Universidade do Minho. Escola de Direito. Outubro de 2015. Disponível em http://repositorium.sdum.uminho.pt/handle/1822/40931 (20-02-2020).
- ✓ **GONÇALVES**, João André Pinto. Enquadramento legal da Cibersegurança em Portugal e no Mundo - O impacto dos crimes cibernéticos no Direito Internacional. Dissertação para obtenção do grau de Mestre em Ciências Militares Navais, na especialidade de Marinha. Disponível em https://comum.rcaap.pt/bitstream/10400.26/15040/1/ASPOF%20EN-M%20Pinto%20Gonçalves%202016.pdf (Acedido aos 19-07-2019).
- ✓ **GOODRICH**, Michael & **TAMISSA**, Roberto. Introduction to computer security. Pearson New International Edition, 2014.
- ✓ **GOUVÊA**, Sandra. O direito na Era Digital. Crimes Praticados por Meio da Informática. MAUAD, Rio de Janeiro, 1997.
- ✓ **HARRISON**, Christine. Cyberspace and Child Abuse Images: A Feminist Perspective. Affilia: Journal of Women and Social Work. Volume 21 Number 4. Winter 2006 365-379. © 2006 Sage Publications 10.1177/0086109906292313. Disponível em http://aff.sagepub.com hosted at http://online.sagepub.com (Acedido aos 25-05-2020).
- ✓ **HEITOR**, Pedro Levi Vieira de Oliveira. Contributo para a compreensão das causas de exclusão de ilicitude e da culpa no crime de acesso ilegítimo. Dissertação de Mestrado em Direito e Informática. Universidade do Minho, Outubro de 2015. Disponível em http://repositorium.sdum.uminho.pt/bitstream/1822/40898/1/Pedro%20Levi%20Vieira%20de%20Oliveira%20Heitor.pdf (Acedido aos 27-11-2019).
- ✓ **HORA**, Evandro Curvelo. Sobre a detecção remota de sniffers para detectores de intruso em redes TCP/IP: Dissertação de Mestrado em Ciência da Computação. Orientado por Fábio Bueno Queda da Silva. Universidade de Pernambuco. Recife, Dezembro de 1999.
- ✓ **IBEKWE**, Chibuko Raphael. The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions. A Thesis Submitted to the School of Law, University of Stirling for the Degree of Doctor of Philosophy (PhD). JULY 2015.
- ✓ Implementation of the Budapest Convention on Cybercrime. Disponível em https://www.oas.org/juridico/PDFs/cyb9_coe_cyb_oas_Dec16_v1.pdf (acedido aos 19-07-2019).
- ✓ **JAKOBSSON** Markus; **MYERS**, Steven. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley-Interscience. 2006.

- ✓ **JEMILOHUN,** Bernard Oluwafemi. *Legislating Against Cybersquatting in Nigeria: Moving Beyond Penal Law Into Protective and Compensational Remedies*. Journal of Law, Policy and Globalizati. ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online) DOI: 10.7176/JLPG. Vol.84, 2019. Disponível em https://www.researchgate.net/publication/333324668_Legislating_Against_Cybersquatting_in_Nigeria_Moving_Beyond_Penal_Law_Into_Protective_and_Compensational_Remedies (Acedido aos 14-11-2019).
- ✓ **JOGENFORS**, Jonathan. Quantum Bitcoin: An Anonymous and Distributed Currency Secured by the No-Cloning Theorem of Quantum Mechanics. Information Coding Group, Department of Electrical Engineering. Linköping University. April 2016.
- ✓ **KOTTASOVA**, Ivana. Arrested Russian linked to theft of 117 million LinkedIn passwords. CNN Tech.
  Disponível em http://money.cnn.com/2016/10/20/technology/russian-hacker-arrested-linkedin-password/ (Acedido aos 11-05-2020).
- ✓ **KSHETRI**, Nir. Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management. Published online: 09 Apr. 2019. Disponível https://www.tandfonline.com/doi/full/10.1080/1097198X.2019.1603527 (Acedido aos 14-11-2019).

- ✓ **KUNRATH**, Josefa Cristina Tomaz Martins. A expansão da criminalidade no cyberespaço. – Feira de Santana: Universidade Estadual de Feira de Santana, 2017. Ebook ISBN: 978-85-7395-275-9. CDU: 343.9(81):004. Disponível em http://www.progesp.ufba.br/sites/progesp.ufba.br/files/dissertacao-final-josefa-cristina-tomaz-martins-kunrath-2014.pdf (acedido aos 19-07-2019).
- ✓ **LONG**, Johnny; **PINZON**, Scott; **WILES**, Jack & **MITNICK**, Kevin D. No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. Syngress. 2008.

- ✓ **LOPES**, Jéssica Rodrigues & **COTRIM,** Ana Carolina Tomicioli. Mecanismos de cooperação internacional de repressão e combate dos crimes cibernéticos. 2014. Disponível http://esamcuberlandia.com.br/revistaidea/index.php/idea/article/view/134 (Acedido aos 19-07-2019).
- ✓ **LU**, Zhou; **WANG**, Wenye & **WANG**, Cliff. Modeling and Evaluating Denial of Service Attacks for Wireless and Mobile Applications. Springer International, 2015.

- ✓ **MACEDO**, João Carlos Cruz Barbosa de, "Algumas considerações acerca dos crimes informáticos em Portugal", *in* Direito Penal Hoje, Coimbra Editora, 2009.
- ✓ **MAGRIÇO**, Manuel Eduardo Aires. Dissertação para a obtenção de grau de mestre em Guerra da Informação da Academia Militar. A exploração sexual de crianças no Ciberespaço - aquisição e valoração de prova forense de natureza digital. Setembro de 2012.
- ✓ **MALLIK**, Avijit; **AHSAN**, Abid; **SHAHADAT**, Mhia Md. Zaglul & **TSOU**, Jia-Chi. Man-in-the-middle-attack: Understanding in simple words. International Journal of Data and Network Science. January 2019, p. 77. Disponível em https://www.researchgate.net/publication/330249434_Man-in-the-middle-attack_Understanding_in_simple_words (Acedido aos 23-04-2020).
- ✓ **MANN**, Ian. Hacking the Human – Social Engineering Techniques and Security Countermeasures. Gower. 2018.

- ✓ **MARQUES**, Garcia & **MARTINS,** Lourenço. Direito da Informática, 2.ª Refundida e Actualizada ed., Almedina, Coimbra, 2006.

- ✓ **MARTINS,** A. G. Lourenço. "Criminalidade Informática." Direito da Sociedade da Informação, Vol. IV, Coimbra Editora, Junho de 2003, p. 9 a 41.
- ✓ **MAZZIOTTI**, Giuseppe. EU digital copyright law and the end-user [1 ed]. Springer-Verlag Berlin Heidelberg. 2008.
- ✓ **McQuade III**, Samuel C. Encyclopedia of Cybercrime. Greenwood Press. 2009.
- ✓ **MENEZES**, Umbelina Teresa João de. O Papel das Forças e Serviços de Segurança no Combate aos Crimes Cibernéticos em Angola. Dissertação para a obtenção do grau de Mestre em Segurança da Informação e Direito no Ciberespaço no Instituto Superior Técnico de Lisboa. Dezembro de 2016. Disponível em https://fenix.tecnico.ulisboa.pt/downloadFile/563345090415229/Dissertacao.pdf (Acedido aos 19-07-2019).
- ✓ **MARTELLOZZO**, Elena. Online Child Sexual Abuse: Grooming, Policing and Child Protection in a Multi-Media World. Routledge. ISBN 9780415732727.November 11, 2013.
- ✓ **MINAHIM**, Maria Auxiliadora de Almeida & **SPÍNOLA**, Luíza Moura Costa. A fraude cometida por meios informáticos sob o prisma da vitimodogmática. Revista de Direito Penal, Processo Penal e Constituição | e-ISSN: 2526-0200 | Maranhão | v. 3 | n. 2 | p. 144 - 160 | Jul/Dez. 2017. Double Blind Review pelo SEER/OJS. Recebido em: 29.11.2017. Aprovado em: 30.12.2017.
- ✓ **MORAIS**, Felipe Soares Tavares. Internet, Pornografia e Infância: a Criminalização da Posse de Pornografia Infantil. Revista do Ministério Público do Rio de Janeiro nº 64, Abr. – Jun. 2017.
- ✓ **NDUBUEZE**, Philip; Hussein, Mustapha D. & Zakariyya Muhammad Sarki. *Cyberstalking Awareness and Perception among Undergraduate Students in Nigeria.* Dutse Journal of Humanities and Social Sciences Vol. 2, Nº 2, September 2017. Disponível em https://www.researchgate.net/publication/325103033_Cyberstalking_Awareness_and_Perception_among_Undergraduate_Students_in_Nigeria (Acedido aos 14-11-2019).
- ✓ **NORMAN**, Alan T. Hacking: How to Make Your Own Keylogger in C++ Programming Language. Kindle Edition, 2017.
- ✓ **NUNES**, Duarte Alberto Rodrigues, O crime de dano relativo a programas ou outros dados informáticos, Revista do Ministério Público, Lisboa, Ano 39, nº 153 (Janeiro-Março 2018), p. 141-165.
- ✓ **NUNES**, Duarte Alberto Rodrigues. O crime de falsidade informática. Julgar Online, Outubro de 2017. Disponível em https://www.academia.edu/36977372/O_crime_de_falsidade_informática (Acedido em 03-01-2020).
- ✓ **OOGARAH-HANUMAN**, V.; **CHING**, Y. Li Luen; **WAN**, A. Y. Pat & **CHETTY**, Daren. Assessing the prevalence of cybercrime in Mauritius – Economic Review Volume 47, 4/2018. Disponível em https://euba.sk/www_write/files/SK/ekonomicke-rozhlady/2018/er4_2018_oogarah_ching_wan_chetty_fulltext.pdf (Acedido aos 14-11-2019).
- ✓ **OLIVEIRA**, Wilson. Técnicas para Hackers II - Soluções para Segurança. Edições Centro Atlântico, Abril de 2003.
- ✓ **ORJI**, U. J. A Discourse on the Perceived Defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity. *Communications Law: The Journal of Computer, Media and Telecommunications Law*, Vol. 17, no. 4. 2019.

- ✓ **ORJI**, U. J. Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation? In: Maybaum, M. et al. (eds.) *Architectures in Cyberspace – 7th International Conference on Cyber Conflict*. Tallinn: NATO CCD. 2015. Disponível em https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdf (Acedido aos 17-7-2019).
- ✓ **ORJI**, Uchenna Jerome. The African Union Convention On Cybersecurity: A Regional Response Towards Cyber Stability? Masaryk University Journal of Law and Technology 12(2):91. September 2018. DOI: 10.5817/MUJLT2018-2-1.Disponível em https://www.researchgate.net/publication/327986841_The_African_Union_Convention_on_Cybersecurity_A_Regional_Response_Towards_Cyber_Stability (Acedido aos 19-07-2019).
- ✓ **ORJI**, Uchenna Jerome.The defects of the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cybersecurity**.** October 2012 DOI: 10.1109/WCS.2012.6780881. Disponível em https://www.researchgate.net/publication/271546922_The_defects_of_the_Draft_African_Union_Convention_on_the_Establishment_of_a_Credible_Legal_Framework_for_Cybersecurity (Acedido aos 19-07-2019).
- ✓ **PARK**, Youngsam; **MCCOY**, Damon & **SHI**, Elaine. Understanding Craigslist Rental Scams. Conference Paper. DOI: 10.1007/978-3-662-54970-4_1. Issn: 0302-9743. May 2017.
- ✓ **PATEL**, Jayshree & **PANCHAL**, S. D. A survey on Pharming attack Detection and prevention Methodology. IOSR Journal of Computer Engineering (IOSR-JCE). e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 1 (Jan. - Feb. 2013).
- ✓ **PAVLIK**, Kimberly. Cybercrime, Hacking and Legislation. Walden University, USA. Journal of Cybersecurity Research – 2017 Volume 1, Number 1. Disponível em https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiX5pft1tnpAhV2ThUIHTyWCooQFjACegQIAxAB&url=https%3A%2F%2Fclutejournals.com%2Findex.php%2FJCR%2Farticle%2Fdownload%2F9966%2F10067%2F&usg=AOvVaw3g6ibiX0CEZrU8ZIn8FWPC (Acedido aos 12-05-2020).
- ✓ **PATROCÍNIO**, José Tomás Vargues. *Tornar-se pessoa e cidadão digital – Formar-se dentro e fora da escola na sociedade tecnológica globalizada* (dissertação de doutoramento). Universidade Nova de Lisboa, Lisboa, 2004. Disponível em http://run.unl.pt/handle/10362/1294 (Acedido aos 02-11-2019).
- ✓ **PEREIRA**, Joel Timóteo Ramos, Compêndio Jurídico da Sociedade da Informação. Quid Juris, Abril de 2004.
- ✓ **PEREIRA**, Joel Timóteo Ramos. Direito da Internet e Comércio Electrónico, Quid Juris, Lisboa, 2002.
- ✓ **PURAM**, Pradeep Kumar; **KAPARTHI**, Mukesh; **RAYAPROLU**, Haas & **KRISHNA**, Aditya. Online scams: taking the fun out of the internet. September 2011.
- ✓ **ROCHA**, Manuel António Lopes. A revisão do código penal: soluções de neocriminalização. In Jornadas de direito criminal: revisão do código penal. Centro de Estudos Judiciários. 1º Vol, 1998.

- ✓ **RODRIGUES**, Benjamim Silva. Direito Penal - Parte Especial. Direito Penal Informático-Digital. Tomo I-D, Coimbra Editora, 2009.
- ✓ **ROXIN**, Claus, Crimes de Posse. Tradução de José Danilo Tavares Lobato. Revista Liberdades, IBCCRIM, nº 12, Jan. – Abr. 2013.
- ✓ **SANTOS**, Adriano Edgar dos. Os meios de tutela do direito de autor e direito conexo no direito angolano. Dissertação de Mestrado em Ciências Jurídicas orientada pela Professora Doutora Adelaide Menezes Leitão. Universidade de Lisboa. Faculdade de Direito. Lisboa Abril/2017. Disponível em https://repositorio.ul.pt/bitstream/10451/31636/1/ulfd134164_tese.pdf (Acedido aos 21-01-2020).
- ✓ **SANTOS**, Ana Felícia Canilho. O Cibercrime: Desafios e Respostas Do Direito. Dissertação de Mestrado para a obtenção do grau de Mestre em Direito, especialidade em Ciências Jurídicas. Universidade Autónoma de Lisboa. Setembro de 2015.
- ✓ **SANTOS**, Paulo; **PIMENTEL**, Carlos & **BESSA**, Ricardo. Cyberwar. FCA. 2008.
- ✓ **SANTOS**, Rita Coelho. O tratamento jurídico-penal da transferência de fundos monetários através da manipulação ilícita dos sistemas informáticos. Coimbra Editora, 2005.
- ✓ **SILVA,** Flávio Manuel Carneiro da. A usurpação da ciberidentidade. *Dissertação de Mestrado em Direito Criminal, realizada sob a orientação do Exmo. Senhor Professor Doutor José M. Damião da Cunha.* Porto 2014.
- ✓ **SILVA**, José da Cruz Andrade e. A integração das TIC no ensino secundário em Cabo Verde: Um estudo de caso. Departamento de Educação e Ensino a Distância. Mestrado em Comunicação Educacional Multimédia. Universidade Aberta, Lisboa. Novembro de 2014.
- ✓ **SOTTO-MAYOR**, Belmiro; **FERREIRA**, Paulo e **LESSA** André. Aspectos sociais da informática criminalidade informática – desafios de uma nova geração. Faculdade de Engenharia da Universidade do Porto. Trabalho realizado no âmbito da disciplina de Aspectos Sociais da Informática, leccionada por Manuel Veiga de Faria. Maio de 2006.
- ✓ **TAYLOR**, M. The nature and dimensions of child pornography on the Internet. Paper prepared for the conference Combating Child Pornography on the Internet, Vienna. (1999, September 29 – October 1).
- ✓ **TAYLOR**, Paul. 'Hacktivism: in search of lost ethics?' Crime and the Internet. Edited by David S. Wall, 2001, 59-73.
- ✓ **TEIXEIRA**, Paulo Alexandre Gonçalves. O fenómeno do *phishing* enquadramento jurídico-penal. Dissertação para obtenção do grau de Mestre em Direito, especialidade em Ciências Jurídico-Criminais. Universidade do Minho. Orientado pelo Prof. Doutor Fernando Conde Monteiro. Fevereiro, Lisboa, 2013.
- ✓ **TOPKARA**, Mercan; **KAMRA**, Ashish; **ATALLAH**, Mikhail J. & **NITA-ROTARU**, Cristina. Viwid: Visible watermarking based defense against phishing. Digital Watermarking. Springer Link. 2005.
- ✓ **THOMPSON**, N. 'You've got fraud!' Foreign Policy, Washington: May/Jun. 2003.
- ✓ **VENÂNCIO,** Pedro Dias. Lei do Cibercrime Anotada e comentada. Coimbra Editora, Fevereiro de 2011.

- ✓ **VENÂNCIO,** Pedro Dias. Breve introdução da questão da investigação e meios de prova na criminalidade informática. Compilações doutrinais verbo jurídico. Dezembro 2006. Disponível em https://www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf (Acedido aos 15-01-2020).
- ✓ **VERDELHO,** Pedro**.** "A nova Lei do Cibercrime", *in* Scientia Ivridica, T. LVII, Universidade do Minho, Braga, 2009, pp. 717 e ss.
- ✓ **VERDELHO**, Pedro. "Cibercrime." Direito da Sociedade da Informação. Vol. IV, Coimbra Editora, Junho de 2003, p. 347 a 383.
- ✓ **VERDELHO**, Pedro. "A Convenção Sobre Cibercrime do Conselho da Europa - Repercussões Na Lei Portuguesa." Direito da Sociedade da Informação, vol. VI, Coimbra Editora, 2006, p. 257 a 276.
- ✓ **VERDELHO**, Pedro. Comentário das Leis Penais Extravagantes. Organizado por Paulo Pinto de Albuquerque e José Branco. Vol. 1, Universidade Católica Editora, 2010.
- ✓ **VIANNA**, Túlio e **MACHADO** Felipe. Crimes Informáticos. Belo Horizonte. Editora Fórum, 2013.

- ✓ **VIDROS**, Sokratis; **KOLIAS**, Constantinos & **KAMBOURAKIS**, Georgios. Online recruitment services: Another playground for fraudsters. George Mason University. Article (PDF Available) in Computer Fraud & Security 2016(3):8-13 · March 2016. DOI: 10.1016/S1361-3723(16)30025-2. Disponível em https://www.researchgate.net/publication/299346771_Online_recruitment_services_Another_playground_for_fraudsters (Acedido aos 12-05-2020).

- ✓ VV. Explanatory Report to the Convention on Cybercrime. Council of Europe, 2001. Disponível em http://conventions.coe.int./Treaty/en/Reports/Html/185.htm (Acedido aos 12-05-2020).
- ✓ **WALDEN**, Ian. Computer crimes and digital investigations. Second Edition. Oxford University Press. 2007.
- ✓ **YANG**, Jie; **CHEN**, Yingying; **TRAPPE**, Wade & **CHENG**, Jerry. Pervasive Wireless Environments: Detecting and Localizing User Spoofing. Springer, 1st ed. 2014.
- ✓ **YU**, Shui. Distributed Denial of Service Attack and Defense. Springer-Verlag New York, 2014.

- ✓ **ZALANA**, Sundi Henrieth. Cibersegurança nas Infraestruturas Críticas Angolanas do Sector das Tecnologias de Informação e Comunicação. Dissertação para a obtenção do grau de Mestre em Segurança da Informação e Direito no Ciberespaço no Instituto Superior Técnico de Lisboa. Dezembro de 2016. Disponível em https://fenix.tecnico.ulisboa.pt/downloadFile/1970719973966302/Dissertacao_Cibersegurança%20nas%20Infraestruturas%20Criticas%20do%20Sector%20das%20TIC%20em%20Angola.pdf (Acedido aos 19-07-2019).

- ✓ **ZDZIARSKI**, Jonathan. Hacking and Securing IOS Applications: Stealing Data, Hijacking Software, and How to Prevent It. O'Reilly Media. 2012.

Documentos Normativos

- ✓ African Union Convention on Cyber Security and Personal Data Protection, 27 June 2014.
- ✓ Anteprojecto de Lei de Combate à Criminalidade no Domínio das Tecnologias de Informação e Comunicação e dos Serviços da Sociedade da Informação de 2011.
- ✓ Anteprojeto de Código Penal Angolano.
- ✓ Código Penal da República de Angola aprovado por intermédio do art.º 165º da Lei Constitucional que adotou para a realidade angolana o então Código Penal Português aprovado pelo Decreto de 16 de Setembro de 1886.
- ✓ Constituição da República de Angola de 2010.
- ✓ Convenção da União Africana sobre o Cibercrime e a Proteção de Dados de 27 de Junho de 2014.
- ✓ Convenção de Budapeste sobre o cibercrime de 23 de Novembro de 2001.
- ✓ Cybercrime Act 2015 – was passed into Law by the Nigerian National Assembly on the 5th of May, 2015. (Lei do Cibercrime da Nigéria aprovada pela Assembleia Nacional da Nigéria em 5 de Maio de 2015).
- ✓ Directiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de Maio de 2001, relativa à harmonização de certos aspectos do direito de autor e dos direitos conexos na sociedade da informação.
- ✓ Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- ✓ Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de Julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.
- ✓ Diretiva 2013/40/UE do Parlamento Europeu e do Conselho de 12 de Agosto de 2013.
- ✓ Lei n.º 109/2009 de 15 de Setembro, Lei do Cibercrime de Portugal.
- ✓ Lei n.º 7/17 da Protecção das Redes e Sistemas Informáticos (Diário da República no dia 16 de Fevereiro de 2017).
- ✓ Lei nº 12.737/12, conhecida como Lei Carolina Dieckmann, que foi acrescida ao Código Penal brasileiro.
- ✓ Lei nº 15/14 de 31 de Julho dos direitos do autor e conexos de Angola.
- ✓ Lei nº 4/90, de 10 de Março, dos Direitos de Autor.
- ✓ Lei sobre o cibercrime (Lei 08/IX/2017) de Cabo Verde.
- ✓ Recomendação nº (89)9 do Conselho da Europa aprovada pelo Comité de Ministros em 13 de Setembro de 1989 na 428.ª reunião dos deputados.
- ✓ Regulamento (CE) nº 808/2004, de 21 de Abril de 2004, relativo às estatísticas comunitárias sobre a sociedade da informação.
- ✓ Regulamento das Tecnologias e dos Serviços da Sociedade da Informação (Decreto Presidencial nº 202/11 de 22 de Julho);
- ✓ The Computer Misuse And Cybercrime Act 2003 – Act No. 22 of 30 July 2003 (Lei do Cibercrime das Ilhas Maurícias Lei nº 22 de 30 de julho de 2003).

Webgrafia

https://angoweb.net/quem-somos/ (Acedido aos 19-05-2020).
http://aei.pitt.edu/8692/1/8692.pdf (Acedido aos 04-11-2019).
http://cert-mu.govmu.org/English/Documents/Cybercrime%20Strategy/National%20Cybercrime%20Strategy-%20August%202017.pdf (Acedido aos 14-11-2019).
http://cibercrime.ministeriopublico.pt/pagina/2a-reuniao-do-forum-cibercrime-praia-cabo-verde (Acedido aos 16-11-2019)
http://cibercrime.ministeriopublico.pt/pagina/jurisprudencia-sobre-cibercrime. Acedido aos 31-08-2020).

http://cibercrime.ministeriopublico.pt/pagina/quem-somos (Acedido aos 22-05-2020).
http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/decl_santa_maria_final.pdf (Acedido aos 22-05-2020).
http://cipstp.st/wp-content/uploads/2018/03/Lei_15_2017-Lei-sobre-Cibercrime.pdf (Acedido aos 17-11-2019).
http://cipstp.st/wp-content/uploads/2018/03/Lei_15_2017-Lei-sobre-Cibercrime.pdf (Acedido aos 18-11-2019).
http://cybercrime.org.za/docs/Cybercrimes_and_Cybersecurity_Bill_2015.pdf (Acedido aos 10-11-2019).
http://dominios.co.ao (Acedido aos 19-05-2020).
http://dpp.govmu.org/English/Documents/Legislation/CHILD%20PROTECTION.pdf (Acedido aos 14-11-2019).
http://emersoft.co.ao/servicos.php (Acedido aos 19-05-2020).
https://en.wikipedia.org/wiki/Cybersquatting (Acedido aos 14-11-2019).
http://euroogle.com/dicionario.asp?definition=487 (Acedido aos 05-11-2019).

http://index-of.es/Sniffers/Sniffers_pdf/Cap6-Sniffers.pdf (Acedido aos 16-04-2020).
http://jornaldeangola.sapo.ao/opiniao/artigos/o_novo_codigo_penal_angolano (Acedido aos 06-09-2019).
https://www.dw.com/pt-002/angola-poderá-o-novo-código-penal-travar-a-criminalidade/a-47199914 (Acedido aos 06-09-2019).
http://jornaldeangola.sapo.ao/politica/ministerio-da-comunicacao-social-fundido-ao-das-telecomunicacoes (Acedido aos 20-07-2020)
http://jornaldeangola.sapo.ao/reportagem/crimes_ciberneticos_carecem_de_legislacao (Acedido aos 19-05-2020).
http://m.portalangop.co.ao/angola/pt_pt/noticias/politica/2019/3/17/Huila-Magistrado-aborda-combate-aos-crimes-ciberneticos,3aa95b82-5744-4c8f-a136-be9b9023b16b.html (Acedido aos 21-05-2020).

http://tpa.sapo.ao/noticias/economia/inacom-alerta-para-ataques-as-redes-de-telefonia-movel (Acedido aos 22-06-2020).
http://www.4law.co.il/portu1.htm (Acedido aos 06-04-2020).
http://www.angonoticias.com/Artigos/item/59445/governo-prepara-lei-para-combater-noticias-falsas (Acedido aos 18-11-2019). https://www.lexlink.eu/conteudo/geral/ia-

serie/3908112/decreto-presidencial-no-27719/14793/por-tipo-de-documentolegal (Acedido aos 18-11-2019).
http://www.angop.ao/angola/pt_pt/noticias/economia/2019/11/51/Angola-tem-mais-seis-milhoes-utilizadores-internet,1b1c3cee-23d4-4bea-9a7f-8395923810f1.html (Acedido aos 14-05-2020).
http://www.avm.biz/conteudo/pt/1268/aprovacao-da-lei-de-proteccao-das-redes-e-sistemas-informaticos/ (Acedido aos 18-11-2019).
http://www.cnpd.cv/leis/Lei%20de%20Cibercrime.pdf (Acedido aos 18-11-2019).
http://www.dgpj.cv/index.php/news/171-seminario-internacional-sobre-cibercrime-e-prova-eletronica-harmonizacao-de-legislacao-e-a-convencao-de-budapest-na-cplp (Acedido aos 22-05-2020).
http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/03f18004fd3cc9f48025815200495ae7?OpenDocument (Acedido aos 11-05-2020).
http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/4ab28f88e6e98b2880257cb7004ee59f?OpenDocument (Acedido aos 12-01-2020).
http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/ae4145b5e5a62059802574f70058c7fe?OpenDocument (Acedido aos 14-01-2020).
http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/e4727d7882f56c9d80257f610055dc8e?OpenDocument (Acedido aos 05-05-2020).
http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/d97beb78d90d426b80257e5800393b9d?OpenDocument (Acedido em 06-01-2019).
http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/505fcfb3e621198980257be30035d463?OpenDocument (Acedido aos 15-01-2020).
http://www.dgsi.pt/jtrl.nsf/e6e1f17fa82712ff80257583004e3ddc/8cac11c0fbb3ec6a80257491003da99f?OpenDocument (Acedido aos 06-10-2019).
http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/b54faf2d4330b8d480257c6e004ff2df?OpenDocument (Acedido aos 6-12-2019).
http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/df9b304aeb07b7958025722c00049ad30?OpenDocument (Acedido aos 29-02-2020).
http://www.dgsi.pt/jtrp.nsf/c3fb530030ea1c61802568d9005cd5bb/872f3063233d8de480257b78003e60f3?OpenDocument (Acedido aos 06-01-2019).
http://www.governo.gov.ao (Acedido aos 14-05-2020).
http://www.governo.gov.ao/VerLegislacao.aspx?id=459 (Acedido aos 29-02-2020).
http://www.hostingangola.com/dominios.html (Acedido aos 19-05-2020).
http://www.itu.int/net/wsis/docs2/regional/outcome-accra.pdf (Acedido aos em 12-11-2019)
http://www.itu.int/net/wsis/implementation/index.html (Acedido aos 04-11-2019).
http://www.markus-jakobsson.com/. (Acedido aos 17-04-2020).
http://www.mtti.gov.ao (Acedido aos 14-05-2020).
http://www.mtti.gov.ao/Institucionais/Historico.aspx (Acedido aos 11-05-2020).
http://www.mtti.gov.ao/VerLegislacao.aspx?id=456 (Acedido aos 18-11-2019).
http://www.mtti.gov.ao/VerLegislacao.aspx?id=456 (Acedido aos 28-07-2019).
http://www.novojornal.co.ao/economia/interior/sonangol-ataque-informatico-obriga-a-medidas-extraordinarias-para-processar-salarios-de-junho-73307.html (Acedido aos 14-01-2020).
http://www.oas.org/juridico/english/89-9&final%20Report.pdf (Acedido aos 17-11-2019).
http://www.parlamento.ao/documents/91841/0/PROPOSTA+DE+LEI+DO+CÓDIGO+PENAL (Acedido aos 03-03-2020)

http://www.parlamento.cv/GDiploApro3.aspx?CodDiplomasAprovados=80329 (Acedido aos 31-10-2020)
https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_201809June_Final_Portuguese.pdf (Acedido aos 31-10-2020).
http://www.parlamento.cv/GDiploApro3.aspx?CodDiplomasAprovados=80329 (Acedido aos 31-10-2020)
https://www.internetsociety.org/wp-content/uploads/2018/05/AUCPrivacyGuidelines_201809June_Final_Portuguese.pdf (Acedido aos 31-10-2020).
http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis (Acedido aos 18-11-2019).
http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1481&tabela=leis&ficha=1&pagina=1 (Acedido aos 12-01-2020).
http://www.portaldeangola.com/2013/05/angola-tem-actualmente-cinco-milhoes-de-usuariosde-internet/ (Acedido aos 20- 07-2019).
http://www.redeangola.info/empresas-alertam-para-aumento-de-ataques-online-no-pais/ (Acedido aos 14-01-2020).
http://www.spamfighter.com/News-20202-Anonymous-Attacks-Government-of-Angola-due-to-Jail-Sentence-for-17-Activists.htm (Acedido aos 09-09-2019).
http://www.tistech.co.ao/home (Acedido aos 15-01-2020).
http://www.unitel.ao/servlet/web/A-Unitel (Acedido aos 13-01-2020).
https://1635-ao.all.biz (Acedido aos 13-01-2020).
https://16minionuapmbc2024.wordpress.com/2015/09/01/assinarratificar-faz-tanta-diferenca-assim/ (Acedido aos 17-11-2019).
https://africacheck.org/reports/does-south-africa-rank-third-in-the-world-for-online-crime-losing-r2-2bn-a-year/ (Acedido aos 10-11-2019).
https://angola.shafaqna.com/PT/AL/296358 (Acedido aos 16-07-2020).
https://angola24horas.com/index.php/politica/item/15036-angorascom-s-a-substitui-angola-telecom-com-a-terceira-operadora-de-telefonia-movel (Acedido aos 14-05-2020).
https://angolaforex.com/2019/05/19/specialist-ao-dr-moses-caiaia-o-direito-angolano-aplicavel-ao-comercio-electronico-ii/ (Acedido aos 16-07-2020).
https://angolaforex.com/2020/03/10/diario-da-republica-i-a-serie-n-o-23-de-3-de-marco-de-2020/ (Acedido aos 06-04-2020).
https://angolasites.com (Acedido aos 19-05-2020).
https://angorussia.com/tech/rede-da-operadora-unitel-sofre-ataque-cibernetico/ (Acedido aos 22-06-2020).
https://animalexdominis.files.wordpress.com/2018/03/proteccc3a7c3a3o-das-redesesistemas-informc3a1ticos-2017.pdf (Acedido aos 18-11-2019).
https://animalexdominis.files.wordpress.com/2018/03/proteccc3a7c3a3o-das-redesesistemas-informc3a1ticos-2017.pdf (Acedido aos 15-01-2020).
https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (Acedido aos 17-11-2019).

https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (Acedido aos 12-11-2019).
https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (Acedido aos 12-11-2019).
https://ccdcoe.org/uploads/2018/10/Art-08-Multilateral-Legal-Responses-to-Cyber-Security-in-Africa-Any-Hope-for-Effective-International-Cooperation.pdf (Acedido aos 17-11-2019).
https://cipesa.org/?wpfb_dl=143 (Acedido aos 17-11-2019).
https://clubofmozambique.com/news/anonymous-cyber-attack-shuts-down-20-angolan-government-websites-after-activists-jailed/ (Acedido aos 14-01-2020).
https://consultor-juridico.jusbrasil.com.br/noticias/100326806/o-novo-crime-de-invasao-de-dispositivo-informatico (Acedido aos 18-02-2020).
https://cordis.europa.eu/event/rcn/2139/es (Acedido aos 04-11-2019).

https://crics.mandela.ac.za (Acedido aos 10-11-2019).

https://cvtradeinvest.com/tics (Acedido aos 10-11-2019).
https://direitofamiliar.jusbrasil.com.br/artigos/597009198/pornografia-de-vinganca-o-que-e-isso (Acedido aos 17-11-2019).
https://eco.sapo.pt/2017/08/22/como-a-queda-do-petroleo-tramou-a-economia-angolana/ (Acedido aos 17-11-2019).
https://e-global.pt/noticias/lusofonia/angola/angola-agencia-nacional-de-proteccao-de-dados-vai-funcionar-em-breve-no-pais/ (Acedido aos 18-11-2019).
https://egmontgroup.org/fr/node/2528https://www.academia.edu/11145613/NIGERIAN_FINANCIAL_INTELLIGENCE_UNIT_SERVES_AS_A_TOOL_TO_PROTECT_THE_INTEGRITY_OF_THE_NIGERIAN_FINANCIAL_SYSTEM(Acedido aos 14-11-2019).

https://empresas.verangola.net/show/13425 (Acedido aos 13-01-2020).
https://en.m.wikipedia.org/wiki/Economic_and_Financial_Crimes_Commission (Acedido aos 12-05-2020).
https://en.wikipedia.org/wiki/Advance-fee_scam (Acedido aos 12-05-2020).
https://en.wikipedia.org/wiki/Anti-Phishing_Working_Group (Acedido aos 20-04-2020).
https://en.wikipedia.org/wiki/Carbon_Black_(company) (Acedido aos 15-01-2020).
https://en.wikipedia.org/wiki/CNET (Acedido aos 14-01-2020).
https://en.wikipedia.org/wiki/Convention_on_Cybercrime (Acedido aos 07-11-2019).

https://en.wikipedia.org/wiki/Cyberspace (Acedido aos 02-11-2019)

https://en.wikipedia.org/wiki/DNS_spoofing (Acedido aos 23-04-2020).
https://en.wikipedia.org/wiki/Internet#cite_note-5 (Acedido aos 08-10-2019).
https://en.wikipedia.org/wiki/Internet_governance (Acedido aos 08-10-2019)
https://en.wikipedia.org/wiki/MAC_address (Acedido aos 27-05-2020).
https://en.wikipedia.org/wiki/Project_Shield (Acedido aos 14-01-2020).
https://en.wikipedia.org/wiki/Sniffing_attack (Acedido aos 15-04-2020).
https://en.wikipedia.org/wiki/WannaCry_ransomware_attack (Acedido aos 20-04-2020).
https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX:31998H0560 (Acedido aos 05-11-2019).

https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046 (Acedido aos 05-11-2019).
https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32001L0029 (Acedido aos 05-11-2019).
https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32004R0460 (Acedido aos 05-11-2019).
https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32004R0808 (Acedido aos 05-11-2019).
https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:52000DC0890 (Acedido aos 05-11-2019).
https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000Y1014(02)&from=EN (Acedido aos 05-11-2019).
https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0040&from=EN (Acedido aos 17-01-2020).
https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32004F0068&from=LV (Acedido aos 20-01-2020).
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0229:FIN:PT:PDF (Acedido aos 05-11-2019).
https://expressodasilhas.cv/eitec/2018/10/12/cibercrime-legislacao-evolui-mas-tecnologia-e-mais-rapida/60468 (Acedido aos 17-11-2019).
https://expressodasilhas.cv/pais/2019/04/11/pgr-quer-resposta-mais-efectiva-ao-cibercrime/63301 (Acedido aos 16-11-2019)
https://informativoangolano.com/tecnologia/angola-sofre-ataque-nas-redes-das-operadoras-moveis-nas-ultimas-horas/ (Acedido aos 22-06-2020).
https://infrasat.net (Acedido aos 14-05-2020).
https://intellipaat.com/blog/tutorial/ethical-hacking-cyber-security-tutorial/sniffing-attacks/ (Acedido aos 15-04-2020).
https://jus.com.br/artigos/5828/do-delito-de-dano-e-de-sua-aplicacao-ao-direito-penal-informatico (Acedido em 26-12-2019).

https://jus.com.br/artigos/72969/convencao-de-budapeste-e-cibercrimes (Acedido aos 07-11-2019).
https://lexlink.eu/conteudo/geral/ia-serie/3925437/resolucao-no-52019/20525/por-tipo-de-documentolegal (Acedido aos 08-05-2020).
https://m.portalangop.co.ao/angola/pt_pt/mobile/noticias/ciencia-e-tecnologia/2019/2/13/Angola-ensaia-regulacao-das-redes-sociais,c8a21f25-86e9-4aa4-917a-f350cd107ec6.html?version=mobile (Acedido aos 14-05-2020).
https://macauhub.com.mo/pt/2019/12/18/pt-angola-tem-14-milhoes-de-utilizadores-de-telefonia-movel/ (Acedido aos 14-05-2020).
https://observador.pt/2019/06/07/imprensa-angolana-da-conta-de-ataque-cibernetico-a-petrolifera-sonangol/ (Acedido aos 14-01-2020).
https://observador.pt/2020/04/21/cibercrimes-aumentam-de-forma-exponencial-durante-a-pandemia/ (Acedido aos 19-05-2020).
https://opais.co.ao/index.php/2019/07/26/angola-entre-os-paises-menos-afectados-por-crimes-ciberneticos/ (Acedido aos 19-05-2020).
https://opais.co.ao/index.php/2019/11/08/angorascom-telecomunicacoes-s-a-e-a-quarta-operadora-de-telefonia-movel/ (Acedido aos 14-05-2020).

https://opais.co.ao/index.php/2020/02/26/angola-e-hungria-cooperam-no-combate-ao-crime-cibernetico-e-transfronteirico/ (Acedido aos 22-05-2020).
https://portswigger.net/daily-swig/south-africa-welcomes-new-cybercrime-legislation (Acedido aos 10-11-2019).
https://pt.wikinews.org/wiki/Crime_cibernético_chega_a_Angola (Acedido aos 23-05-2020).
https://pt.wikipedia.org/wiki/Acesso_à_Internet (Acedido aos 28-07-2019)
https://pt.wikipedia.org/wiki/África_do_Sul (Acedido aos 10-11-2019).
https://pt.wikipedia.org/wiki/Aldeia_Global (Acedido aos 02-11-2019).
https://pt.wikipedia.org/wiki/Analisador_de_pacotes (Acedido aos 15-04-2020).
https://pt.wikipedia.org/wiki/AngoSat-1 (Acedido aos 13-01-2020).
https://pt.wikipedia.org/wiki/Ataque_man-in-the-middle (Acedido aos 23-04-2020).
https://pt.wikipedia.org/wiki/Ataque_man-in-the-middle (Acedido aos 24-04-2020).
https://pt.wikipedia.org/wiki/Carding (Acedido em 03-01-2020).
https://pt.wikipedia.org/wiki/Crime_informático (Acedido aos 28-01-2020).
https://pt.wikipedia.org/wiki/Cyberstalking (Acedido aos 14-11-2019).
https://pt.wikipedia.org/wiki/Dia_Mundial_da_Sociedade_da_Informação (Acedido aos 04-11-2019).
https://pt.wikipedia.org/wiki/Engenharia_social_(segurança) (Acedido aos 07-04-2020).
https://pt.wikipedia.org/wiki/Pornografia_de_vingança (Acedido aos 17-11-2019).
https://pt.wikipedia.org/wiki/Unitel (Acedido aos 13-01-2020).
https://pt.wikipedia.org/wiki/William_Gibson (Acedido aos 02-11-2019).
https://repositorium.sdum.uminho.pt/bitstream/1822/40898/1/Pedro%20Levi%20Vieira%20de%20Oliveira%20Heitor.pdf (Acedido aos 27-11-2019).
https://rm.coe.int/dpa-2017-maurice/168077c5b8 (Acedido aos 14-11-2019).
https://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan (Acedido aos 18-02-2020).
https://sniac.cv/wp-content/uploads/2018/03/SNIAC-Lei-nº-43-VIII-2013-Cria-e-Regula-SNIAC.pdf (Acedido aos 17-11-2019).
https://softwarelab.org/pt/hacking/ (Acedido aos 07-04-2020).
https://threatpost.com/iot-botnets-are-the-new-normal-of-ddos-attacks/121093/ (Acedido aos 14-01-2020).
https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html (Acedido aos 23-04-2020)
https://usa.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer (Acedido aos 15-04-2020).
https://valoreconomico.co.ao/artigo/lei-contra-crimes-informaticos-ja-em-vigor (Acedido aos 21-05-2020).
https://www.aapsi.og.ao/noticia/angola-instala-primeira-replica-de-um-servidor-raiz-de-internet (Acedido aos 19-05-2020).
https://www.aapsi.og.ao/sobre-nos#mission (Acedido aos 19-05-2020).
https://www.angohost.ao (Acedido aos 19-05-2020).
https://www.angolacables.co.ao (Acedido aos 13-01-2020).
https://www.angop.ao/angola/en_us/noticias/economia/2019/5/23/Oil-company-Sonangol-targeted-cyber-attack,9f7b89d6-bb91-42c3-b886-93cdb3691e3a.html (Acedido aos 14-01-2020).

https://www.angop.ao/angola/pt_pt/noticias/africa/2016/10/47/Cabo-Verde-Assembleia-aprova-lei-sobre-cyber-crime-recolha-provas-suporte-electronico,a67d4fa8-2dbc-47f9-bd63-270396e8c681.html (Acedido aos 16-11-2019).
https://www.apc.org/fr/pubs/case-“open-access”-communications-infrastructure-africa-sat-3wasc-cable (Acedido aos 13-01-2020)
https://www.cambridge.org/core/books/principles-of-cybercrime/misuse-of-devices/42940535CBFE1E3834219EF14ADAACBD (Acedido aos 18-02-2020).
https://www.canterbury.ac.uk/social-and-applied-sciences/law-criminal-justice-and-policing/docs/poc/PoC-24-7-Final-Report.pdf (Acedido aos 31-01-2020).
https://www.cbn.gov.ng/Out/2016/CCD/NEFF%202014%20Annual%20Report%20.pdf (Acedido aos 14-11-2019).
https://www.cbn.gov.ng/Out/2016/CCD/NeFF-%20Annual%20Report%202015.pdf (Acedido aos 14-11-2019).
https://www.cbn.gov.ng/Out/2017/CCD/A%20CHANGING%20PAYMENTS%20ECOSYSTEM%20NeFF%202016%20Annual%20Report.pdf (Acedido aos 14-11-2019).
https://www.cnet.com/news/google-project-shield-botnet-distributed-denial-of-service-attack-ddos-brian-krebs/ (Acedido aos 13-01-2020).
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Acedido aos 06-10-2019).
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Acedido aos 07-11-2019).
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (Acedido aos 10-11-2019).
https://www.coe.int/en/web/cybercrime/glacyplus (Acedido aos 14-11-2019).
https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/nigeria/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=fr_FR (Acedido aos 15-11-2019).
https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese-ExpRep.pdf (Acedido aos 16-01-2020).
https://www.consultancy.africa/news/30/africa-will-break-through-1-billion-mobile-internet-connections-by-2022 (Acedido aos 14-11-2019).

https://www.csm.org.pt/ficheiros/pareceres/2009/parecer09_05.pdf (Acedido aos 16-04-2020).
https://www.deco.proteste.pt/tecnologia/tablets-computadores/noticias/pornografia-de-vinganca-pode-dar-pena-de-prisao-ate-5-anos# (Acedido aos 17-11-2019).
https://www.dn.pt/lusa/aprovacao-do-novo-codigo-penal-angolano-foi-momento-historico—presidente-10680112.html (Acedido aos 18-11-2019).
https://www.dn.pt/lusa/conselho-de-europa-pede-adesao-de-paises-lusofonos-a-convencao-sobre-cibercrime–10785869.html (Acedido aos 10-11-2019).
https://www.dn.pt/lusa/pgr-angolana-vai-criar-gabinete-para-combate-de-crimes-informaticos-6246264.html (Acedido aos 21-05-2020).
https://www.eff.org/deeplinks/2019/09/nigeria-misuses-overbroad-cyberstalking-law-levels-charges-against-political (Acedido aos 14-11-2019).

https://www.fd.unl.pt/Anexos/Investigacao/1274.pdf (Acedido aos 19-07-2020).
https://www.forcepoint.com/cyber-edu/man-in-the-middle-attack (Acedido em 24-04-2020).

https://www.globalreach.com/about/newsletters/grip-newsletter/6-ways-to-avoid-internet-scams/6-scam-savvy-tips/ (Acedido aos 12-05-2020).
https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjF2-u1od7pAhWORhUIHZdTCEUQFjAEegQIBhAB&url=http%3A%2F%2Fwww.mtti.gov.ao%2Fdownload.aspx%3Fid%3D1202%26tipo%3Dlegislacao&usg=AOvVaw2Q3Bt3c4xvog1qcHn0Sc7Y (Acedido aos 31-05-2020).
https://www.google.pt/search?q=cyber+attack+angolan+government&client=opera&sa=N&biw=1496&bih=722&tbm=isch&source=iu&ictx=1&fir=8J8-AOPYpnmKPM%253A%252C_4JhB6R6UQNq_M%252C_&vet=1&usg=AI4_-kRQpupoKbkJWx9UPbddjSsFxiTuiQ&ved=2ahUKEwiilPyxrLnjAhXmA2MBHSE-DYg4ChD1ATADegQIBhAE#imgrc=8J8-AOPYpnmKPM:&vet=1 (Acedido aos 14-01-2020).
https://www.governo.gov.ao/VerLegislacao.aspx?id=2430 (Acedido aos 20-07-2020).
https://www.greycampus.com/opencampus/ethical-hacking/sniffing-and-its-types (Acedido aos 16-04-2020).
https://www.iberweb.co.ao/alojamento/ (Acedido aos 19-05-2020).
https://www.icta.mu/docs/laws/ict_act.pdf (Acedido aos 14-11-2019).
https://www.infopedia.pt/dicionarios/lingua-portuguesa/cibercriminoso (Acedido aos 28-07-2019)
https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (Acedido aos 13-01-2020).
https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (Acedido aos 13-01-2020).
https://www.itu.int/net4/ITU-D/idi/2017/index.html (Acedido aos 10-11-2019).
https://www.jn.pt/justica/extorsao-sexual-na-net-nao-para-de-aumentar-4774319.html (Acedido aos 03-11-2019).
https://www.jornaldenegocios.pt/economia/mundo/africa/angola/detalhe/sonangol-foi-alvo-de-ataque-informatico (Acedido aos 14-01-2020).

https://www.lexology.com/library/detail.aspx?g=f16ede4c-f04a-40a7-96c3-e6a4899f3cf0 (Acedido aos 15-11-2019).
http://nji.gov.ng/images/Workshop_Papers/2016/Refresher_Magistrates/s09.pdf (Acedido aos 15-11-2019)
https://www.makaangola.org/2019/08/ataque-cibernetico-a-sonangol/ (Acedido aos 15-01-2020).
https://www.menosfios.com/en/sonangol-suffered-cyber-attack/ S (Acedido aos 08-05-2020).
https://www.menosfios.com/infrasat-torna-sociedade-comercial-tratara-rentabilizar-angosat/ (Acedido aos 14-05-2020).

https://www.menosfios.com/lei-os-ciberataques-ja-esta-vigor-angola/ (Acedido aos 14-01-2020).
https://www.menosfios.com/policia-nacional-leva-criminalidade-informatica-debate-hoje-as-19h-na-ugs/ (Acedido aos 14-01-2020).
https://www.mstelcom.co.ao (Acedido aos 13-01-2020).
https://www.newsweek.com/2013/05/29/hackers-are-spying-you-inside-world-digital-espionage-237478.html (Acedido aos 14-01-2020).
https://www.plataformamedia.com/pt-pt/noticias/economia/libanesa-africell-selecionada-para-4-operadora-de-telecomunicacoes-em-angola-11877296.html (Acedido aos 14-05-2020).
https://www.plataformamedia.com/pt-pt/noticias/sociedade/agencia-de-protecao-de-dados-admite-uso-indevido-de-dados-pessoais-em-instituicoes–11385102.html (Acedido aos 18-11-2019).

https://www.plenglish.com/index.php?o=rn&id=42936&SEO=angolan-oil-company-suffers-attempted-cyber-attack (Acedido aos 08-05-2020).
https://www.policiajudiciaria.pt/acesso-ilegitimo-a-centrais-telefonicas-e-devassa-da-vida-privada-por-meios-informaticos-2/ (Acedido aos 6-12-2019).
https://www.portalgsti.com.br/2018/11/sniffing-de-rede.html (Acedido aos 16-04-2020).
https://www.publico.pt/1999/12/03/jornal/uma-agenda-europeia-para-a-sociedade-do-conhecimento-127314 (Acedido aos 04-11-2019).

https://www.refworld.org/docid/5a547d6e4.html (Acedido aos 13-01-2020).
https://www.reg.it.ao/support?who_is_regitao (Acedido aos 19-05-2020).
https://www.sentinelone.com (Acedido aos 15-01-2020).
https://www.sepe.gov.ao/ao/catalogo/eloja/dominios/registo-de-dominio-ao/ (Acedido aos 19-05-2020).
https://www.skillset.com/questions/how-is-sniffing-usually-categorized (Acedido aos 16-04-2020).
https://www.thestar.com.my/tech/tech-news/2016/03/31/anonymous-cyberattack-hits-angola-govt-after-activists-jailed/ (Acedido aos 14-01-2020).
https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing.htm (Acedido aos 15-04-2020).
https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing.htm (Acedido aos 15-04-2020).
https://www.uneca.org/publications/african-information-society-initiative-aisi-decade's-perspective (Acedido aos 12-11-2019).
https://www.unicef.pt/media/2766/unicef_convenc-a-o_dos_direitos_da_crianca.pdf (Acedido aos 19-01-2020).
https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Comments/Nigeria_2.pdf (Acedido aos 14-11-2019).
https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/computer-related-offences.html (Acedido aos 20-02-2020).
https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/content-related-offences.html (Acedido aos 12-01-2020).
https://www.unodc.org/res/cld/document/cybercrime-act_html/CYBERCRIMEACT-2015.pdf (Acedido aos 14-11-2019).
https://www.un-page.org/files/public/mauritius_jan-feb_2017_reprint_compr.pdf (Acedido aos 14-11-2019).

https://www.vda.pt/xms/files/v1/O_QUE_FAZEMOS/NEWSLETTERS_E_FLASHES/Flash_informativo_Lei_Protecao_das_Redes_e_Sistemas_Informatico__Angola__PT.pdf.PDF (Acedido aos 18-11-2019).
https://www.verbojuridico.net/doutrina/tecnologia/meiosprovacriminalidadeinformatica.pdf (Acedido aos 15-01-2020).
https://www.wipo.int/edocs/lexdocs/laws/en/mu/mu011en.pdf (Acedido aos 14-11-2019).
https://www.wipo.int/edocs/lexdocs/laws/en/mu/mu012en.pdf (Acedido 14-11-2019).

https://www.wipo.int/edocs/lexdocs/laws/en/mu/mu024en.pdf (Acedido14-11-2019).
https://www.wipo.int/edocs/lexdocs/laws/pt/ao/ao002pt.pdf (Acedido aos 21-01-2020).
https://www.wipo.int/edocs/lexdocs/laws/pt/ao/ao026pt.pdf (Acedido aos 06-10-2019).
https://www2.deloitte.com/content/dam/Deloitte/ao/Documents/tax/Tax%20News%20Flash/2018/NF_8_Decreto%20Executivo%2074_19_%20Aprova%20as%20regras%20e%20requisitos%20

para%20Validação%20de%20Sistemas%20de%20Processamento%20Electrónico%20de%20Facturação%20dos%20Contribuintes..pdf (Acedido aos 19-05-2020).
http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/737b074e63612dc880257de100582533?OpenDocument (Acedido aos 21-07-2020).
www.dgsi.pt (Acedido em 03-01-2020).
https://en.wikipedia.org/wiki/Hacker (Acedido aos 24-09-2020).
https://pt.wikipedia.org/wiki/Phishing (Acedido aos 24-09-2020).
https://pt.wikipedia.org/wiki/Pharming (Acedido aos 24-09-2020).
https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf (Acedido aos 19-07-2019).
https://www.portaldeangola.com/2013/05/21/angola-tem-actualmente-cinco-milhoes-de-usuarios-de-internet/ (Acedido aos 19-07-2019).