UNIVERSIDADE DE LISBOA

FACULDADE DE DIREITO

APROPRIAÇÃO INDEVIDA DE IDENTIDADE: ENQUADRAMENTO JURIDICO-PENAL

EVA DA SILVA RODRIGUES PINTO DOS REIS

DISSERTAÇÃO DE MESTRADO EM DIREITO E PRÁTICA JURIDICA

ESPECIALIDADE: DIREITO PENAL

ORIENTADORA: PROFESSORA DOUTORA TERESA QUINTELA DE BRITO

COORIENTADOR: MESTRE DAVID SILVA RAMALHO

2019

À minha mãe e ao meu avô.

"Where there is great power there is great responsibility"

Winston Churchill - Câmara dos Comuns, 28 de Fevereiro de 1906

""Vem por aqui" --- dizem-me alguns com olhos doces,
Estendendo-me os braços, e seguros
De que seria bom se eu os ouvisse
Quando me dizem: "vem por aqui"!
Eu olho-os com olhos lassos,
(Há, nos meus olhos, ironias e cansaços)
E cruzo os braços,
E nunca vou por ali..."

José Régio - Cântico Negro. In **Poemas de Deus e do Diabo, 1926**

"Come chocolates!
Olha que não há mais metafísica no mundo senão chocolates.
Olha que as religiões todas não ensinam mais que a confeitaria."

Alváro de Campos – **Tabacaria**, 15 de Janeiro de 1928

Resumo

O fenómeno sobre o qual vamos refletir nesta dissertação tem sofrido mudanças visíveis ao longo do tempo, resultado dos avanços tecnológicos que têm surgido e do lugar, crescentemente importante, que têm tomado no nosso quotidiano. O mundo digital trouxe consigo facilidades inegáveis na maneira como agimos e nos movimentamos na sociedade, dando origem a vantagens e desvantagens, muitas ainda por explorar. Como resposta a esta mudança, o legislador criou a Lei do Cibercrime que deve funcionar, lado a lado com o Código Penal, como barreira inultrapassável frente às atuações possibilitadas pelas novas tecnologias.

A forma de ver o direito e os conceitos jurídicos que o compõe, teve e terá de ser, continuamente, alterada e adaptada em função deste novo mundo: diferente, não só pelo que a tecnologia possibilita, mas pela mudança que isso gera na mente e comportamento humanos. Desta adaptação terão de resultar novas proteções, para fenómenos que antes pareciam desnecessariamente carenciados de tutela penal; e proteções acrescidas ou diferentes para fenómenos já tutelados. Certos conceitos terão de ser repensados, à medida que se apresentam transmutados perante a sociedade. Um deles será, sem dúvida, a identidade. Cabe-nos tentar perceber se o conceito de identidade mudou e se isso deve forçar um tratamento diferente desta, por parte do direito penal.

Por fim, havendo necessidade de encarar a identidade moderna distintamente e reconhecendo novas formas de ataque contra esta, é nossa obrigação encontrar novas e melhoradas linhas de proteção. É urgente perceber as desvantagens trazidas pela sociedade de informação e reagir apropriada e atempadamente. Desvantagens que se tornaram em vantagens e ferramentas poderosas para todos aqueles que cometem crimes. Este é só um dos muitos exemplos que se potenciaram, em quantidade e danosidade, aliando a tecnologia ao crime, mas é também, parece-nos, um dos pilares fundamentais desta discussão e, afinal, "da discussão nasce a luz".

Palavras – chave

Apropriação indevida de identidade; Cibercrime; Dados; Identidade; *Phishing*

Abstract

Technological improvements, as well as the consequent changes they bring to everyday life and their growing importance in our lives, have had a constant impact on the object of the present dissertation. The digital world provided undisputable facilities over our actions and movements, creating advantages and disadvantages that have yet to be explored. To answer to these changes, the legislator has created the Cybercrime Law, whose purpose, supported by the Penal Code, is to create an insurmountable barrier to the actions made possible by the new technologies.

The way in which Law and its legal concepts are perceived has been constantly changing and adapting in accordance with this new world: different due to the technology it provides, but also because of the changes it enforces on human mind and behavior. This will continue to be so in the future. This adaptation must result in groundbreaking protection against phenomena that previously appeared to need no legal involvement, and in additional and specific protection against already legislated phenomena. Certain concepts will need rethinking as they surface transmuted. Identity will, most certainly, be one of these. We must try to understand if the concept of identity as already changed; and if so, should this change enforce a different treatment in Criminal Law.

At last, provided we need to view modern identity distinctively, and to acknowledge the new threats it faces, it is our duty to find new and better lines of protection. Its urgent to understand the disadvantages that arise from the information society, and to react accordingly in good time. These disadvantages have become advantages and powerful tools for those who commit crimes. This is merely one perspective regarding the rise in quality and damage potentiated by the alliance between technology and crime. Nevertheless, in our opinion, it is the crucial pillar that supports this discussion - and enlightenment arises from it.

Keywords

Cybercrime; Data; Identity; Identity Theft; Phishing

Siglas e Abreviaturas

Ac. – Acórdão

al. – Alínea

Art. – Artigo

B.I – Bilhete de identidade

CC – Código Civil

CCiber. – Convenção sobre o Cibercrime

Cfr. – Confira-se

Coord. – Coordenação

CP – Código Penal

CRP– Constituição da República Portuguesa

Dir. – Direção

i.e. – Isto é

L – Lei

LC – Lei do Cibercrime

LCI –Lei da Criminalidade Informática

Nº– Número

Ob. cit. – Obra citada

PGR – Procuradoria Geral da República

p. – Página

pp. – Páginas

Rel. – Relator

RGPD – Regulamento Geral sobre a Proteção de Dados

STJ – Supremo Tribunal de Justiça

STS – Sentencia Tribunal Supremo

TC – Tribunal Constitucional

TRE – Tribunal da Relação de Évora

TRG – Tribunal da Relação de Guimarães

TRL – Tribunal da Relação de Lisboa

TRP – Tribunal da Relação do Porto

Vol. – Volume

Vols. – Volumes

Índice

Introdução 8

Capítulo I –A apropriação indevida de identidade: delimitação de conceitos 10

1. A tutela da identidade pessoal no direito português 10
2. O conceito de ciberidentidade 12
3. A apropriação indevida de identidade 15

Capítulo II – A apropriação indevida de identidade 19

1. A apropriação indevida de identidade como ato motivador à prática de outros ilícitos 19
2. A criminalização da apropriação indevida de identidade noutros ordenamentos jurídicos 30
3. A insuficiência do quadro legal vigente em Portugal para criminalizar todo o fenómeno..……...……..…37

Capítulo III – A existência de margem constitucional para criminalização 40

1. A especial necessidade de intervenção do direito penal no contexto digital 40
2. A existência de bem jurídico dotado de dignidade penal 44
3. A carência de tutela penal 47

Capítulo IV – A eventual criminalização da apropriação indevida de identidade 51

1. O tipo objetivo 51
2. Eventuais agravações 55
3. O tipo subjetivo 57
4. O grau de lesão do bem jurídico exigido 58

Conclusão 61

Referências Bibliográficas 63

Referências Jurisprudenciais 68

ANEXOS 70

Anexo I – A evolução do "roubo de identidade" 70

Anexo II - Identity Theft and Assumption Deterrence Act (EUA) 71

Anexo III - UNITED STATES CODE, Title 18 (Crimes and Criminal Procedure) – Chapter 47 (Fraud and False Statements) 76

Anexo IV – Código Criminal (Alemanha) 83

ANEXO V - Código Penal (Espanha) 85

Anexo VI – Código Penal Para el Distrito Federal (México) 89

Introdução

Lá onde a identidade individual se apaga, não há nem punição nem recompensa.

Ernst Jünger

A palavra identidade significa, etimologicamente, "o mesmo" ou "a mesma coisa"[1]. O que é igual a dizer que a identidade de cada um corresponde – é o mesmo – a tudo aquilo que nós somos, expressa ou tacitamente. Releva, para este estudo, aquela que é a nossa identidade "expressa", isto é, tudo aquilo que nos identifica, como sendo nós, perante a sociedade (o nosso nome, data de nascimento, nome dos nossos pais, NIF, entre outros). Afinal, só esta é que pode ser apropriada.

Quando falamos em apropriação indevida de identidade (vulgo, roubo ou furto de identidade), referimo-nos ao uso indevido desta por outrem. Este fenómeno criminoso existe desde sempre, apesar de só recentemente ter vindo a ser reconhecido como suscetível de merecer autonomia própria. O crescimento deste fenómeno foi, nos últimos anos, exponencial, por uma única razão: o surgimento da internet. A internet, como veículo supremo de informação, potenciou a facilidade de acesso à identidade. A informatização crescente da informação torna o quotidiano mais simples e prático, mas torna também a prática de condutas associadas à apropriação indevida de identidade mais fácil, o que levanta a questão: estamos a reagir tão rápido como estamos a agir? É preciso perceber, como sociedade e como juristas se estamos a conseguir acompanhar os avanços tecnológicos a que temos assistido recentemente.

Esta dissertação tem como objetivo explorar os perigos inerentes aos avanços tecnológicos, especificamente no que toca à apropriação indevida de identidade e compreender se o direito e a legislação estão a conseguir dar resposta às novas formas de perpetração deste crime. Para tal, vamos começar por caracterizar o cibercrime, que trata deste problema e que se tem tornado, cada vez mais – e cada vez mais se vai tornar -, uma área do direito a ter em atenção e estudar em profundidade, pelo facto de o crime, em todas as suas vertentes, se estar a tornar fortemente informatizado. A evolução da apropriação indevida de identidade é consequência direta da proliferação do cibercrime. Depois deste importante enquadramento entramos na análise do fenómeno criminoso que constitui o

[1] Do latim *identitas.*

objeto do nosso estudo, para perceber o que é, como pode ser cometido e explicar o porquê da sua importância. Para que possamos chegar a conclusões e sugerir (possíveis) soluções, iremos considerar o quadro legal e a jurisprudência portugueses e estrangeiros.

Atualmente, este comportamento não é reconhecido como crime autónomo na nossa legislação, avaliaremos ao longo desta exposição se se justifica uma incriminação, tentando perceber se a lei atual é (in)suficiente. Os nossos tribunais, no entanto, referem várias vezes esta figura, chegando à decisão final através de outros tipos de crime que consideram abranger este fenómeno. O que esperamos conseguir, no final desta jornada, é sobretudo perceber: a) se certas atuações típicas associadas a este fenómeno estão inclusas em tipos legais já existentes b) se este crime devia ter uma consagração legal autónoma; e c) se, independentemente disso, os nossos tribunais têm conseguido justiça para as vítimas, isto é, se a realização do direito, ainda que com uma lei porventura insuficiente, tem sido conseguida.

Capítulo I –A apropriação indevida de identidade: delimitação de conceitos

1. A tutela da identidade pessoal no direito português

Tal como dissemos na Introdução a identidade de cada um corresponde a tudo aquilo que nós somos. É o conjunto de características individuais e pessoais, que faz de cada um de nós um ser diferente e único. "é aquilo que caracteriza cada pessoa enquanto unidade individualizada que se diferencia de todas as outras pessoas por uma determinada vivência pessoal" e "abrange o direito de cada pessoa a viver em concordância consigo própria, sendo, em última análise, expressão da liberdade de consciência projetada exteriormente em determinadas opções de vida"[2]. Uma boa maneira de definirmos as várias faces da nossa identidade seria, por exemplo, consultar o art.13º, nº2 da CRP:

Artigo 13.º

(Princípio da igualdade)

1. Ninguém pode ser privilegiado, beneficiado, prejudicado, privado de qualquer direito ou isento de qualquer dever em razão de ascendência, sexo, raça, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual.

A nossa identidade é muito mais que isto, mas, para o direito, esta seria uma boa resposta à pergunta: o que é que constitui a nossa identidade? Para a Constituição estes são os elementos fundamentais[3].

A Constituição da República Portuguesa, consagra, no seu artigo 26º, o direito à identidade pessoal, determinando ainda, no nº2, que "a lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias". Torna-se claro que o direito à cidadania e identidade são direitos fundamentais e não, só, qualidades jurídicas. Este artigo reflete, desde logo, a ideia basilar de qualquer Estado de Direito: a dignidade humana (art.1º CRP). A identidade – bem como os restantes direitos elencados no art.26º CRP - é a concretização da dignidade humana. Este princípio é dirigido a pessoas concretas e reais, homens e mulheres, cuja identidade os define – "a dignidade da pessoa é dignidade da pessoa concreta, na sua vida

[2] MIRANDA, Jorge/ MEDEIROS, Rui – **Constituição Portuguesa Anotada,** p. 609.

[3] "O direito à identidade pessoal liga-se, ainda, à proibição da discriminação do artigo 13º, nº2, da Constituição, pois as características aí identificadas são, na sua generalidade, constitutivas da identidade pessoal" - MIRANDA/ MEDEIROS – Ob. cit., p. 609.

real e quotidiana; não é de um ser ideal e abstrato. É o homem ou a mulher, tal como existe, que a ordem jurídica considera irredutível, insubstituível e irrepetível e cujos direitos fundamentais a Constituição enuncia e protege[4]". A identidade, enquanto conjunto de características que caracterizam uma pessoa e não enquanto ideia ou princípio abstrato, é, portanto, uma das manifestações, senão a mais importante, do princípio da dignidade humana. Assim o confirma o art.19º, nº6 da CRP ao proibir a afetação deste direito, mesmo em caso de declaração de estado de sítio ou estado de emergência.; e o art.20º, nº5 CRP, ao conferir uma tutela processual superior aos *direitos, liberdades e garantias pessoais*, nos quais se inclui este. Este direito desdobra-se em várias componentes: a identidade genética própria; o direito fundamental ao conhecimento e reconhecimento da paternidade e maternidade; o direito ao conhecimento das origens genéticas; a identidade civil, onde se inclui o direito ao nome, elemento primordial de identificação e "parte essencial da identidade pessoal"[5]. Consideramos, ainda, que o direito à autodeterminação informacional[6] se classifica como um direito emergente do direito de identidade, sendo este um dos direitos de personalidade não expressamente tipificado no art.26º da CRP[7], mas que já encontra consagração, no que toca a dados informáticos, no art.35º da CRP. Este direito traduz-se no poder de controlar as informações que nos dizem respeito, o que significa ter controlo sobre a nossa identidade. Afinal a nossa informação, os nossos dados pessoais, são a nossa identidade exteriorizada, são aquilo que a sociedade vê e assimila como sendo a nossa identidade. Num mundo em que a informação se torna cada vez mais acessível e incontrolável, maior é a necessidade deste direito se afirmar.

Esclarece a Lei nº 33/99, de 18 de maio – que regula a identificação civil e emissão do BI -, na sua versão mais recente de 2017, que são elementos identificadores de qualquer pessoa: o seu nome completo; filiação; naturalidade; data de nascimento; sexo; residência; fotografia e assinatura (art.5º - elementos identificadores). Define também, no seu art.26º (acesso direto à informação civil) que "as entidades autorizadas a aceder diretamente à base

[4] MIRANDA/ MEDEIROS – Ob. cit. p.81.
[5] Assim, MIRANDA/ MEDEIROS – Ob. cit., pp. 609 a 611 e ALVES, Jones Figueirêdo – **Identidade pessoal na sociedade de informação: dimensões de autodeterminação e ilicitude civil**, p. 37.
[6] Este direito começou a ganhar expressão em 1983, tendo uma importância crescente à medida que as novas tecnologias, também elas, evoluíam – "Neste cadinho difunde-se a autodeterminação informacional – *informationelle Selbstbestimmung* – de origem germânica, proveniente da Decisão dos Censos de Dezembro de 1983 do Tribunal Constitucional Federal Alemão. Aí se afirmou que o titular dos dados pessoais tinha o direito de conhecer e consentir na recolha, armazenamento, uso e transmissão de informação pessoal, salvo quando a lei funcionasse como condição de legitimidade" – SOUSA PINHEIRO, José Alexandre Guimarães de - **Privacy e protecção de dados pessoais : a construção dogmática do direito à identidade informacional**, p. 964.
[7] "E não admira, também, que possam reconhecer-se direitos de personalidade não tipificados na Constituição como será o caso do direito ao nome, do direito à autodeterminação informacional ou do direito à ressocialização" - MIRANDA/ MEDEIROS – Ob. cit., pg. 608.

de dados adotarão as medidas administrativas técnicas necessárias a garantir que a informação não possa ser obtida indevidamente nem usada para fim diferente do permitido", concretizando o art.26º, nº2 da CRP. O RGPD, reportando-se ao conceito de dados pessoais, indica serem elementos identificadores, por exemplo "um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular" (art.4º - Definições).

A identidade é, portanto, expressamente reconhecida como um direito fundamental, sendo, consequentemente, garantida a sua tutela, em vários outros diplomas. Levanta-se então a questão de saber se este direito está suficientemente protegido, em todas as suas vertentes, no nosso ordenamento jurídico.

2. O conceito de ciberidentidade

"We do not merely move through life's stages, as Jacques's monologue suggests, but leave a multitude of data traces as we go. In an era of social media, these data traces do not merely document our passage in life's play but mediate our parts."

Hogan, 2010[8]

Apesar de não haver menção expressa na CRP, consideramos que o conceito de identidade, tal como configurado no ponto anterior, enquanto direito fundamental, também engloba a nossa "ciberidentidade"[9]. Faremos, no entanto, uma distinção teórica, dentro do conceito de ciberidentidade, entre aquela que é a nossa identidade "ciberformal", mais uma vez aquela que nos *carimba* como membros da sociedade, e a nossa identidade "cibersocial". A nossa identidade "ciberformal" é constituída por todos os elementos identificadores que sempre existiram e foram progressivamente informatizados, i.e., todos os dados que referimos *supra* e que constam da Lei nº 39/99, por exemplo; a nossa identidade "cibersocial" passa por todas as informações que disponibilizamos na internet, seja nas redes sociais; seja em inquéritos on-line; seja no nosso email pessoal ou de trabalho. Enquanto que a identidade "ciberformal", apresentando-se como a nossa identidade no mundo material, mas

[8] HOGAN, Bernie - The presentation of self in the age of social media: distinguishing performances and exhibitions online, p. 377.

[9] "Assim, o direito à identidade informacional tem integração constitucional por via não só do art.35º, mas especialmente do art.26º da CRP. O conjunto de posições jurídicas abrangidas inclui os aspectos próprios da proteção de dados pessoais mas excede-os, aproximando-se dos direitos à identidade pessoal e ao livre desenvolvimento da personalidade." - SOUSA PINHEIRO, José Alexandre Guimarães de – Ob. cit. p. 959.

"transferida" para o mundo digital, está claramente protegida pela CRP e por leis como a nº 39/99, afinal trata-se dos mesmos dados, num suporte digital, i.e., não é um novo conceito de identidade, mas simplesmente uma forma de suporte nova; já a nova identidade "cibersocial" pode parecer uma zona cinzenta, de liberdade. Há então que perceber em que consiste exatamente este novo conceito de ciberidentidade e o que contém, para sabermos se o tratamento deve ser o mesmo, havendo uma igual proteção jurídica.

SHERRY TURTLE[10], fala-nos de três características essenciais da ciberidentidade: multiplicidade, invisibilidade e anonimato. A multiplicidade corresponde à possibilidade de criação, por cada utilizador, de várias *personas online*, ou seja, no mundo digital, contrariamente ao mundo físico, é possível adotar uma multiplicidade de identidades. A invisibilidade, no seguimento da multiplicidade, consiste em poder ocultar ou acrescentar certas características que não correspondem à nossa identidade real. O anonimato, tal como o nome indica, é a faculdade de o utilizador não se identificar[11] e "navegar" *online* sem ter de mostrar a sua identidade.

Ora, estas características são as opostas da nossa identidade, tal como configurada no capítulo anterior. Apesar de reconhecermos a importância desta visão da ciberidentidade, não nos parece que esta possa ser reconhecida e protegida, como tal, pelo Direito Penal e Constitucional. A multiplicidade, invisibilidade e anonimato são características do modo como nos apresentamos na internet, motivadas pelo funcionamento dos sistemas informáticos, contudo isso não basta para dizer que formam a nossa ciberidentidade, num sentido jurídico. Muito menos nos parece, na senda do que nos diz CARNEIRO DA SILVA, que esta possa ser considerada para efeitos da apropriação, pois "a ciberidentidade enquanto bem jurídico eminentemente pessoal suscetível de usurpação, tem necessariamente que refletir a identidade de uma pessoa humana a ponto de ser possível identificá-la"[12].

O artigo 35º da CRP reforça a ideia de que a identidade informática faz parte da nossa identidade, ao dispor que qualquer um pode exigir a retificação e atualização dos "dados informáticos que lhe digam respeito". Porque, claro, se é a nossa identidade, deve ser por nós controlada. Mostra-nos, ainda, que a identidade relevante é constituída pelos nossos dados pessoais, aqueles que nos dizem respeito. Mais uma vez se demonstra que o legislador

[10] *Apud*, CARNEIRO DA SILVA, Flávio Manuel - **A Usurpação da Ciberidentidade**, p.14.
[11] O direito ao anonimato já foi reconhecido como inalienável, enquanto manifestação do direito à reserva da intimidade da vida privada –consagrado na Declaração Universal dos Direitos do Homem – art.12.º -, na Convenção Europeia dos Direitos do Homem – art.8.º -, e no Pacto Internacional dos Direitos Civis e Políticos – art.17.º.
[12] Ob. cit., p. 16.

configura, facilmente, a nossa ciberidentidade "formal", i.e., os nossos dados pessoais informáticos, como parte da nossa identidade e, portanto, merecedora da mesma tutela. Neste sentido, veja-se também a definição de dados pessoais no art.º 4º, nº1 do RGPD: "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente". Entendeu-se aqui que os dados a proteger só poderiam ser aqueles relativos a "pessoa singular identificada e identificável". Mais se diz, que "a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8º, nº 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16º, nº 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.".

Por isso, concordamos com CARNEIRO DA SILVA(Silva, 2014) – não só por uma questão de merecimento de tutela, como por uma questão de interpretação sistemática - a "ciberidentidade" é tudo aquilo que corresponde "à identidade real da própria pessoa", razão pela qual acreditamos que o conceito de identidade da CRP deve abranger também a ciberidentidade (na sua forma "ciberformal"), como qualquer manifestação identificável e reconduzível a certa pessoa[13]. De frisar, que esta afirmação se aplica a todas as vertentes da nossa identidade, tal como referidas no capítulo anterior - identidade genética própria; direito fundamental ao conhecimento e reconhecimento da paternidade e maternidade; direito ao conhecimento das origens genéticas; identidade civil e autodeterminação informacional. Contudo, não nos parece que a proteção se baste com a "identidade real". Sem dúvida que esta deve ser protegida, exatamente da mesma forma que a identidade configurada na CRP, tratando-se dos mesmos dados, mas num suporte diferente. Isto não significa, que só os dados existentes antes do aparecimento da informática mereçam a mesma tutela. Na realidade existem imensos dados "puramente" informáticos que também podem ser reconduzíveis a uma pessoa identificada ou identificável: o *email* pessoal; a conta no eBay; o perfil no Facebook, Instagram, Twiter; os dados de acesso à página de *homebanking*, entre tantos outros. Todos estes dados, apesar de não existirem antes, tonaram-se parte do nosso dia-a-dia e da nossa identidade e a sua apropriação indevida é tão, ou mais ofensiva, do que o nosso número de segurança social ou a nossa carta de condução. Estes dados preenchem um conceito de ciberidentidade jurídico, são dados que correspondem a uma pessoa real e

[13] O mesmo nos diz ALVES: "entende-se por identidade digital aquela que apresenta a pessoa na sociedade informacional, por meio de fotos, imagens, dados, arquivos e perfis que a identificam individualmente, dentro do ambiente virtual, mediante o uso de modernas tecnologias da informação" – Ob. cit. pg. 64.

cuja usurpação pode causar danos sérios e reais, são uma extensão digital da nossa identidade real, razão pela qual devem ser tratados da mesma forma e ter a mesma proteção constitucional que tem a identidade.

Tendo por base este conceito de identidade, onde se inclui a faceta da ciberidentidade acima apontada, enquanto direito fundamental protegido pela CRP, no seu art.26º, nº1, temos o ponto de partida que circunscreve os casos sobre os quais incide o fenómeno que trataremos ao longo deste trabalho.

3. A apropriação indevida de identidade

Apropriação indevida de identidade foi o termo, por nós escolhido, para designar o uso de dados pessoais de outrem, com a intenção de assumir a sua identidade, perante terceiros. Existem, no entanto, vários termos para designar esta realidade, adotados por diferentes sectores da doutrina ou pelo legislador de outros ordenamentos jurídicos.

Nos EUA e no Reino Unido, a doutrina[14] e a lei[15] usam o termo *identity theft* e *identity fraud*, o que significa, numa tradução literal, roubo de identidade e fraude de identidade, respetivamente. A distinção entre os dois fenómenos, passa por se tratar simplesmente de um "roubo" de dados (*identity theft*), ou, por já constituir, numa fase seguinte, o uso desses dados para benefício próprio ou de terceiros (*identity fraud*). Esta configuração da fraude, equivale ao crime de burla no nosso ordenamento jurídico. A Burla, nas suas várias configurações, tem sempre como elemento típico a intenção de receber algum tipo de benefício[16]: *art.217º - Burla, 1. Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo; art.220º - Burla para obtenção de alimentos, bebidas ou serviços, 1. Quem, com intenção de não pagar.* A distinção parece-nos útil, no sentido em que, são de facto duas partes ou fases de um mesmo comportamento. Para se assumir a identidade de outrem, é preciso primeiro, obter os seus dados, o que, em si, já constitui um crime. Contudo, esta terminologia não se

[14] Assim, WHITE, Michael D. / FISHER, Christopher - Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Effort; WANG, Wenjie/ YUAN, Yufei/ ARCHER, Norm - A Contextual Framework for Combating Identity Theft; LYNCH, Jennifer - Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks; WALL, David S./ Williams, Mathew L. – **Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing.**

[15] Veja-se o "*Identity Theft and Assumption Deterrence Act*" ou o Capítulo 47 (Título 18), do Código dos EUA – Anexo II e III.

[16] "O crime de burla desenha-se como a forma evoluída de captação do alheio em que o agente se serve do erro e do engano para que incauteladamente a vítima se deixe espoliar, e é integrado pelos seguintes elementos:- intenção do agente de obter para si ou para terceiro enriquecimento ilegítimo;" – Ac. do STJ de 20 de Março de 2003, Proc. 03P241, Rel. Simas Santos.

afigura a mais correta, na nossa opinião. Para perceber porquê atentemos a alguns tipos legais, do nosso Código Penal.

Tanto o furto como o roubo consubstanciam uma conduta de subtração de coisa móvel (ou animal), tal como definida no artigo 202º e 205º do CC, sendo que, de acordo com este último, são consideradas coisas móveis todas as coisas não imóveis, todas elas suscetíveis de subtração. Esta subtração tem de ser feita com intenção de ficar com a coisa, i.e., mantê-la na sua esfera jurídica ou de terceiro (*intenção de apropriação*), sem, para tanto, ter legitimidade. Ambos os crimes, se encontram no Capítulo II – Dos crimes contra a propriedade, inserido no Título II – Dos crimes contra o Património. Património esse que é definido por FARIA COSTA como "o complexo de relações jurídicas encabeçadas por um sujeito que tem por objeto último coisa dotadas de utilidade, isto é, de capacidade de satisfazer necessidades humanas, materiais ou espirituais"[17]. Ao analisar o crime, especificamente, considera-se, que, aquando da consumação do furto/roubo, existe uma transferência de utilidades que, sendo não consentida, é ilegítima. Esta coisa (ou animal) – que representa a utilidade transferida – é merecedora de tutela jurídico-penal pela "especial relação que intercede entre o detentor da coisa e a própria coisa"[18].

No que toca ao tipo subjetivo, o elemento essencial é a *ilegítima intenção de subtração*. Nesta linha, FARIA COSTA esclarece que "o furto é um "delito intencional" (ou *essencialmente doloso*"[19], o que se confirma pelo facto de não haver forma negligente do ilícito. Isto significa também que "desde que o *ladrão* consegue o chamado *domínio sobre a coisa*, completando a *subtração*[20] e consumando o *furto*, nada mais tem de fazer para daquela coisa de apropriar"[21]. O elemento subtração, por seu turno, consubstancia a "violação da posse exercida pelo lesado e a integração da coisa na esfera patrimonial do agente ou de terceira pessoa"[22]. A subtração constitui, portanto, condição *sine qua non* destes dois crimes.

No que toca à diferença entre furto e roubo diz-nos EDUARDO CORREIA que a distinção se faz pela "exigência da violência e da ameaça com perigo iminente para a

[17] *Apud* PEREIRA, Victor de Sá/ LAFAYETTE, Alexandre - **Código penal anotado e comentado, Legislação conexa e complementar**, p. 574.
[18] PEREIRA/ LAFAYETTE – Ob. cit., p. 574.
[19] *Apud* PEREIRA/ LAFAYETTE – Ob. cit., p. 575.
[20] Subtração, essa, que tem de ser de coisa alheia, definida por PAULO SARAGOÇA DA MATA como "toda a coisa que esteja ligada, por uma relação de interesse, a uma pessoa diferente daquela que praticou a infração" - *Apud* PEREIRA/ LAFAYETTE – Ob. cit., p.578.
[21] PEREIRA/ LAFAYETTE – Ob. cit., p. 575.
[22] PEREIRA/ LAFAYETTE – Ob. cit., p. 580.

integridade física e para a vida"[23] – no caso do roubo. O roubo, enquanto crime, produz, portanto, danos ao nível da propriedade e de bens pessoais, como sejam, a liberdade (*constranger a; ou pondo-a na impossibilidade de resistir)*, a integridade física e a vida (*ameaça com perigo iminente para a vida ou para a integridade física)*. Esta ameaça tem de recair sobre o titular da coisa a subtrair, ainda que diretamente dirigida a terceiro, criando, para aquele outro, alguma forma de constrangimento[24].

A apropriação ilegítima em caso de acessão ou de coisa ou animal achados, prevista no art.209º do CP, pese embora seja, também, crime contra a propriedade, apresenta algumas diferenças. Aqui, a coisa é apropriada, não existindo subtração (caso do furto e roubo) ou entrega (caso do roubo). A coisa já se encontra na esfera de outrem seja por *efeito de força natural, erro, caso fortuito, ou por qualquer outra maneira independente da sua vontade,* ou ainda, por ter sido encontrada (nº2). É, portanto, um caso de "*finders, keepers*". Este crime será relevante para os casos em que o documento de identificação é encontrado e não deliberadamente retirado do seu titular. FARIA COSTA esclarece que "as coisas sem dono não constituem objeto possível do crime em análise"[25]. Este nunca será o caso na apropriação indevida de identidade, pois que a identidade, seja em que elemento for, nunca será *res nullius*.

Este esclarecimento do que seja furto, roubo e apropriação ilegítima tem como intenção dar a perceber que o termo "roubo de identidade" não é tecnicamente correto, porquanto a identidade é uma realidade complexa que não pode ser simplesmente subtraída de outrem, através do uso da violência. Alias a identidade, sendo por natureza informação, não pode ser considerada uma coisa móvel, não é algo que se entrega, ou uma coisa corpórea suscetível de ser subtraída (i.e. furtada ou roubada). O furto ou roubo pode ser, no entanto, a fase inicial do processo criminoso que é a apropriação indevida de identidade, no sentido em que os documentos que formalizam a nossa identidade, dentro de uma sociedade, são coisas móveis. Como se verá adiante, em maior pormenor, a apropriação passa, inicialmente, pela obtenção de dados alheios, o que pode significar, ou não, o furto, roubo ou apropriação ilegítima, de um documento de identidade ou com conteúdos de identificação – um cartão de cidadão, um passaporte, um cartão de débito ou crédito.

As Leis Mexicana e Espanhola, por seu turno, falam de "*usurpación de identidad*"[26] , ou seja, de usurpação de identidade, referindo-se unitariamente à realidade de alguém se apresentar

[23] *Apud* PEREIRA/ LAFAYETTE – Ob. cit., p. 605.
[24] PEREIRA/ LAFAYETTE – Ob. cit., pp. 605 e 606.
[25] *Apud* PEREIRA/ LAFAYETTE – Ob. cit., p. 603.
[26] *Vide* Anexos V e VI.

com uma identidade alheia, não havendo distinção entre a fase de obtenção de dados e a fase de apropriação. O termo usurpação é usado para assinalar a não concordância com o termo menos correto roubo de identidade, pois a identidade não pode ser roubada, meramente usada[27].

Também na nossa doutrina, há já quem use esta expressão. CARNEIRO DA SILVA (2014), na sua dissertação, explica que o termo usurpação "oferece maior rigor jurídico", por 3 razões: primeiro, referindo-se a um argumento histórico, a Lei nº 12/91, de 21 de Maio (Lei da Identificação Civil e Criminal) – revogada pela Lei 33/99, de 18 de Maio – tinha como epigrafe do seu artigo 38º "Usurpação de Identidade"[28]; segundo, à semelhança do nosso argumento ao por de parte o uso dos termos roubo e furto, a apropriação da identidade por outrem não pode pressupor uma subtração, por não se tratar de uma coisa móvel; terceiro, porque a doutrina tem entendido que a usurpação é "a apresentação como próprio do que é alheio" – citando Oliveira Ascensão.

Concordamos com o autor, razão pela qual achamos que, também esta designação, é correta. Numa perspetiva semântica, tanto a palavra apropriação como usurpação significam tomar para si ou tornar seu; numa perspetiva jurídica, ambas as palavras são também usadas com este sentido, não parecendo haver distinção (veja-se o exemplo da *usurpação de título, uniforme ou insígnia de empregado público, civil ou militar*, do art.º204º/1/g) do CP; da *apropriação ilegítima em caso de acessão ou de coisa achada*, do já referido art.º209º do CP; e da *usurpação de coisa imóvel*, do art.º 215º do CP). Esta apropriação ou usurpação será sempre indevida, por ser feita sem consentimento do titular dos dados. A falta de consentimento, a existir um tipo legal no nosso ordenamento, é elemento essencial do tipo e enforma a ideia de que este é um crime que atinge o titular de dados pessoal e diretamente.

[27]"*El término robo de identidad, enrealidad, no es del todo correcto; de hecho, no es posible robar literalmente una identidad como tal, sino que sólo se puede usar.*" – ÁLVAREZ, Rogelio Barba -El robo de identidad en México, pp. 250 e 251.
[28] "Quem induzir alguém em erro, atribuindo, falsamente, a si ou a terceiro, nome, estado ou qualidade que por lei produza efeitos jurídicos, para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem será punido com prisão até 2 anos ou multa até 100 dias, se o facto não constituir crime mais grave" –art. 38º da Lei 33/99, de 18 de Maio.

Capítulo II – A apropriação indevida de identidade

1. A apropriação indevida de identidade como ato motivador à prática de outros ilícitos

Tal como mencionado, no início desta exposição, no nosso ordenamento jurídico não existe uma criminalização autónoma da apropriação indevida de identidade. No entanto, certos crimes conexos já existem na nossa lei e, a existir uma eventual criminalização, poderiam entrar em conflito (seja em relações de concurso, subsidiariedade ou outras) com a apropriação indevida de identidade. É muito importante, por isso, conhecer todos os crimes associados a este fenómeno e motivados por ele. Só assim poderemos realmente delimitar o seu escopo e consequente forma adequada de tutela exigida.

Existem duas fases essenciais que levam à apropriação indevida de identidade: a obtenção de dados (equivalente ao *identity theft*) e o uso desses dados (*identity fraud*). Importa esclarecer, desde já, que nem todas estas fases configuram, ainda, o fenómeno criminoso em estudo. A obtenção e uso de dados são, ou podem ser, os crimes meio para o crime fim. Como veremos, muitos destes exemplos, já se encontram protegidos pela nossa lei. A apropriação indevida de identidade exige a aparência, perante outros, de que aquela pessoa é o titular legitimo dos dados, pelo que só existirá quando tal aconteça – a avaliação tem de ser casuística e centrada neste critério. Existem, no entanto, uma série de atuações criminosas que gravitam em torno da apropriação indevida e que possibilitam e interagem entre si, antes, durante e após a sua consumação. Comecemos por ver de que maneira podem ser obtidos os dados, passando para as formas de uso de dados e respetivos enquadramentos legais.

Trashing/ Dumpster Diving

Esta é a mais antiga forma de obter os dados pessoais de alguém e é também, neste momento, a menos usada. O *trashing* ou *dumpster diving* é uma forma "física" de obtenção de dados e passa pelo roubo, furto ou apropriação ilegítima de documentos de identificação. Ambas as designações estão relacionadas com lixo/caixotes do lixo (*trash* e *dumpster)*, exatamente porque, muitas vezes, estes documentos eram encontrados em caixotes do lixo ou caídos pela rua[29]. É isto que motiva, hoje em dia, muitas entidades governamentais a

[29] *"Trashing or 'dumpster diving' has long been the most conventional way that fraudsters have obtained personal information. They would obtain discarded documents from trash cans, or steal personal documents from their owner (during burglaries for example)"* - WALL, David S./ Williams, Mathew L. – Ob. cit., p. 6.

aconselhar sempre a destruição de todo e qualquer documento com informações pessoais[30]. Este é, portanto, o único caso em que faz sentido e é tecnicamente correto falar de furto, roubo ou apropriação ilegítima, por estar em causa um bem móvel, um documento de identificação "físico", que é obtido através do contacto direto com o seu titular (exemplo do furto ou roubo de uma carteira ou mala) ou, no exemplo clássico de "*finders, keepers*", encontrando os documentos na rua. Com o surgimento da *Internet*, este método perdeu expressão, dando lugar aos métodos digitais, sendo que, atualmente, a apropriação indevida de identidade é feita quase inteiramente no ambiente digital. As formas de obtenção de dados são cada vez mais variadas e acarretam um risco muito baixo para alguém que comete o crime à distância e de uma forma praticamente indetetável.

Tal como indicado, este método de obtenção de dados traduz-se juridicamente, num crime de furto (art.203º do CP), roubo (art.210º do CP) ou apropriação ilegítima em caso de acessão ou de coisa achada (art.209º do CP), dependendo da forma que é usada para obter o documento de identificação.

Phishing

A forma digital mais usual, hoje, é o chamado *phishing*[31], técnica que emerge em 1996, lado a lado com o *homebanking*. O *phishing* é um processo informático complexo, que consiste em obter dados pessoais alheios[32], através do uso de emails falsos que direcionam o utilizador a um *link* fraudulento, onde fornece os seus dados - pensado tratar-se aquela página da do seu banco pessoal, ou de outro *site* onde o utilizador normalmente facultaria este tipo de informações. De uma forma mais abrangente, podemos dizer que se refere a toda e qualquer "criação e utilização de meios *online* para atuação fraudulenta"(Vaz, 2013). O facto de enviar emails sem qualquer especificidade, permite ao *phisher* atingir uma quantidade enorme de utilizadores, com o clique de um botão. Apesar do conhecimento e prevenção destes ataques ser cada vez maior, ainda há muitas pessoas que não conseguem conhecê-los, tornando esta forma de obtenção de dados uma das mais danosas ou com maior potencial de danosidade. O ataque pode, também, ser mais direcionado, se o *phisher* escolher uma pessoa determinada,

---

[30] Veja-se, por exemplo, este *website* do governo dos EUA com conselhos de prevenção: https://www.usa.gov/identity-theft ou o *website* do *European Consumer Centre Germany*: https://www.evz.de/en/consumer-topics/online-shopping/internet-fraud-scams/.

[31] "(...) tem origem no termo *fishing* "pescar" resultante da atividade da procura na internet de dados, enquanto o "ph" é derivado do termo (...) "*Password Harvesting*"" - DUQUE, Jorge Rafael V. Reis – **A prova digital e o phishing como caso de estudo,**p. 5. Há quem refira também que o "ph" vem de "*Phone Phreaking*" - GERALDES, Ana Vaz - *Phishing*: fraude online, p.89.

[32] É maioritariamente usado para dados bancários e foi essa a sua origem, mas também se pode aplicar, e aplica cada vez mais, a outro tipo de informações pessoais.

ou um grupo de pessoas determinadas, a quem mostrar um certo *website*, aparentemente legítimo, alguém que o use regularmente, no qual a pessoa vai inserir diretamente os dados[33]. A este tipo de ataque dá-se o nome de *spear phishing*[34], havendo um maior índice de resposta e sucesso para o *phisher,* que toma partido de conhecimentos pessoais dos alvos - o uso de ferramentas como *cookies*[35], permitem adaptar o ataque a utilizadores específicos, através do conhecimento dos seus gostos e preferências. O *phishing* utiliza comummente a técnica de *spoofing*[36]e *pharming*[37]. O *spoofing* faz com que o *email* do emitente pareça o de outra pessoa, dando credibilidade à atuação fraudulenta sem ser necessário invadir a conta de correio eletrónico de outrem. No caso do *pharming*, o *email* não tem como objetivo a introdução de dados sensíveis por parte do recetor, mas sim a entrada, no computador do recetor, de *malware*. O que acontece, aqui, é que alguém recebe um email de uma instituição de confiança, alertando sobre o possível comprometimento da sua conta ou dos seus dados e ilustrando a melhor forma de prevenir que tal aconteça. Normalmente, estes emails vêm acompanhados de um *link* que descarrega *malware*, ou seja, um *software* que tem o objetivo de se infiltrar ilicitamente no computador do utilizador para obter os seus dados. A partir do momento em que estes ficheiros são instalados, tudo o que o utilizador faz no computador, é monitorizado.

Smishing e *Vishing*

O *phishing* evoluiu para outras formas de obtenção de dados, o *smishing* (*sms phishing*) e o *vishing* (*voice phishing*). No fundo, o método é o mesmo, utilizando plataformas diferentes de comunicação, o email dá lugar ao *sms* e à chamada telefónica. Mais uma vez os ataques acompanham a evolução das formas de comunicação das instituições oficiais. À medida que os bancos e as operadoras de telecomunicações (por exemplo), passaram progressivamente a usar estes meios de comunicação com os clientes, também os *phishers* o fizeram. O email torna-se cada vez mais obsoleto e a nossa vida passa a girar à volta do telemóvel e quanto mais direto for o contacto, maior é o nosso interesse e recetividade, para o bem e para o mal.

---

[33] *Domain spoofing.*

[34] WALL, David S./ Williams, Mathew L. – Ob. cit., p. 6.

[35] Os Cookies são atualmente usados pela maioria dos *websites*, especialmente os de *e-commerce* e representam um pequeno conjunto de informações, enviadas de certo *website* para o computador do utilizador, de forma a perceber os seus padrões de comportamento. Possibilitando a mostra de informação mais apelativa e individualmente direcionada.

[36] "(...) *spoofing (sending a message to a computer from a source that pretends the message is coming from a trusted computer's IP address)*" - WANG/ YUAN/ ARCHER, - Ob. cit., p. 31.

[37] "Trata-se aqui de comprometer o *Domain Name System* do utilizador para com o *malware* redirecionar o browser da internet do sítio que se pretende visitar para uma réplica. O utilizador vítima insere informação na base de dados do sítio ilegítimo ou descarrega um ficheiro malicioso. Outro subterfúgio técnico é o de infetar o computador com *key loggers* para registo da utilização do teclado" – GERALDES – Ob. cit., p. 90.

No *vishing* a vítima fornece as suas informações pessoais diretamente ao *phisher*, isto é, através de chamada telefónica, realizada pelo mesmo ou por um sistema de chamadas automáticas, por ele criado. Neste caso, o *phisher* personifica alguém que conheça a vítima, por exemplo mascarando o seu número com o dessa pessoa conhecida; ou alguém de uma instituição de que a vítima seja cliente (bancária; operadora telefónica, etc.), para, sob o pretexto da necessidade de uma qualquer informação urgente, conseguir extrair os mesmos dados pessoais. No *smishing* são enviadas *sms* de forma massiva – tal como os emails no *phishing* – a fazer-se passar por uma instituição que precisa de uma atualização dos dados pessoais (é dado um *link*, tal como nos emails, redirecionando o cliente para a pretensa página oficial, onde deve inserir os dados)[38]. Pode ainda ser pedido ao recetor que ligue a determinado número – passando ao *vhishing* – para fornecer os dados. *Vishing* e *smishing* são, frequentemente, usados juntos, para transmitir uma maior credibilidade do processo[39].

Devido à complexidade destes processos a subsunção legal é possível em diversos tipos criminais. Qualquer forma de *phishing* se pode subsumir ao crime de burla (art.217º do CP), quando e só quando, haja prejuízo patrimonial[40], sendo que o email, *sms* ou chamada de voz que leva alguém a fornecer os seus dados, constitui *meio de erro ou engano.*

A criação de páginas (como as de *homebanking*), para além de poder ser instrumento do crime de burla (havendo resultado), pelas razões acima descritas, é também um caso de falsidade informática (art.3º da LC). Este crime tem como conduta típica objetiva *introduzir, modificar, apagar ou suprimir dados informáticos ou interferir, por qualquer modo, no tratamento informático de dados* e como resultado típico a produção de *dados ou documentos não genuínos*. Isto, ainda, com a intenção de provocar engano nas relações jurídicas e de que estes dados ou documentos não genuínos sejam *considerados ou utilizados para finalidades juridicamente relevantes como se fossem genuínos* – elemento subjetivo especial do dolo[41]. Apesar de os meros e-mails, *sms* ou chamadas telefónicas, não se poderem classificar, sem mais, como um crime de falsidade

---

38 "'*Smishing' is the sending of SMS text messages to potential victims that contain much the same message as in the original phishing emails. They ask victims to reconfirm their 'important security information' immediately by return SMS message, or via a www site.*" - WALL, David S./ Williams, Mathew L. – Ob. cit., p. 7.

39 "*Victims are tricked into ringing back the number given, or asked to log onto a web address given in the message"* - WALL, David S./ Williams, Mathew L. – Ob. cit., p. 7.

40 "O bem jurídico protegido no crime de burla é o património, constituindo a burla um crime de dano que se consuma com a ocorrência de um prejuízo efetivo no património do sujeito passivo da infração ou de terceiro" Ac. do STJ de 4 de Junho de 2003, Proc.03P1528, Rel. Henriques Gaspar.

41"Do ponto de vista subjetivo, o tipo legal supõe o dolo, sob qualquer das formas previstas no artigo 14º do Código Penal, exigindo, enquanto elemento subjetivo especial do tipo, a intenção de provocar engano nas relações jurídicas, bem como, relativamente á produção de dados ou documentos não genuínos, a particular intenção do agente de que tais dados ou documentos sejam considerados ou utilizados para finalidades juridicamente relevantes como se fossem genuínos." – Ac. do TRE de 19 de Maio de 2015, Proc. 238/12.8PBPTG.E1, Rel. António Latas.

informática[42], por nem sempre produzirem dados ou documentos não genuínos, no caso das páginas criadas já existe um resultado, a página falsificada já preenche a última parte do art.3º, nº1 da LC - *produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem*[43]. Por outro lado, no caso das *sms* ou chamadas que aparentam ser de uma qualquer entidade real, por exemplo fazendo com que apareça no ecrã do telemóvel da vítima a designação dessa entidade, já são um caso de falsidade informática, criando o dado falso do nome que aparece. Não será esse o caso, quando o número aparece sem qualquer identificação, o simples conteúdo da mensagem ou chamada não são suficientes para dizer que houve produção de um dado ou documento falso, tão só de uma atuação fraudulenta.

Quando não exista produção de dados falsos estaremos perante outro tipo de enquadramento legal e que dependerá da maneira como foi cometido o *phishing*. GERALDES explica que o *phishing* pode ser sinonimo de dano informático (art.4º da LC); acesso ilegítimo (art.6º da LC) ou interceção ilegítima (art.7º da LC)[44]. Nas palavras da autora, o caso já referido do *pharming*, em que são descarregados programas maliciosos no computador do utilizador, é, antes de mais, um crime de acesso ilegítimo. O bem jurídico protegido por este crime é, nas palavras de SILVA RODRIGUES[45], "a formal esfera da privacidade e do segredo" ou a "integridade do sistema informático lesado", de forma a proteger a inviolabilidade do domicílio informático. Ao instalar *malware* no computador da vítima, o *phisher* está a violar o seu domicílio informático, intrometendo-se na sua esfera privada. Para além do acesso ilegítimo, pode também dar-se uma interceção ilegítima, quando o *malware* é utilizado para monitorizar o tráfego de internet da vítima, seja para capturar as suas *passwords* e credenciais *online*, seja para "simplesmente" monitorizar o seu quotidiano. Por fim, a instalação de *malware* que permita alterar ou afetar a capacidade de acesso à internet do utilizador, já configura, também, um caso de dano informático.

[42] A criação de um email não configura, só por si, um caso de falsidade informática, na realidade existe liberdade total para a designação de um email que pode ser criado a qualquer momento, pelo que um endereço de email com uma designação de uma entidade bancária ou com o nome de uma pessoa já existente, não produz *dados não genuínos*.

[43] Contrariamente veja-se GERALDES – Ob. cit., p. 92, subsumindo o *phshing*, nestes casos, ao crime de falsidade informática.

[44] GERALDES – Ob. cit., p. 93

[45] *Apud* GERALDES – Ob. cit., p. 94

Falsificação de documentos

O passo lógico que segue a obtenção de dados é o seu uso e este uso pode-se traduzir em diferentes atuações. A mais antiga e usual dessas formas é a falsificação de documentos, seja através da criação de um documento completamente novo de identificação, com dados alheios, seja o uso desses dados em documentos que carecem de elementos de identificação para serem válidos/cumprirem as exigências legais necessárias (escrituras, pedidos de crédito, contratos de compra e venda, entre outros).

Segundo PERL[46], existem 3 tipos de "fraude de identidade": financeira, quando a identidade externa é usada para obter dinheiro ou para a abertura de conta bancária ou de crédito através do uso dos dados pessoais da vitima; não-financeira quando os dados são usados para aceder a um qualquer serviço como telecomunicações ou seguro médico, por exemplo; criminal[47] quando o ofensor comete crimes ou qualquer ato ilegal fazendo-se passar pela vitima e usa a sua identidade, quando detido, para evitar que tal ilegalidade fique no seu cadastro. Os danos, para a vítima, podem ser os mais variados, dependendo do tipo de uso dos dados. Estes danos podem materializar-se em perdas monetárias "ativas" – como acontecerá na maior parte das vezes -, o que poderá posteriormente influenciar qualquer pedido de crédito ou tentativa de compra, momento em que a vítima finalmente se apercebe do que ocorreu. As perdas patrimoniais podem também ser "passivas", se os dados forem usados para conseguir um crédito ou hipoteca, o que vai gerar dividas para a vítima[48]. As consequências podem ser a nível do bom nome, quando os dados são usados para evitar a prisão, o que vai criar um cadastro falso, i.e., em nome de pessoa errada; ou quando são usados para conseguir um emprego, o que poderá "manchar" a reputação profissional. Em qualquer destes casos, pode haver necessidade de falsificar documentos.

A falsificação de documentos encontra-se criminalizada, com bastante pormenor, nos artigos 256º e seguintes do CP.

O artigo 255º, primeiro do *Capítulo II – Dos crimes de Falsificação*, contém algumas definições legais que servem de suporte à compreensão dos crimes deste Capítulo. A definição de documento indica-nos, desde logo, que o que releva é a declaração constante do documento e não o material que contém essa declaração. O que interessa é, portanto, a

[46] *Apud* WHITE/ FISHER – Ob. cit., pp. 3 e 4.
[47] Tradução nossa, o termo original usado é "criminal record".
[48] Por exemplo, os dados são utilizados para conseguir um crédito de 50.000€, que é autorizado. Quem usou os dados indevidamente fica com os 50.000€ e o titular dos dados fica com uma dívida de 50.000€, mais juros, em seu nome.

vontade que a parte ou partes decidiram expressar e não o suporte em que o fizeram[49]. Coloca-se então a questão: um documento digital também se inclui no conceito de documento do Código Penal? O espelho deste crime na Lei do Cibercrime seria o já referido crime de falsidade informática. Isso significa, então, que o crime de falsidade informática veio esvaziar de sentido o crime de falsificação ou contrafação de documentos? Não nos parece. Ao contrário do art.256º que dá espaço para várias formas de entendimento sobre o que seja documento, não ficando claro se o documento digital se inclui ou não, no caso da falsidade informática fica claro que este artigo só se aplica a ficheiros informáticos. Sendo assim, a aplicação de um artigo exclui a aplicação do outro, ou pode haver um concurso entre os dois tipos criminais no documento físico? Parece-nos sim, de acordo com OLIVEIRA ASCENSÃO, "que temos afinal um tipo novo, e não propriamente um tipo qualificado em relação ao art.256 do Código Penal. A aplicação deste tipo exclui a do art.256º. Não se pode recorrer a este como o tipo geral"[50]. Logo, quando resulte do uso de dados um documento físico, será de aplicar o art.256º do CP, mesmo que a obtenção dos dados necessários para a falsificação tenha sido realizada em meio digital; quando, pelo contrário, a falsificação é realizada diretamente no documento informático, será de aplicar o art.3º da LC. O critério, aqui, será o do formato do documento sobre o qual incidiu a falsificação[51]. O mesmo raciocínio será de aplicar, aos restantes casos de falsificação previstos no Código Penal.

Caso especial: os cartões bancários e outros documentos com dados informáticos incorporados

O caso da falsificação de cartões bancários afigura-se ligeiramente diferente, dada a natureza do documento. A contrafação de cartões de crédito bastava-se, no passado, com a cópia do cartão em si, uma vez que este não tinha incorporados quaisquer dados. Qualquer pessoa apresentava o cartão falso e automaticamente a compra era feita (sem necessidade de passar o cartão num POS[52]). Hoje em dia, o processo é mais complexo: com a existência da banda magnética/chip, não é suficiente que o cartão pareça verdadeiro (exteriormente), é necessário que tenha em si incorporados os dados bancários correspondentes aos do seu titular. Isto significa que uma falsificação que era unicamente "física", passa a ter que ser obrigatoriamente informática. O que impõe a questão: o crime de contrafação de cartão de

[49] Assim o confirma o CP Anotado: "o documento é, antes do mais, uma declaração corporizada em escrito ou registado em qualquer meio técnico. Não é, pois, o material que corporiza a declaração, mas a própria declaração, em si, enquanto representativa de um pensamento humano (função de perpetuação)" - PEREIRA/ LAFAYETTE – Ob. cit., p. 712.

[50]OLIVEIRA ASCENSÃO, José de – Criminalidade Informática, p. 222.

[51] Se a falsificação foi feita num documento em papel, posteriormente digitalizado, relevante continua a ser o art.256º do CP. O mesmo se dirá se um documento foi impresso e falsificado em papel. Pelo contrário se foi digitalizado e só no computador aletrado, aplica-se o art.3º da LC.

[52] POS – sigla representativa de *point of sale*, em português ponto de venda.

crédito (art.262º *ex vi* art.267º, nº1, al. c)) ainda faz sentido? A resposta é, em nosso entender, negativa. Efetivamente, o cartão de crédito não passa dos dados que em si estão inseridos; o cartão em si é absolutamente inútil, sem o conteúdo da banda magnética. O que faz deste um crime intrinsecamente informático, devendo, por isso, ser regulado pela lei do cibercrime. Foi exatamente isso que o legislador fez ao consagrar o crime de falsidade informática, e ao prever explicitamente no nº2 o exemplo do cartão bancário[53] , esvaziando totalmente de conteúdo a contrafação de cartão de crédito. Até porque este crime exige que o documento não genuíno, o seja, exatamente, porque houve uma viciação dos dados informáticos ou do tratamento informático de dados. É necessário que a não genuinidade resulte, diretamente, da viciação, o que acontece aqui. Sem viciação informática é impossível falsificar cartões de crédito ou qualquer outro documento de identificação atual, sendo que todos eles têm dados incorporados[54]: o Cartão do Cidadão tem um chip com todos os dados do titular e o Passaporte passou a ser eletrónico (convertendo-se progressivamente desde 2006, quando surgiu a nova versão eletrónica).

A verdade é, no entanto, que a nossa jurisprudência continua a aplicar o crime de contrafação de cartão de crédito e fá-lo, essencialmente, por considerar que os dois crimes protegem bens jurídicos diferentes[55]. Este argumento não procede por uma simples razão: a lei do cibercrime é uma lei muito particular, que não protege somente bens jurídicos iminentemente informáticos. A LC é uma adaptação a uma nova realidade, capaz de maiores danos e maior alcance, tendo em mente os mesmos valores de sempre. Não nos podemos esquecer que o mundo digital tem a capacidade de afetar qualquer bem jurídico, os sistemas informáticos são um meio para atacar bens jurídicos. A afirmação de que o bem jurídico protegido pelo crime de falsidade informática é a integridade dos sistemas informáticos, é vazia. Os sistemas informáticos não são coisas a proteger, mas sim todos os dados que contêm. O *software* é constituído por dados, mesmo que estes se exprimam em 0 e 1, e o *hardware* é uma *coisa* (art.202º, nº1 CC), na verdadeira aceção jurídica da palavra. Tal como defendemos *supra* no que toca à ciberidentidade, os bens a proteger são exatamente os mesmos, num suporte diferente. O mesmo será dizer que a integridade dos sistemas

[53] Há uma certa resistência da nossa jurisprudência a aplicar este artigo – e outros da LC – sem concorrer com um qualquer outro crime. Quase nos leva a crer que a LC é uma lei acessória e complementar dos "verdadeiros crimes": os do CP.

[54] Sendo verdade que a mera falsificação física/aparente dos documentos já é subsumível no crime de falsificação de documentos do CP, a verdade é que a falsificação integral necessitará sempre de viciação informática – sem esta, a utilidade do documento ficaria substancialmente limitada.

[55] Assim, o Ac.do TRP de 21 de novembro de 2012, Proc. 1001/11.9JAPRT.P1, Rel. Borges Martins e o Ac.do TRL de 10 de julho de 2012, Proc. 7876/10.1JFLSB.L1-5, Rel. Luís Gominho (por exemplo).

informáticos contém, em si, todos os valores que se querem proteger nos crimes por este meio perpetrados. Por isso mesmo concordamos com VENÂNCIO[56] quando este nos diz que o artigo 3º da LC tutela a segurança das relações jurídicas enquanto interesse público essencial[57] . No caso da contrafação de cartões, o facto de os dados bancários estarem acessíveis na internet, faz com que qualquer atuação destinada a introduzir, modificar, apagar ou suprimir dados informáticos que garantem acesso a uma conta bancária, atinja imediatamente a integridade dos sistemas informáticos, na medida em que afeta o sistema económico, o direito à privacidade dos cidadãos e, bem assim, a segurança das relações jurídicas como um todo. Pelo que faz todo o sentido que a falsidade informática abarque todos estes bens jurídicos. Mais se acrescenta, que o facto desta jurisprudência condenar sempre os agentes por falsidade em concurso efetivo com contrafação de cartão de crédito, mesmo quando não se consegue fazer prova de que foram aqueles agentes a adquirir os dados de outrem e de que forma, é uma admissão clara de que este crime é iminentemente informático. A simples produção do documento já deve ser, (e ao que parece é) considerada falsidade informática. Desta forma, é levantado um grave problema de dupla incriminação, pois que se admitimos que a produção do documento falso é falsidade informática, então a condenação de exatamente o mesmo facto por contrafação viola o *ne bis in idem*.

Mais ajuda o nosso argumento, o exemplo de alguém que detém um cartão de crédito falsificado – não por si – adquirido de um terceiro. Neste caso, a resolução mais óbvia e instintiva[58] seria a de que pratica um crime de aquisição de moeda falsa para ser posta em circulação, até porque não há, supostamente, práticas informáticas por parte deste agente. Contudo este pensamento significaria, mais uma vez, ignorar a essência das coisas. Quem tem em sua posse um cartão de outrem falsificado, tem claramente a intenção de usar e por isso mesmo o legislador inseriu esta possibilidade no número 3 do artigo 3º[59]. Ora se até aqui, quando não há atos informáticos, estamos na presença de um crime de falsidade informática que utilidade real poderá ter ainda o crime de contrafação? Só vemos três: primeira, a moeda em papel; segunda, o cheque; terceira, a dos documentos identificativos que ainda não passaram à sua versão informatizada, i.e., BI (para quem ainda o tenha) e Passaporte (não

[56] VENÂNCIO, Pedro Dias – **Lei do Cibercrime: Anotada e Comentada**, p.38.
[57] Na mesma linha veja-se o acórdão da Relação de Évora de 19 de maio de 2015, Proc. 238/12.8PBPTG.E1, Rel. António Latas. Como admite o GABINETE DE CIBERCRIME, não é pacífico o entendimento jurisprudencial quanto aos interesses jurídicos protegidos pelo tipo de crime, referindo-se à falsidade informática PROCURADORIA-GERAL DA REPÚBLICA – GABINETE CIBERCRIME – **Nota prática nº 5/2015 27 de Agosto de 2015: Jurisprudência sobre cybercrime**, pp. 1 e 2.
[58] E concordante com a jurisprudência que defende o concurso efetivo.
[59] O uso de documento não genuíno (nº3 do artigo 3) apenas é punido se o for por pessoa distinta da que praticou a "falsificação" – Ac. do TRE de 19 de maio de 2015, *supra* citado.

eletrónico). Pese embora todos estes documentos possam ser falsificados com ajuda de meios informáticos – e serão na maior parte dos casos, o que aumenta a probabilidade de parecerem autênticos, como será de esperar quando comparados com os feitos manualmente, terão sempre de ser transformados no seu suporte físico que não tem incorporados quaisquer dados. Nestes casos justifica-se o concurso efetivo entre a LC e o CP. Claro está que até estas aplicações em breve deixarão de se justificar, tanto o cheque como os documentos de identificação antigos, tendem a desaparecer. No que toca à moeda, a evolução é no sentido de também esta passar pelo processo de informatização. Já este ano, foi anunciado pela Suécia que se prepara para emitir moeda digital própria e acabar com a circulação de moeda em papel.

Parece então que, segundo esta visão, o crime de falsidade informática resolve todos os nossos problemas no que toca a documentos informáticos: o nº1 engloba a obtenção de dados de outrem por meio de qualquer "criação e utilização de meios *online* para atuação fraudulenta", bem como a utilização desses dados para produção de "dados ou documentos não genuínos"; o nº2 cria uma agravação[60] para estas condutas quando direcionadas a "acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado"; o nº3 especifica que o mero uso destes documentos é punido da mesma forma; o nº4 aplica a pena do nº2 a quem "importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo" referido no nº2[61]; o nº5 cria uma agravação para a pratica destas condutas por funcionário no exercício das suas funções.

Compras online

As compras online são uma forma de usar os dados obtidos sem ter de falsificar um documento de pagamento. Em vez disso, o *phisher* passa diretamente ao uso de dados para comprar produtos *online*. Graças ao *e-commerce*, a falsificação do documento é mais uma fase possível de "saltar". Isto significa um aumento exponencial da possibilidade de produção de danos patrimoniais e uma diminuição exponencial do tempo que se demora a fazê-lo.

O caso das compras online, parece-nos ser aquele que mais facilmente se subsume ao crime de falsidade informática, sem haver questão quanto à aplicação em concurso de

[60] Elimina a hipótese de pena de multa e define um mínimo de 1 ano para a pena de prisão.
[61] Parece-nos que esta remissão devia ter sido feita ao nº1 e não ao nº2 do art.3º, ficando de fora todos os dados que não tenham a finalidade de "acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado".

algum dos crimes do CP. O processo é estritamente informático, sem chegar a haver uma falsificação de documento, somente um uso ilegítimo de dados, como se fossem seus. Existe, de facto, uma intenção de engano nas relações jurídicas, através do uso de dados genuínos, mas que produzem uma aparência falsa – a aparência de que os dados estão a ser usados pelo seu real titular.

Catfishing

Catfishing é um novo método de *phishing* que consiste em criar um perfil falso nas redes sociais, com o intuito de enganar outros, assumindo uma identidade que não é a sua. Este pode ser um método de obtenção e/ou utilização de dados. No caso de o perfil online ser feito com informações pessoais de outrem, com o objetivo de adquirir informações de mais pessoas, estamos num caso de uso e obtenção de dados. No entanto, normalmente, o *catfishing* é uma das formas de uso de dados e não obtenção. O objetivo de um *catfisher* é fazer-se passar por outra pessoa, evadindo-se de quem é. Para tal, usa fotografias ou informações de pessoas que pensa serem mais bonitas, socialmente "populares". No fundo, esta é a expressão da ciberidentidade tal como concebida por SHERRY TURTLE: multiplicidade, invisibilidade e anonimato. O que, em si, não apresenta problemas, tirando quando se envolve o uso de dados de outrem ou o uso de dados falsos, com o intuito de enganar alguém. É isto que acontece no *catfishing*. Mesmo que não haja uso de dados verdadeiros (de outrem), o intuito é sempre enganar alguém, por exemplo, levando outra pessoa a partilhar pormenores da sua vida íntima.

Neste caso, pode haver uma burla, se o objetivo for o enriquecimento ilegítimo, o que, como já referimos, raramente será o caso. Pode haver, com mais probabilidade, um crime de Devassa da vida privada (art.192º do CP), de Devassa por meio informática (art.193º do CP), ou, ainda, de Gravações e fotografias ilícitas (art.199º do CP); sem esquecer, claro, a Difamação é Injúria, que foram exponenciados pelo aparecimento da internet e, mais concretamente, das redes sociais. O enquadramento legal vai depender do resultado do *catfishing* – fotografias; vídeos; conversas online; partilha de detalhes da vida íntima – e daquilo que o *catfisher* decide fazer com estes dados – mantê-los; divulgá-los; usá-los para conseguir uma aproximação à vítima.

2. A criminalização da apropriação indevida de identidade noutros ordenamentos jurídicos

Chegados à conclusão de que não existe uma tipificação legal do fenómeno apropriação indevida de identidade no nosso ordenamento jurídico, afigura-se útil compreender de que forma é que a legislação estrangeira o criminaliza. Como vimos, existem já vários países que decidiram criminalizar autonomamente a apropriação indevida de identidade, ou fases da mesma (como o *phishing*). Falaremos aqui dos Estados Unidos da América; Alemanha; Espanha e México. De forma a termos uma visão holística do entendimento do crime, é importante analisarmos a sua consagração, tanto em sistemas Anglo-Saxónicos, como em sistemas Romano-Germânicos.

Estados Unidos da América

A análise comparada com a legislação americana é, possivelmente, a mais importante, por ser este o país com mais crimes de roubo de identidade registados e, por isso, com mais trabalho de investigação, estatístico e jurídico feito sobre a matéria. Em 2001 o aumento deste crime nos EUA foi de 105% em comparação com o ano anterior[62]. As perdas em 2005 foram de 56$ milhares de milhões no "roubo de identidade" a pessoas coletivas e singulares[63]. O Departamento de Justiça dos EUA identificou 17.6 milhões de vítimas em 2014[64]. Os serviços secretos dos EUA detetam 30 ataques por dia a *websites*[65]. Para além disso os crimes mais comuns de "roubo de identidade" incidem sobre cartão de crédito e telemóvel, onde o potencial de ganhos é superior[66] e sobre bancos e sites de compras online - 30% estão ligados ao eBay (empresa de e-commerce dos EUA) e ao PayPal (empresa de pagamento online dos EUA) e 60% ao CitiBank (Banco dos EUA) – de acordo com LYNCH[67]. Infelizmente não existem, até à data, estatísticas divulgadas em Portugal. Os dados serão, certamente, significativamente mais baixos, mas o aumento tem sido exponencial em todo o Mundo.

O Código criminal dos EUA tipifica no seu artigo 1028 *Fraud and related activity in connection with identification documents, authentication features, and information* (inserido no Capítulo 47 – *Fraud and False Statements*, do Título 18 - *Crimes and Criminal Procedure*), o crime do roubo de identidade, de acordo com o *Identity Theft and Assumption Deterrence Act*. Segundo este artigo é

[62] WHITE/ FISHER – Ob. cit., p.12.
[63] ROMANOSKY, Sasha – Do Data Breach Disclosure Laws Reduce Identity Theft?, p.256.
[64] Dados do website de estatística do Departamento de Justiça (*US Bureau of Justice Statistics* -www.bjs.gov).
[65] CHOU, Neil [et al.] - **Client-side defense against web-based identity theft,** p. 1.
[66] WANG/ YUAN/ ARCHER, - Ob. cit., p.31.
[67] LYNCH, Jennifer – Ob. cit., p.267

crime a produção; transferência; detenção com intenção de uso e tráfico de documentos de identificação. Existe agravação caso se trate de uma certidão de nascimento; carta de condução; bilhete de identidade (no que toca à natureza do documento), ou caso a falsificação seja feita para facilitar um crime de tráfico de droga ou um crime violento (no que toca à razão subjacente à falsificação). O mesmo artigo passa, depois, a estabelecer algumas definições legais, como a de documento de identificação e a de elementos de autenticação[68].

Os EUA criminalizam, portanto, a fase de uso dos dados e não a sua obtenção. Tal como dissemos, existe uma distinção, no direito anglo-saxónico, entre *identity theft* e *identity fraud*, sendo que só este último é criminalizado – o uso de dados alheios[69], de modo a criar um qualquer benefício. A fraude de identidade é um crime de resultado, que tutela os dados pessoais, quando estes são usados na produção de um novo documento de identificação, ou num documento de identificação falso[70]. Outros documentos legais relacionados com o roubo de identidade têm medidas de prevenção para este crime. São exemplo o *Gramm-Leach-Bliley Act* (1999), que exige medidas de prevenção para a revelação não autorizada de informações financeiras dos seus clientes, bem como medidas de dissuasão para o acesso fraudulento a essas informações[71]; o *Computer Fraud and Abuse Act* (2001) criminaliza atuações informáticas que tenham por intenção o acesso, sem consentimento, a informação financeira e de cartões de crédito[72] - enquadra-se aqui qualquer exemplo de *phishing*, que tenha por intenção a obtenção deste tipo de dados; e o *Fair and Accurate Credit Transaction Act (FACTA)* aprovado em 2003, possibilita alertas de fraude, a pedido dos clientes, nos seus extratos bancários e exige uma série de medidas de prevenção para os agentes de crédito a ser definidas pela *Federal Trade Commission*[73].

---

[68] "*the term "authentication feature" means any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified*".

[69] Foi já decidido no caso FLORES-FIGUEROA *v.* UNITED STATES que o agente tem de estar consciente de que os dados são de facto alheios e pertencentes a uma pessoa real: *"Section §1028(a)(1) requires the Government to show that the defendant knew that the means of identification at issue belonged to another person."* - FLORES-FIGUEROA *v.* UNITED STATES, No. 08–108. Argued February 25, 2009 - Decided May 4, 2009.

[70] O ITADA (*Identity Theft and Assumption Deterrence Act*), aprovado em 1998, deu origem à reformulação do citado artigo 1028 e define roubo de identidade como qualquer ato através do qual alguém *"knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit or to aid or abet any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under applicable state or local law"*.

[71] *Vide* WHITE/ FISHER – Ob. cit., p. 5.

[72] WHITE/ FISHER – Ob. cit., p. 6.

[73] CURTIS, George – **The Law of Cybercrimes and their Investigations**, p. 120.

Apesar de este ser o panorama geral, sendo os EUA uma república constitucional federal, as leis estatais têm diferentes configurações do que é o roubo de identidade e das sanções a aplicar. Como nos explicam WHITE/ FISHER, para alguns Estados este fenómeno constitui um crime, para outros um ilícito de menor gravidade ("*Felony versus misdemeanor*")[74] e, para alguns, a distinção entre a sanção é feita através de critérios do valor da perda financeira. Existe a possibilidade de agravação da pena caso haja reincidência na lei do Estado de Nova Iorque, por exemplo. Na Geórgia, Carolina do Norte, Utah, Wyoming e Califórnia, é permitido, a pedido da vítima/obrigatório (dependendo do Estado em causa) que sejam corrigidos os registos criminais, apagando os dados erradamente associados à pessoa cuja identidade foi indevidamente usada, de modo a restituir a situação da vítima que existia antes do crime. No que toca aos limites do crime, o Michigan é o único que reconhece e proíbe expressamente o roubo de identidade a fim de conseguir emprego. Pese embora as diferenças de tratamento, importante é perceber que a maioria[75], senão todos os Estados dos EUA, têm legislação sobre roubo de identidade.

Alemanha

A legislação alemã não autonomiza o crime de apropriação indevida de identidade, no entanto, tem, neste âmbito, duas normas relevantes no Código Penal. A "Secção 152a. Contrafação de cartões de débito, etc, cheques e notas promissórias"[76], criminaliza a contrafação de cartões de débito, cheques e notas promissórias, à semelhança da nossa *falsificação de moeda, título de crédito e valor selado* (artigos 262º a 268º do CP). Contudo, ao contrário daquilo que se passa no caso português, não nos parece que este artigo tenha sido esvaziado de sentido, devendo continuar a aplicar-se, nos exemplos que não envolvam dados informáticos, como o cheque e as notas promissórias[77]. Diferentemente do legislador português, o legislador alemão decidiu acrescentar os crimes informáticos ao Código Penal, ao invés de fazer uma lei especifica, como a nossa Lei do Cibercrime. Paralelamente ao crime de falsidade informática, existe o crime de adulteração de dados – "Secção 303a. Adulteração de dados"[78]. Seguindo o nosso raciocínio, com base nestas duas normas e fazendo um

[74]WHITE/ FISHER – Ob. cit., p. 6.
[75] Na obra de Perl de 2003, eram identificados 48 Estados com legislação aprovada – *Apud* WHITE/ FISHER – Ob. cit., p. 6.
[76] Anexo IV.
[77] Ainda que, no caso alemão, a questão do concurso seja mais discutível, porque o crime correspondente à falsificação informática da LC – adulteração de dados – não refira expressamente o caso dos cartões bancários.
[78] *"Section303a. Data Tampering*
(1) Whosoever unlawfully deletes, suppresses, renders unusable, or alters data (section 202a(2)) shall be liable to imprisonment not exceeding two years or to a fine.
(2) The attempt shall be punishable."

paralelismo com a nossa lei, no que toca à contrafação de cartões bancários, seria aqui de aplicar o crime de adulteração de dados não havendo concurso entre os dois. Não nos parece que assim seja. Diferentemente do crime de falsificação informática, a adulteração de dados não exige a produção de um documento, tão só o apagamento, supressão, inutilização e alteração dos dados. O que significa que este artigo não cobre todas as fases do crime, desde a obtenção de dados ao uso. Neste caso, a obtenção de dados estaria protegida por este crime de adulteração de dados (ou pelo de *phishing*, como veremos) e o uso desses dados pelo crime de contrafação.

A "Secção 202b. *Phishing"* criminaliza a técnica de obtenção de dados mais comum, o *phishing*. Este crime está descrito como a interceção ilegal de dados não destinados ao agente criminoso, para seu benefício ou de terceiros. A norma seguinte, criminaliza os atos preparatórios do crime, através do uso de palavras-passe, códigos de segurança ou aproxima-se ao nosso crime de interceção ilegítima (art.7º da LC). A vantagem desta norma é, claro, a facilidade de subsunção destes atos ao tipo legal. Enquanto que em Portugal o *phishing* pode integrar uma série de tipos legais, discutindo-se quais serão ou quais os mais indicados – burla, acesso ilegítimo, interceção ilegítima, falsidade informática -, no caso da lei alemã, essa dúvida fica dissipada, pelo que nos parece útil a sua incriminação autónoma, tendo em conta a expressão e danosidade destas atuações. A desvantagem passa pelo facto algumas fases da apropriação indevida de identidade poderem ficarem desprotegidas. As formas de obtenção de dados, como vimos, podem ser, para lá do *phishing*, o *trashing*, o *skimmer*, ou o *catfishing* – todos estes casos, apesar de não estarem autonomamente previstos, podem subsumir-se ou

ao crime de *phishing* ou ao crime de fraude[79] ou fraude informática[80], do código alemão. Falamos aqui de *phishing*, porque no caso do *skimmer*, dada a formulação da Secção 202b., parece-nos ainda razoável conseguir incluir esta conduta. Apesar de não ser uma forma de *phishing*, pode ainda enquadrar-se naquela que é a formulação legal desta norma, sendo também uma forma de interceção ilegal de dados. Contrariamente, as formas de uso de dados só estão contempladas na vertente financeira da apropriação indevida de identidade na *Secção 152a.* Significa isto que as formas restantes – não financeira e criminal - ficam desprotegidas. De facto, não há nenhuma norma no Código Penal Alemão que acautele situações como o uso de dados alheios para conseguir um seguro médico ou evitar registo criminal, por exemplo. Só ficam garantidas as formas de uso de dados que resultem num dano financeiro, ou que tenham essa intenção.

Espanha

A lei Espanhola optou por um sistema de consagração legal diferente dos EUA e da Alemanha. A usurpação de identidade, designação usadas pelos países de língua Espanhola, foi incluída no capítulo das falsificações - *TÍTULO XVIII De las falsedades*, mais concretamente no título das falsidades documentais - *CAPÍTULO II De las falsidades*

---

[79] *Section 263 - Fraud*
(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by causing or maintaining an error by pretending false facts or by distorting or suppressing true facts shall be liable to imprisonment not exceeding five years or a fine.
(2) The attempt shall be punishable.
(3) In especially serious cases the penalty shall be imprisonment from six months to ten years. An especially serious case typically occurs if the offender
1. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of forgery or fraud;
2. causes a major financial loss of or acts with the intent of placing a large number of persons in danger of financial loss by the continued commission of offences of fraud;
3. places another person in financial hardship;
4. abuses his powers or his position as a public official; or
5. pretends that an insured event has happened after he or another have for this purpose set fire to an object of significant value or destroyed it, in whole or in part, through setting fire to it or caused the sinking or beaching of a ship.
(4) Section 243(2), section 247 and section 248a shall apply mutatis mutandis.
(5) Whosoever on a commercial basis commits fraud as a member of a gang, whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269 shall be liable to imprisonment from one to ten years, in less serious cases to imprisonment from six months to five years.
(6) The court may make a supervision order (section 68(1)).
(7) Section 43a and 73d shall apply if the offender acts as a member of a gang whose purpose is the continued commission of offences under sections 263 to 264 or sections 267 to 269. Section 73d shall also apply if the offender acts on a commercial basis.

[80] *Section 263a – Computer fraud*
(1) Whosoever with the intent of obtaining for himself or a third person an unlawful material benefit damages the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing shall be liable to imprisonment not exceeding five years or a fine.
(2) Section 263(2) to (7) shall apply mutatis mutandis.
(3) Whosoever prepares an offence under subsection (1) above by writing computer programs the purpose of which is to commit such an act, or procures them for himself or another, offers them for sale, or holds or supplies them to another shall be liable to imprisonment not exceeding three years or a fine.
(4) In cases under subsection (3) above section 149(2) and (3) shall apply mutatis mutandis.

documentales[81].O Título XVII começa pela falsificação de moeda; passando pela falsificação de documentos públicos, oficiais, mercantis e emitidos por serviços de telecomunicações; documentos privados; certificados e cartões de crédito, débito e cheques de viagem. O Capítulo III equipara aos crimes descritos acima o fabrico, receção, aquisição ou posse de ferramentas, materiais, instrumentos, substâncias, dados e programas de computador, dispositivos, elementos de segurança ou outros meios especificamente destinados a cometer tais crimes - *Artículo 400*. No artigo 400bis, os documentos de identidade são expressamente referidos como devendo ser entendido integrando o conceito de documento falso nos artigos 392, 393, 394, 396 e 399. Finalmente, no artigo 401 surge o crime correspondente à apropriação de identidade, com a designação de "*De la usurpación del estado civil*", com uma pena de 6 meses a 3 anos (sem hipótese de multa). No sistema jurídico Espanhol, o conceito de Estado Civil é equivalente ao nosso conceito de identidade, onde se integram a idade; o casamento; a filiação; a nacionalidade e, para algum setor doutrinário, também o nome e o género[82]. Trata-se de um crime de perigo, não sendo exigida a produção de um dano. Apesar do objetivo final ser causar um dano ou alcançar um benefício, a realização basta-se com a usurpação.

O crime de usurpação de identidade, na lei espanhola, exige que a pessoa representada por outrem seja uma pessoa real, não cabendo neste tipo legal representações de pessoas inventadas ou fictícias. É indiferente se a pessoa representada está viva ou não, o que releva é que haja uma adotação da identidade de outra pessoa real, mesmo que já tenha falecido[83]. A doutrina entende que se trata de um crime que exige dolo direto, sendo que a mera conduta de alguém se fazer passar por outro não é relevante, a menos que haja uma intenção de prejuízo ou benefício ao fazê-lo[84]. Para que haja usurpação é necessária uma verdadeira incorporação de várias facetas da pessoa representada, é um facto global e não somente a utilização de um documento falsificado ou furtado para o cometimento de um ato isolado – assim considerou a STS nº1045/2011, de 14 de Outubro[85]. A usurpação é, portanto,

---

[81] Ver Anexo V.

[82] *In*http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAAUMTE0tztbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAnRyZhzUAAAA=WKE[Última Consulta 4 de Jan. 2019].

[83]STS nº331/2012, de 4 de Maiode 2012, Proc. 11221/2011, Rel. Jose Ramon Soriano

[84] *"La doctrina dominante entiende que este delito solo puedecometerse por dolo directo, absolviendo el TS en sentencia de 26 de marzo de 1991 a quien se hizopasar por suhermano para escapar a la justicia, evitando ser condenado enunproceso penal."– In*https://www.legalitas.com/pymes-autonomos/actualidad/articulos-juridicos/contenidos/La-usurpacion-de-identidad [Última Consulta 4 de Jan. 2019].

[85]E o STS em 15 de Junho de 2009:"*Para usurpar no basta con usar unnombre y apellidos de otra persona, sino que esnecesario hacer algo que sólopuede hacer esa persona por las facultades, derechos u obligaciones que a ellasólocorresponden; como puede ser el obrar como si uno fueraotro para cobrar undinero que es de este, o actuaren una reclamación judicial haciéndosepasar por otra persona, o simular ser la viuda de alguien para ejercitarunderechoen tal condición, hacersepasar por un determinado*

uma alteração consciente da verdade, criando uma aparência da mesma. Essa alteração tem de ter sempre presente a intenção de prejudicar o titular real dos dados ou obter um benefício (elemento específico do dolo), embora o preenchimento do crime se baste com a usurpação, mesmo que ainda não se tenham produzido os danos.

México

O México consagrou expressa e autonomamente o crime de usurpação de identidade no artigo 211 Bis do seu Código Penal[86]. De forma simples, a lei mexicana define o crime como a usurpação, por qualquer meio e para fins ilícitos, da identidade de outrem. O crime é agravado para quem se aproveite de ter o mesmo nome, parecenças físicas ou de voz em relação à pessoa cujas identidades vão usurpar. Esta última parte do artigo é uma total inovação em relação aos restantes ordenamentos jurídicos.

O acréscimo desde crime ao código penal foi proposto em 2016, depois deste país ter sido declarado, pela Comissão Nacional para a Proteção e Defesa dos Usuários de Serviços Financeiros (Condusef), como o oitavo país com mais incidência deste fenómeno criminoso, com um aumento de 40% de reclamações relacionadas de 2014 para 2015[87]. Reconhecendo o vazio legal que existia e o direito à identidade como um direito fundamental e meio de acesso a todos os outros direitos[88], foi proposta a autonomização da usurpação de identidade como crime. Os argumentos da proposta foram os seguintes: o direito à identidade é o que nos permite exercer a nossa cidadania, por ser aquele que implica o reconhecimento de um direito ao nome, nacionalidade e personalidade jurídica; a Constituição Politica dos Estados Unidos Mexicanos reconhece, no seu artigo 4º, a identidade como um direito fundamental[89]; a Convenção Americana de Direitos Humanos (1969), ratificada pelo México em 1981, estabelece obrigações, nos seus artigo 3º,18º e 20º, de reconhecer tais direitos como fundamentais e adotar medidas legislativas que garantam o

---

periodista para publicar algún artículo o intervenirenun medio de comunicación"- STS nº635/2009, 15 de Junho de 2009, Proc. 1721/2008, Rel. Joaquin Delgado Garcia.

[86] Anexo VI.

[87] Assim o confirma a iniciativa parlamentar que sugeriu o artigo hoje em vigor – **Iniciativa que adiciona diversas disposicionesdel Código Penal Federal, suscrita por la Dip. Lorena Corona Valdés (PVEM) e integrantes del grupo parlamentário del PVEM** – *In*http://sil.gobernacion.gob.mx/Archivos/Documentos/2016/10/asun_3426616_20161013_1476464827.pdf, [Última Consulta 4 de Jan. 2019].

[88] "*El derecho a la identidades tanto un derecho en sí mismo como medio para acceder a los demás derechos que consagran las leyes y los tratados, ya que permite la individualización de cada persona, haciéndo la única e insustituible. A si mismo, la identidad permite establecer las posibles consecuencias de una conducta para su autor."* - **Iniciativa que adiciona diversas disposicionesdel Código Penal Federal, suscrita por la Dip. Lorena Corona Valdés (PVEM) e integrantes del grupo parlamentário del PVEM**, p. 1.

[89] "*El artículo 4o., párrafo octavo, de la Constitución Política de los Estados Unidos Mexicanos dispone en su parte conducente que "Toda persona tiene derecho a la identidad ..."* – p. 1.

seu respeito; a identidade digital pode ser composta por dados pessoais, cuja apropriação é potencialmente perigosa; o número de pessoas afetadas e perdas patrimoniais são cada vez mais elevadas; os crimes que regulam o acesso ilícito a equipamentos e sistemas informáticos não são suficientes, pois só acautelam a fase de obtenção de dados e não o seu uso[90]. A proposta também prevê que o crime se divida em duas fases essenciais, a obtenção e o uso dos dados[91], e que a proteção de ambas é fundamental para que não haja um vazio legal.

3. A insuficiência do quadro legal vigente em Portugal para criminalizar todo o fenómeno

Como já vimos, a apropriação indevida de identidade não constitui um crime autónomo no nosso ordenamento jurídico, contudo, vários são os crimes já existentes, quer no Código Penal, quer na Lei do Cibercrime, aos quais são subsumíveis grande parte, das atuações possivelmente constitutivas deste fenómeno. Torna-se então necessário perceber se estes vários crimes cobrem todo o espectro criminoso da apropriação indevida de identidade ou se há lesões – e quais – ainda desprotegidas e que carecem de tutela penal.

Na fase da obtenção de dados, os crimes a considerar – em conformidade com a análise feita no Capítulo II, ponto 1 – podem ser: furto (art.203º do CP); roubo (art.210º do CP); apropriação ilegítima em caso de acessão ou de coisa achada (art.209º do CP); burla (217º do CP); Falsidade informática (art.3º da LC); dano informático (art.4º da LC); acesso ilegítimo (art.6º da LC)ou interceção ilegítima (art.7º da LC). Na fase do uso de dados: qualquer das formas de falsificação de documentos correspondente à atuação criminosa (art.256ºss do CP); a Falsidade informática, mais uma vez; a difamação, injúria ou devassa da vida privada. Uma sentença coerente, segundo esta visão do fenómeno criminoso, passaria por condenar o criminoso em concurso efetivo entre o crime subsumível à forma de atuação que levou à obtenção de dados e o crime subsumível à forma de uso de dados, quando sejam diferentes.

---

[90] *"De la lectura de los preceptos transcritos se desprende que és tos unicamente sancionan la obtención ilícita de información, más no su uso que, por una parte, lesionaría la intimidad y sua poderamiento podría producir la usurpación o robo de identidad y, por otra parte, la conducta se realicecon el fin de obtenerun lucro indebido, por lo que a falta de regulación se dejaría sin protección el bien jurídico que se pretende tutelar con la presente iniciativa que es por un lado el patrimonio y por otro el derecho a la propiá imagen del titular de la identidad".* ***Iniciativa que adiciona diversas disposicionesdel Código Penal Federal, suscrita por la Dip. Lorena Corona Valdés (PVEM) e integrantes del grupo parlamentário del PVEM***, p. 1.

[91] "*La usurpación o robo de identidad se presenta cuando una persona se apropia indebidamente de los datos de otra persona para cometer un delito. Conducta que se realiza en dos pasos, el primero consiste enrobar la información de una persona; esdecir que una persona se apropia y utiliza de manera indebida los datos de otra persona sin sua utorización y, el segundo, en que quien robó la información o datos personales se hace pasar por esa persona ante terceros para cometer un delito, es decircon la información contrata productos y servicios financieros a nombre de la víctima*". ***Iniciativa que adiciona diversas disposiciones del Código Penal Federal, suscrita por la Dip. Lorena Corona Valdés (PVEM) e integrantes del grupo parlamentário del PVEM***, p. 2.

Por exemplo, alguém que recorre ao *phishing* e realiza compras online com os dados assim obtidos, devia responder pelo crime de dano informático, acesso ilegítimo ou interceção ilegítima (*phishing*) e pelo crime de falsidade informática (compras *online*), em concurso efetivo. O mesmo será dizer, que quem só praticou uma das fases, uso ou obtenção, só deverá ser condenado pelo crime correspondente. Por exemplo, quem envia emails fraudulentos com a intenção de obter dados de outrem, conseguindo fazê-lo, mas não chegando a dar uso a esses dados, só deve ser condenado pelo dano informático, acesso ilegítimo ou interceção ilegítima (dependendo do conteúdo e objetivo do email enviado), sendo que o simples ato de enviar emails, não chegando a produzir documentos não genuínos[92], ainda não preenche o tipo objetivo da falsidade informática (ainda não há resultado), nem tão pouco, o crime de falsificação de documento.

Parece, então, que o nosso Código Penal e Lei do Cibercrime já acautelam todas as condutas possíveis, mas será assim? A verdade é que nenhuma destas condutas, só por si, configura uma apropriação indevida de identidade. Como já dissemos, estamos perante algo muito mais complexo, a aparência de ser outra pessoa – o titular legitimo dos dados. Ora, se eu vou a uma loja e apresento o cartão de crédito de outra pessoa, ou que tem em si incorporados os dados de outrem, alguém me está a reconhecer como essa pessoa? Não nos parece que assim seja. Qualquer um de nós pode pegar no cartão de um amigo ou de um familiar e ir a uma loja efetuar um pagamento, nem por isso nos estamos a apropriar da identidade dessa pessoa. O ato de pagar, é um ato automático e que não gera, nas outras pessoas, a ideia de que, quem usa o meio de pagamento, é o seu necessário titular. Traduzindo isto para tipos legais: pode haver um furto, roubo ou apropriação ilegítima de um meio de pagamento e, consequente, uso, mas isso não significa que tenha existido uma apropriação da identidade do titular desse meio de pagamento. O mesmo se pode dizer do *phishing*, em determinada aceção. O facto de eu enviar um email, através do endereço de email falsificado paypalnet@paypalnet.com a pedir ao recetor desse email que atualize os dados da sua conta, não corresponde a uma apropriação de identidade. Primeiro porque, como já se explicou, há total liberdade para criar endereços de email e o facto de eu usar a palavra *paypal* não equivale a uma apropriação de identidade. Em segundo lugar, porque as pessoas coletivas não têm uma identidade passível de ser apropriada. Têm direitos, deveres e até responsabilidade civil e penal, mas não têm identidade – esta está reservada, unicamente, para pessoas singulares.

[92] Não cabe neste exemplo, o caso em que são feitas páginas falsas de *homebanking*. Aqui, como defendemos supra, já existe falsidade informática, devendo o agente ser condenado pelo crime de burla e falsidade informática, em concurso efetivo.

Por outro lado, o acesso ilegítimo à conta de email de alguém ou a uma sua rede social, para, dessa forma, conseguir os dados pessoais de outrem, já configura um caso de apropriação indevida de identidade. Também assim será, o uso de dados pessoais para criar uma página numa rede social e assim chegar a outras pessoas (*catfishing*). A falsificação de documentos (quer se trate de falsificação de documentos ou falsidade informática, de acordo com o critério definido *supra*) para conseguir pedir um cartão de crédito online, em nome de outra pessoa, também cria a aparência no recetor, de que se trata dessa pessoa. O mesmo se dirá para quem falsifica documentos e vai ao banco pedir um empréstimo habitação ou um crédito automóvel, com os dados de outra pessoa.

A apropriação indevida de identidade pode dar-se de muitas formas diferentes e só a análise casuística da atuação criminosa nos pode fazer concluir, se naquele caso específico, existiu ou não. É possível perceber que as formas de chegar a esta apropriação, já estão criminalizadas, então haverá razão para autonomizar esta atuação criminosa e criar um novo tipo legal penal? Consideramos que sim. Primeiro porque, os crimes apresentados e a apropriação indevida de identidade protegem bens-jurídicos diferentes, questão que focaremos a pormenor abaixo. Segundo, porque os crimes informáticos são, muitas vezes de difícil prova – é difícil provar que houve crime e as provas são de fácil manipulação e, por isso, muitas vezes, inadmissíveis. Nestes casos, em que não se consegue provar a existência do crime prévio – usando o exemplo do acesso ilegítimo ao email de alguém para chegar a outra pessoa – não resta nada. Se eu conseguir provar que a identidade de alguém foi usurpada, mas não de que forma, deve esta conduta ficar impune? Não nos parece. Podia-se argumentar, contra este raciocino, que haverá sempre uma burla, mesmo que não haja mais nada. Mas não é assim. A burla exige o prejuízo patrimonial[93] e, mesmo a existir este prejuízo, a vítima é quem sofreu o dano patrimonial e não a pessoa cuja identidade foi apropriada, para consegui-lo. Continuamos, portanto, com um vazio legal.

[93] "(...) a burla constitui um crime de dano, que só se consuma com a ocorrência de um prejuízo efetivo no património do sujeito passivo da infração ou de terceiro" – FIGUEIREDO DIAS, Jorge de (dir.) - **Comentário conimbricense do código penal: parte especial**, p. 276.

Capítulo III – A existência de margem constitucional para criminalização

1. A especial necessidade de intervenção do direito penal no contexto digital

"A Internet invadiu todos os sectores da vida do cidadão e do Estado. Como tal, tornou-se também um recurso valioso para aqueles que visam a prossecução de fins ilícitos."[94]

O termo cibercrime surgiu para designar a criminalidade cometida através de, ou com o auxílio, de um sistema informático[95] ou da Internet. Apesar de se poder considerar que a mera captura de dados informáticos (sem necessidade de movimentação de dados na Web) já é cibercrime[96], a verdade é que o surgimento da *World Wide Web (WWW)* em 1992 exponenciou o cibercrime[97], tornando-o num problema cada vez mais real e necessitado de uma resposta legal. As facilidades trazidas pela Internet, em todos os sentidos, provocam, não só um crescimento de delitos, mas também um aumento de criminosos[98]. A desnecessidade de confrontar fisicamente a vítima traz mais "coragem" para cometer este crime. Para além disso, com um mínimo conhecimento informático e acesso à *dark web*, torna-se quase certo o anonimato do autor.

A nossa intervenção, no que toca à apropriação indevida de identidade, deve ter especial incidência no contexto digital[99]. Primeiro, porque, atualmente, este é o contexto

---

[94] PINTO, Ana - **Investigação criminal com recurso a meios telemáticos: em especial, as buscas online e o agente infiltrado online**, Abstract.

[95] Utilizamos aqui a expressão sistema informático, por ser aquela que o legislador da LC entendeu ser a mais correta.

[96] Isto é, que a internet não é na verdade o único potenciador do cibercrime (nem o primeiro).

[97] "(...) as práticas e capacidades da informática, em particular, da internet, potenciam exponencialmente a internacionalização da criminalidade" - VENÂNCIO – Ob. cit., p.15

"Para a tão falada globalização contribuíram outros factores como as telecomunicações e as redes de transportes, mas foi com a Internet que nasceu a "sociedade global", caracterizada pela interligação mundial de computadores, redes e sistemas informáticos e telemáticos." - DIAS, Vera Elisa Marques – **A problemática da investigação do cibercrime**, p.4.

[98] "Estas "facilidades" têm gerado, por um lado, uma deslocação criminosa para a Web, fazendo com que cada vez mais pessoas se sintam tentadas a utilizar a internet para as suas práticas criminosas, ou mesmo a arriscar-se na consumação de crimes que por outros meios não praticariam" - VENÂNCIO – Ob. cit., p. 15;

"Todavia, as vantagens da internet que levaram a uma explosão de utilizadores e volume de circulação de informação, também levaram à multiplicação na penumbra de condutas lesivas e ilícitas, praticáveis e praticadas, na internet, ou por intermédio dela. Foi descoberto um campo fértil, vulnerável, de lucro fácil, com riscos físicos inexistentes, a baixo custo, e com uma grande probabilidade de impunidade, não só para o cometimento de novos delitos, como também para revisitar os crimes tradicionais, agora com a exponencial ajuda e cumplicidade da internet." - DIAS, Vera Elisa Marques – Ob. cit., pg. 5

[99] "A forte relação de dependência da sociedade da informação - e com tendência a aumentar – em relação às redes e sistemas informáticos, leva a que o cibercrime se torne cada vez mais frequente, diverso, móvel, internacional e perigoso, o que impõe um elevado grau de segurança, fiabilidade e eficiência, de modo a evitar que este crime se torne no almejado crime perfeito. Para tal é necessário que a sociedade de informação assente

privilegiado e quase exclusivo em que se comete esta atuação criminosa – a facilidade é maior e o risco é menor. No que toca à facilidade, não há dúvida que a internet trouxe meios técnicos que o tornam quase aliciante. O *homebanking*; as compras online; as redes sociais; o email; as agendas online (exemplo do Google Calendar), todos eles são fóruns onde guardamos cada vez mais informação – as nossas senhas, as nossas credenciais, os eventos do nosso dia-a-dia, onde estamos, para onde vamos. Por questões de funcionalidade e mobilidade, a nossa vida está a ser, gradual e exponencialmente, informatizada[100]. O reverso da nossa vida ter sido tão facilitada, contudo, é que se tornou muito mais suscetível de ser "roubada"[101]. Os ataques informáticos, não só aos nossos sistemas como aos sistemas que supostamente protegem as nossas informações (o nosso banco, a operadora de telecomunicações, a companhia de seguros); o *malware* (cavalos de troia, *worms*, vírus informáticos[102]), são formas cada vez mais eficazes e imprevisíveis de atacar os sistemas informáticos e, com eles, levar o que temos nos nossos computadores, o que, grande parte das vezes, é tudo. Tal como nos explicou SHERRY TURTLE, o anonimato é uma das características de como nos expressamos online e isto é verdade tanto para nós, como para os criminosos – reduzindo o risco de ser detetado[103].

Segundo, porque as formas através das quais esta atuação pode ser cometida, no mundo físico, estão suficientemente acauteladas. Atentemos nos seguintes exemplos: a) alguém que encontra/furta/rouba os documentos de identificação de outra pessoa e passa a usá-los como seus; b) alguém que consegue os dados de identificação de outrem (seja por que forma for) e vai a uma instituição de crédito pedir um empréstimo, com documentos

---

numa segurança informática que assegura a confidencialidade, a integridade e a disponibilidade fiável dos sistemas." - DIAS, Vera Elisa Marques – Ob. cit., 5

100 "Nos dias de hoje, com especial incidência nos países mais desenvolvidos, a internet tem um papel fulcral ao nível de todas as infraestruturas estratégicas e nevrálgicas do país, como governamentais, militares, de segurança, económicas, de telecomunicações, de transportes, educacionais, energéticas, de saúde e serviços de socorro e emergência. Mas a sua importância não se fica por aqui pois estende-se a todo o tipo de relações, como as comerciais, negociais, empresariais, financeiras e económicas, e com o nascimento das redes sociais, blogues e fóruns, passou a fazer parte da vida social, pessoal e dos tempos livres dos utilizadores." - DIAS, Vera Elisa Marques – Ob. cit., p. 4

101 "Tendo também que se ponderar e prevenir o perigo (...) de se conseguir obter, através da articulação de ficheiros, uma imagem completa da pessoa capaz de identificar todos os seus movimentos, os seus bens, as suas doenças, as suas crenças, em suma, todos os espaços mais recônditos da sua vida privada e pessoal." – MIRANDA/ MEDEIROS – Ob. cit., p.789.

102 "(...) Podemos referir o *cracking, phreaking, cracking of passwords, identity theft, data diddling, trojan horse, trap doors, between-the-lines entry, bitknapping, pharming, SMiShing, vishing, web defacing, phatbot, trojan horses, botnets, worms, hijackers, keylogger, spyware*, bomba lógica ou programa-*crash* e virus vários." - DIAS, Vera Elisa Marques –Ob. cit., p.6

103 "O anonimato é muito apreciado nas redes, poder navegar, visitar e conversar sem ter de se identificar. Contudo, este anonimato quando sai do âmbito do direito à reserva da vida privada e entra na impossibilidade de punição dos actores dos actos ilícitos é abdicável. (….) Podem, assim, os cibercriminosos diminuir ou eliminar o risco de ser descoberto ou condenado, apagando todas as provas do ciberrastro." - DIAS, Vera Elisa Marques – Ob. cit., p.16

falsificados que contêm esses dados. No exemplo a), há várias hipóteses de punir o criminoso: por furto; roubo ou apropriação ilegítima em caso de acessão ou de coisa achada – dependendo de como foram obtidos os documentos. Mesmo que não se consiga provar que quem usou o documento é quem o obteve, haverá ainda a hipótese, nos casos subsumíveis à norma, de aplicar o art.261º do CP – uso de documento de identificação ou de viagem alheio. Portanto, quer no momento de obtenção do documento, quer, aquando do seu uso, há normas jurídicas que protegem o titular. Em qualquer um dos casos, o titular pode constituir-se como assistente, durante o processo, sendo o agente passivo direto destas normas[104]. No exemplo b), mesmo que os dados tenham sido obtidos online, como a falsificação se concretiza em documentos físicos, há sempre a opção de imputar um crime de falsificação ou contrafação de documento. Isto significa que, mesmo que seja impossível provar a origem da obtenção dos dados (o que acontece muitas vezes), quando estes são usados e suscetíveis de causar dano, as normas do Código Penal abrangem qualquer situação.

Terceiro, porque a investigação criminal apresenta graves dificuldades no cibercrime e, consequentemente, na apropriação indevida em meio digital. O referido anonimato faz com que, na maior parte das vezes, o autor do crime seja não identificado e dificilmente identificável. Já para não falar da questão, tão debatida, do caráter transfronteiriço do cibercrime. Os crimes perpetrados através dos sistemas informáticos são considerados pela doutrina como transfronteiriços e atemporais[105], i.e. os ataques podem ser feitos de qualquer parte do mundo para qualquer parte do mundo (no caso da apropriação indevida, é possível obter os dados de um servidor americano, por exemplo e usar os dados em Portugal, ou obter os dados e usá-los internacionalmente, mas através de um sistema informático com base em Portugal). Esta característica, aliada às normas do nosso sistema jurídico, levam a situações complicadas, como seria o caso de alguém cujos dados são "roubados" e utilizados fora de Portugal, não havendo uma queixa apresentada pelo ofendido (sendo que o titular dos dados não é visto como ofendido, mas tão só aquele sobre o qual a atuação fraudulenta recai, i.e., o "destinatário" da identidade falsa), o titular nada poderá fazer para se defender. Ou, ainda, não se sabendo quem é autor dos factos ou onde se encontra o autor, não haveria fator de conexão ao ordenamento jurídico português, nos termos do art.4º do CP – não se sabe onde é que o agente atuou, não havendo lugar à aplicação do principio da territorialidade, e o resultado típico da mera obtenção dos dados dificilmente se conseguirá

[104] "Considera-se ainda que o crime de falsificação de documentos para além de ser um crime contra a prova documental é também um crime de fraude contra a identidade do autor do documento" – FIGUEIREDO DIAS, Jorge de (dir.) – **Comentário conimbricense…**Ob. cit., p. 681.

[105] *Vide* DIAS, Vera Elisa Marques – Ob. cit., pp.13 a 15.

provar. Pelo contrário havendo responsabilização pelo mero uso de dados, facilmente haveria conexão, através da aplicação do princípio da nacionalidade – art.5º, nº1, al. b) do CP. Numa tentativa de resolução deste problema, a LC consagrou no seu artigo 27º regras especificas de aplicação da lei penal portuguesa, devendo-se dar especial atenção às regras da alínea c) e d), do nº1, segundo as quais a lei portuguesa se aplica quando os crimes sejam fisicamente praticados em território português, independentemente de visarem sistemas informáticos fora deste (alínea c)), ou sejam atingidos sistemas informáticos localizados no território nacional, mesmo que o facto não tenha sido aqui praticado (alínea d))[106]. Estas duas regras justificam-se pelo caráter transfronteiriço destes crimes, resolvendo algumas das situações referidas.

A atemporalidade resulta do facto de estes ataques muitas vezes se prolongarem no tempo, sendo concretizados de forma faseada[107]. Por exemplo, o agente obtém os dados, mas só os usa passado meio ano, ou um ano, dificultando ainda mais a investigação sobre a forma como foram obtidos os dados. Ambas as características dificultam visivelmente a investigação criminal, exigindo cooperação internacional – com todas as dificuldades burocráticas e políticas inerentes ao processo - e são mais um argumento que justifica a criminalização do uso de dados, mesmo (e apesar de) não se conseguir apurar a ilegalidade da sua obtenção. Focamos aqui a obtenção *vs* uso dos dados porque estas duas condutas são visivelmente diferentes em termos de efeitos e consequente possibilidade de investigação. Quando alguém obtém dados o rasto informático é muito menor do que quando os dados são usados. Usar dados implica uma conduta ativa e continua do agente. Por exemplo, num esquema de *catfishing*, a ação é continuada, para eu conseguir ludibriar alguém, fazendo-o acreditar que eu sou o titular de certos dados e levando-o a partilhar comigo seja o que for que eu queira, tenho de manter um perfil online ativo, durante algum tempo - há uma possibilidade de chegar a mim, passo de ser só emissor a ser também destinatário e aí a vulnerabilidade aumenta. Na obtenção de dados não. Eu obtenho os dados e nesse mesmo segundo fico offline se assim quiser, espero e só mais tarde ajo sobre isso, tornando a hipótese de chegar a mim muito mais remota.

[106] Havendo vários Estados competentes, será de recorrer aos órgãos e mecanismos da União Europeia de forma a dirimir o conflito – art.27º/2 da LC

[107]Há ainda a questão do prazo no qual as vítimas descobrem que os seus dados foram objeto destas condutas. FOLEY descobriu que mais de metade das vítimas só descobrem nos três meses seguintes e um quarto das vítimas só se apercebe até dois anos depois do facto (*Apud* WHITE/ FISHER – Ob. cit., p.8). SYNOVATE chegou à conclusão de 40% das vítimas não reporta o crime e só um quarto faz denuncia às autoridades (*Apud* WHITE/ FISHER – Ob. cit., p.9).

O facto de ser um "crime" relativamente novo (na sua vertente digital) e altamente complexo[108], sobre o qual ainda temos pouca informação, pouca jurisprudência e doutrina torna a resposta policial, a intervenção do legislador e o trabalho dos tribunais mais complicado e dúbio. O ritmo com que as coisas acontecem e sofrem mutações no mundo digital é sofrivelmente acompanhado pela lei e pela jurisprudência. Por todos os motivos enunciados, parece-nos urgente a intervenção na obtenção de dados em ambiente digital, razão pela qual defendemos que, a haver uma incriminação, esta deveria incluir-se na Lei do Cibercrime, complementando os tipos legais já existentes de obtenção de dados.

2. A existência de bem jurídico dotado de dignidade penal

> "Verifica-se, portanto, a pouco e pouco, um fenómeno de crescente captura silenciosa da identidade pessoal de cada um, com um potencial lesivo, direto ou indireto, quase ilimitado"[109]

A haver uma incriminação autónoma desta atuação criminosa terá de haver um bem-jurídico que a justifique. Na nossa opinião, este será a autodeterminação informacional. Num mundo em que a informação é, cada vez mais, um bem precioso e de fácil divulgação, é necessária uma proteção acrescida desta informação, quando relacionada com a identidade pessoal. Sendo a identidade um direito fundamental, com todas as consequências que isso implica e sendo esta constituída pelos nossos dados pessoais, há que haver um controlo efetivo sobre estes dados e uma tutela direcionada ao seu titular.

O direito à autodeterminação informacional é extraível de dois preceitos essenciais da CRP – o art.26º, tacitamente e o art.35º, expressamente. O artigo 26º, já referido no início deste trabalho, consagra o direito à identidade, em conjunto com outros direitos pessoais, como o desenvolvimento da personalidade, a cidadania, o bom nome, entre outros. Todos estes direitos são, além de uma expressão do princípio da dignidade humana, extensões do direito à identidade de cada um de nós, pois é ele que nos permite ser detentores de direitos e deveres em sociedade. Para lá destes direitos expressamente referidos, são reconhecidos outros não tipificados na **Constituição Portuguesa Anotada**, nos quais se inclui o direito

[108] "Ora, a sua descodificação e manipulação de programas, a identificação do infractor, a busca do rasto das operações informáticas e de toda a trama maliciosa, e a recolha de provas digitais aceitáveis em julgamento impõem uma alta tecnicidade ao investigador, dificultando tanto a investigação como a prova, o que aumenta a probabilidade de impunidade" - DIAS, Vera Elisa Marques – Ob. cit., p. 17

[109] TEIXEIRA, Guilherme da Fonseca – Identidade e autodeterminação informacional no novo Regulamento Geral da Proteção de Dados: a inevitável privatização dos deveres estatuais de proteção, p. 13.

à autodeterminação informacional[110]. O art.35º da CRP, por outro lado, já consagra expressamente este direito[111], apesar de só o fazer na vertente digital. À primeira vista esta escolha poderia parecer insuficiente, tendo em conta que a autodeterminação informacional não se destina só a dados informáticos, destina-se a qualquer dado pessoal, independentemente do seu suporte. No entanto, e tal como explicamos no ponto anterior, a informática é, de facto, o que justifica a crescente preocupação e regulamentação no que diz respeito aos dados pessoais[112]. É, pois, nesta área, que mais faz sentidos exigir mecanismos de tutela efetivos que protejam a "captura silenciosa"[113]. Este direito, tal como consagrado no art.35º tem uma dupla vertente: negativa, na medida em que "possibilita ao individuo a negação de informação pessoal, bem como a possibilidade de que ele se oponha à sua recolha e consequente processamento"[114]; positiva por ser "a realização de um direito de autodeterminação informacional a qual pressupõe não só uma liberdade de atuar sobre as informações prestadas, como também o conhecimento necessário do uso que entidades façam dos dados por si disponibilizados"[115]. Reforça esta ideia RIBEIRO DE FARIA, ao dizer que este conteúdo negativo dá o direito de escolher que informações ocultar, independentemente de poderem ser bem ou mal vistas pela comunidade. A faceta positiva está expressa nas faculdades consagradas nos vários números deste art.35º[116]. Entende-se que este direito deve ser autonomizado porque o acesso a dados pessoais permite formar um perfil de alguém e restringir grandemente a sua liberdade[117], correspondendo à nossa ideia de

[110] MIRANDA/ MEDEIROS – Ob. cit., p. 608.

[111] "Na verdade, talvez visando, apenas, introduzir medidas de segurança no domínio informático, o legislador constitucional acabou por consagrar o direito à proteção de dados enquanto direito à identidade e autodeterminação informacional, que assume uma vertente ativa de titularidade do poder de controlo sobre os seus próprios dados pessoais (...)" - TEIXEIRA, Guilherme da Fonseca – Ob. cit., p.20.

[112] "Enquanto a proteção de dados é pensada como uma garantia, o seu fundamento, ou seja, a autodeterminação informacional, exprime-se como uma liberdade" SOUSA PINHEIRO, José Alexandre Guimarães de – Ob. cit., p. 944

[113] "(...)no sentido da tutela efetiva da dignidade da pessoa humana em face da sociedade atual de reconhecido risco tecnológico, o que não se coaduna com a limitada vertente (historicamente) passiva como é concebido o direito à privacidade, que meramente habilita o titular do direito a excluir terceiros, sejam entidade privadas ou públicas, da sua esfera de intimidade." - TEIXEIRA, Guilherme da Fonseca – Ob. cit., p.20

[114]NETO, Luísa/ LEÃO, Anabela, coord. - **Constituição anotada: obra colectiva de estudantes da Faculdade de Direito da Universidade do Porto no âmbito das comemorações dos 10 anos da Faculdade e dos 30 anos da Constituição da República Portuguesa de 1976**, p.139

[115] NETO, Luísa/ LEÃO, Anabela, coord. – Ob. cit., p.140.

[116] MIRANDA/ MEDEIROS – Ob. cit., p. 789.

[117] "Uma vez que a partir do tratamento informatizado de dados pessoais é possível construir uma determinada imagem ou perfil da pessoa, e uma vez que o uso desses elementos pode condicionar ou restringir fortemente a sua liberdade, deve fazer parte dos direitos fundamentais de cada um a possibilidade de controlar e de decidir por si quando, e em que condições, se usarão, ou se tornarão públicas, informações que lhe digam respeito" – MIRANDA/ MEDEIROS – Ob. cit., p. 784.
Da mesma forma, SOUSA PINHEIRO – Ob. cit., p.950 "(...) a Ciência Jurídica foi confrontada com novos factos que colocavam em crise a vida privada e elementos de identificação pessoais que, agregados por via computacional, podem expor por completo a personalidade de uma pessoa".

que os dados pessoais são a exteriorização da nossa identidade[118], o que, na nossa opinião, é o mesmo que dizer que este direito é a forma de tutela da nossa identidade social, de todo o conjunto de informações que fazem a sociedade reconhecer-nos enquanto parte integrante. Não nos parece que este direito seja tanto relacionado com a esfera íntima da vida de cada um, como defendem alguns autores[119], mas sim ao direito à identidade pessoal, que inclui o direito de ninguém se apropriar dela ou manipulá-la a seu favor[120]. Até porque, se o fim do direito fosse meramente a intromissão de outros na vida privada e íntima de cada um, não faria sentido abranger aqui informações de cariz público acessíveis a cada um, como o nosso registo criminal ou grau académico, por exemplo. Trata-se de um real direito, não só de não divulgar certos dados, como de garantir que os que são divulgados, são verdadeiros[121].

Sendo certo que a autodeterminação informacional é um direito fundamental, reconhecido pela CRP e pela doutrina como tal, será este um bem jurídico com dignidade jurídico-penal? Segundo FIGUEIREDO DIAS, este só existe "onde se encontre refletido num valor jurídico-constitucionalmente reconhecido em nome do sistema social total e que, deste modo, se pode afirmar que "preexiste" ao ordenamento jurídico penal"[122]. isto significa que um bem jurídico dotado de dignidade penal terá sempre de espelhar um direito fundamental, ainda que implicitamente[123]. O que, de resto, é confirmado pelo art. 18º/2/1ª parte da CRP[124]. O reconhecimento deste direito como um bem jurídico penal exige que este não configure uma mera violação moral, pois estas "não conformam como tais a lesão de um autêntico bem jurídico e não podem, por isso, integrar o conceito material de crime"[125]

---

[118] Já afirmava SOUSA PINHEIRO que "o que está em causa não são "dados" ou a sua "proteção", mas a pessoa" – Ob. cit., p. 967.

[119] MIRANDA/ MEDEIROS – Ob. cit., pp.785 e 786.

[120] Em sentido semelhante: "(...) abrange todos os poderes e faculdades que permitem garantir que a pessoa não é usada como fonte de informação para terceiros contra a sua vontade, podendo além disso controlar a informação que é fornecida e os termos de abrangência em que ela é tratada" – MIRANDA/ MEDEIROS – Ob. cit., p. 786.

[121] Por isso é que no novo RGPD se prevê quer a proibição geral de tratamento de certas categorias de dados (art.9º); como o direito de oposição (art.20º), mas, também, o direito a pedir a correção dos seus dados (art.16º).

[122] FIGUEIREDO DIAS, Jorge de – **Direito Penal: Parte Geral**, p.120.

[123] "Pois enquanto os crimes do direito penal de justiça se relacionam em último termo, directa ou indirectamente, com a ordenação jurídico-constitucional relativa aos direitos, liberdades e garantias das pessoas, já os do direito penal secundário (...) se relacionam essencialmente com a ordenação jurídico constitucional relativa aos direitos sociais e à organização económica." – FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p.121. Da mesma forma se pronuncia o STJ no Ac. de 27 de Abril de 2011, Proc. 456/08.3GAMMV, Rel. Henriques Gaspar: "A expressão da dignidade penal e da carência de tutela penal para determinados bens resulta da ordenação axiológica jurídico-constitucional, no sentido de que só bens jurídicos de valor constitucional podem ser legitimamente protegidos pelo direito penal".

[124] "Determina-se, assim, (...) uma primacial independência dos direitos, liberdade e garantias relativamente à atividade (ou inatividade) do legislador ordinário. E prescreve-se, em simultâneo, um âmbito alargado de vinculatividade subjetiva dos mesmos direitos, que abrange positiva e negativamente todos os sujeitos e poderes públicos, independentemente das suas formas concretas de atuação, assim como os próprios sujeitos jurídicos privados nas relações que estabelecem entre si." – MIRANDA/ MEDEIROS – Ob. cit., p.316.

[125] FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p.124.

ou a defesa de uma proposição meramente ideológica. A violação deste direito não se reflete numa mera amoralidade perante a sociedade ou ideologia social[126], reflete-se sim numa verdadeira lesão de um direito fundamental, capaz de gerar danos reais na vida dos seus titulares e ofensiva de direitos pessoais e patrimoniais conexos[127], como a reputação, imagem, reserva da intimidade da vida privada e familiar e até, em casos extremos, da liberdade – todos eles direitos fundamentais, expressamente reconhecidos. A criminalização também não pode ter como motivo a "violação de valores de mera ordenação social", pois esta seria resultado da violação de um bem jurídico-administrativo e não jurídico-penal. neste caso, não existe uma obrigação prévia de criminalização, por ser o bem jurídico "construído através da proibição e por força dela"[128]. Não é o caso aqui. A adesão ao direito penal do bem jurídico já foi demonstrada pela jurisprudência no Ac. do TC 211/95, segundo o qual a criminalização penal se justifica pela censurabilidade e gravidade ética de certas condutas, que demonstra a sua prévia normatização jurídica e claro, pela necessidade da pena, i.e., a "lógica de estrita necessidade das restrições de direitos e interesses que decorrem da aplicação de penas públicas". São, portanto, dois os elementos essenciais que compõe o conceito material de crime tal como definido por FIGUEIREDO DIAS e pelo TC: a existência de uma bem-jurídico com dignidade penal e a necessidade de tutela penal. Provada que está a existência de um bem jurídico dotado de dignidade jurídico-penal – a autodeterminação informacional – resta perceber se este bem carece de tutela penal.

3. A carência de tutela penal

O estudo de direito penal mostra-nos, em primeira linha, que este é um ramo do direito em que a interferência estatal leva a uma especial restrição de direitos, liberdades e garantias dos cidadãos, por isso mesmo, deve ser sempre usado como última *ratio*[129]. Isto implica que a criminalização de uma conduta seja sempre feita de forma subsidiária, quando os restantes instrumentos se mostrem desadequados ou insuficientemente protetores dos bens jurídicos

[126] O autor oferece como exemplos excluídos do conceito de bem jurídico, por serem meras violações morais, a criminalização da homossexualidade e prostituição e como exemplos de proposições meramente ideológicas, a propagação de doutrinas contrárias a uma certa religião ou determinada conceção do Estado – FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., pp.124 e 125.

[127] "a autodeterminação informacional reveste natureza de posição jurídica complexa, abrangendo elementos próprios das diferentes posições activas – direitos, liberdades, garantias, poderes – que compõem os direitos fundamentais" – SOUSA PINHEIRO – Ob. cit., p.944.

[128] FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., pp.126.

[129] "Ora, o direito penal apenas intervém na regulação e resolução de litígios emergentes na comunidade como última *ratio*, ou seja, quando a lesão de bens jurídicos assume uma gravidade justificativa da intervenção do sistema jurídico e da justiça na limitação da liberdade individual." – Ac. do TRC de 11 de Março de 2009, Proc. 36/03_3GCTCS.C1., Rel. Fernando Ventura.

em causa[130]. Esta especial natureza do direito penal é o que justifica o critério designado pela doutrina e jurisprudência como necessidade ou carência de tutela penal, consagrado no art.18º, nº2, 2ª parte da CRP. Sendo este critério uma concretização do princípio constitucional da proporcionalidade, a criminalização de uma conduta terá sempre de atender aos seus três subprincípios: adequação; exigibilidade e proporcionalidade em sentido estrito. A adequação exige que a restrição dos direitos fundamentais em causa seja a mais indicada para proteger determinado bem jurídico. A exigibilidade concretiza-se quando aquele meio é necessário para alcançar o fim em vista, por não haver outra medida que alcance o mesmo fim. O último subprincípio deve confirmar os dois primeiros, na medida em que considere que os fins não estão a ser alcançados de forma desproporcionada ou excessiva[131]. Associado ao critério de necessidade da pena, surge o princípio da não-intervenção moderada, postulando que o Estado, enquanto criador da política criminal, deve interferir o menos possível e agir apenas quando absolutamente necessário[132]. Contudo, valores inversos também existem, valores esses que impõe uma proteção efetiva dos direitos fundamentais e dos bens jurídicos por estes tutelados, através de um dever de concretização das imposições constitucionais expressas nas normas relativas a estes direitos[133]. Uma análise adequada da existência (ou não) de carência penal, terá sempre de considerar os dois "lados da moeda": primeiro, que se trata de um bem jurídico, tutelado por um direito fundamental que merece uma proteção apropriada; segundo, que a sua proteção pode implicar a desproteção ou, mesmo, a anulação de outros direitos fundamentais (como a liberdade). Implica, resumindo, uma cuidada ponderação entre os direitos fundamentais em jogo.

Impõe-se, então, a questão de saber se a conduta em estudo é, para além de censurável, adequada e necessariamente controlável pela lei penal[134]. A facilidade do cometimento desta

---

130 "A violação de um bem jurídico-penal não basta por si para desencadear a intervenção, antes se requerendo que esta seja absolutamente indispensável à livre realização da personalidade de cada um na comunidade. Nesta precisa aceção o direito penal constitui, na verdade a última *ratio* da política social e a sua intervenção é de natureza definitivamente subsidiária." FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p. 128.

131 Cfr. Ac. do TC de 23 de Dezembro de 2008, Proc. 977/2008, Rel. Maria Lúcia Amaral; Ac. do TRC de 17 de Janeiro de 2013, Proc. 282/11.2TTCVL.C1, Rel. Jorge Loureiro.

132"(...) o Estado e o seu aparelho formalizado de controlo do crime devem intervir o menos possível; e devem intervir só na medida requerida pelo asseguramento das condições essenciais de funcionamento da sociedade. A esta proposição se dá o nome de princípio da não-intervenção moderada" – FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p. 131.

133 "Negativamente, os órgãos legislativos começam por ficar impedidos de emanar normas que sejam materialmente incompatíveis ou desconformes com a letra ou com o espírito das normas constitucionais consagradoras daqueles direitos (...) Depois, positivamente, fica o legislador adstrito a um conjunto diversificado de deveres específicos de atuação (...)" – MIRANDA/ MEDEIROS – Ob. cit., p. 326.

134 "A carência de tutela penal analisa-se, assim, num duplo e complementar juízo: em primeiro lugar, um juízo de necessidade, por ausência de alternativa idónea e eficaz de tutela não penal; em segundo lugar, um juízo de idoneidade do direito penal para assegurar a tutela, e para o fazer à margem de custos desmesurados no que

conduta, em meio digital, leva a que só o direito penal se mostre como adequado para proteger o bem jurídico ofendido. Efetivamente, proteger a autodeterminação informacional por meios civis ou contraordenacionais, leva a que as vantagens de levar a cabo qualquer conduta de apropriação de dados, sejam muito superiores às desvantagens. Sendo a apropriação de dados, tendencialmente, um crime meio para atingir um outro fim, seja o benefício patrimonial, seja a ofensa à honra e sendo o meio mais eficaz para chegar ao resultado pretendido, a imposição de uma coima, por exemplo, não será suficiente para dissuadir o agente. A facilidade em obter os dados de terceiros e usá-los, de forma praticamente anónima, significa um risco quase nulo para o agente, que só irá ser dissuadido do crime se confrontado com a possibilidade de uma restrição à sua liberdade. O mundo informático ainda é visto como um mundo sem lei, uma espécie de "faroeste do mundo moderno"[135], onde não há consequências e isso só irá mudar quando o direito penal mostrar que não é assim. Todos os argumentos usados para incriminar as formas de obtenção de dados online, serão de aplicar aqui, concretizando o princípio legal *a minori, ad maius*[136]. Afinal se há carência de pena para a fase de obtenção, haverá ainda mais para a fase de uso, pois é essa que irá provocar danos reais na esfera do titular dos dados e/ou do "destinatário" da identidade falsa – aquele que será confrontado com a identidade falsa, criada através dos dados obtidos de forma ilegítima. No que toca à idoneidade do direito penal assegurar a cessação ou, pelo menos, a diminuição desta conduta, cremos que se verifica. De facto, não se trata só de as restantes alternativas se mostrarem insuficientes, mas, também, de esta ser a única alternativa com força suficiente para se tornar efetiva. O direito penal só pode ser efetivo quando a ameaça de prisão supere a vantagem que poderá ser obtida. Neste caso, é nossa opinião, que a criminalização desta conduta será o único meio capaz de travar o comportamento criminoso. Poder-se-ia argumentar que a sanção – perda de liberdade – é excessiva face à (eventual) conduta típica – utilização de dados de terceiro -, o que não nos parece verdade. A utilização de dados pode ter, como já vimos, resultados catastróficos na vida de alguém, desde não conseguir empréstimos, passando por não conseguir emprego e, até, à restrição de liberdade, quando a utilização de dados resulta na existência de cadastro em nome de alguém que nada fez. As consequências pessoais, familiares, profissionais,

toca ao sacrifício de outros bens jurídicos, máxime a liberdade." Ac. do TC de 13 de Fevereiro de 2001, Proc. 166/2001.

[135] "A elevada cifra negra neste tipo de criminalidade tem como causas a falta de denúncia, a grande tecnicidade, a deficiente segurança, a falta de meios de detecção e controlo adequados, a falta de prevenção e a diminuta percentagem de detecção e condenação. Tal leva ao nascimento de um sentimento de impunidade em relação a estes crimes" - DIAS, Vera Elisa Marques – Ob. cit., p. 18.

[136] i.e. A lei que proíbe o menos, também proíbe o mais.

patrimoniais e de imagem são muitas e serão cada vez mais e mais graves, com a continua informatização da sociedade. Quanto mais cedo o legislador se aperceber disto e atuar em conformidade, maiores serão as possibilidades de diminuição e prevenção deste tipo de atuações.

Cremos, portanto, que a apropriação indevida de identidade protege um bem jurídico dotado de dignidade penal – a autodeterminação informacional – que estará cada vez mais em perigo na sociedade digital em que vivemos e que merece, por isso, uma tutela progressivamente acrescida. A imposição de sanções penais não só se mostra adequada, como necessária para tentar impedir a vaga de obtenção e utilização de dados que tanto tem crescido nas últimas décadas. Somente uma proibição de todas as fases (obtenção e utilização dos dados), poderá ter um resultado efetivo na tentativa de controlo deste fenómeno. A informática é a maior ferramenta criminosa de todos os tempos e exige, como nunca antes, que o legislador pense à frente do seu tempo.

Capítulo IV – A eventual criminalização da apropriação indevida de identidade

1. O tipo objetivo

Sabendo nós que a apropriação indevida de identidade consiste na utilização, sem consentimento dos dados de outrem e que o bem jurídico a proteger seria, aqui, a autodeterminação informacional, resta-nos concretizar esta ideia, oferecendo uma sugestão para a eventual criminalização desta atuação. Há que determinar qual seria o (possível) tipo objetivo mais adequado; perceber se deveriam existir agravações e quais; efetivar o tipo subjetivo e mostrar qual o grau de lesão do bem jurídico exigido. Vamos, desde já, deixar a nossa sugestão completa daquela que poderia ser, em nossa opinião, uma formulação indicada e adequada do tipo legal, passando depois a explicar detalhadamente a escolha e o porquê desta formulação concreta.

Apropriação indevida de identidade

1. Quem, com intenção de provocar engano e sem consentimento, utilizar dados informáticos pessoais de terceiro, apresentando-se como seu titular, é punido com pena de prisão até três anos ou com pena de multa.

2. A pena de prisão é de até cinco anos se:

a) Desse modo provocar prejuízo patrimonial ao titular ou a terceiro;

b) Desse modo divulgar dados relativos à intimidade da vida privada e familiar do titular ou de terceiro.

O tipo objetivo deste crime (tal como entendido para nós) é constituído pela descrição da conduta típica e respetiva sanção, no nº1, e pelas agravações de punição, quando a conduta é levada a cabo de certa forma ou quando haja determinado resultado, no nº2 – existindo três hipóteses de agravação, as quais passaremos a expor *infra*. Como já havíamos referido, este crime seria de integrar na Lei do Cibercrime, especificamente, no seu Capítulo II – Disposições penais materiais, estando inteiramente sujeito às definições e regras processuais da mesma e, subsidiariamente, às do Código Penal.

O nº1, começa a sua formulação com o típico "Quem", referindo-se ao agente da atuação criminosa, que pode ser pessoa singular ou coletiva (nos termos do art.9º da LC) – pese embora, a apropriação indevida de identidade só possa recair sobre os dados pessoais de

uma pessoa singular, o crime pode ser cometido quer por pessoas singulares, quer por pessoas coletivas, através dos seus representantes. Trata-se, pois, de um crime comum, podendo ser cometido por qualquer pessoa, não há necessidade de uma qualidade específica do agente. Dois elementos típicos e necessários da atuação criminosa serão a "intenção de provocar engano" e a falta de consentimento. É a intenção de provocar engano que transforma o simples uso de dados numa apropriação de identidade, através da intenção de criação da ilusão na contraparte, de que a pessoa que se apresenta com aqueles dados, é o seu legitimo titular. É, portanto, elemento constitutivo, tal como no crime de burla, "a) - o emprego de astúcia pelo agente"[137]. Sendo este um dos elementos do crime, defendemos, tal como tem defendido alguma doutrina para o crime de burla, que só haverá comissão por ação e não por omissão[138]. Não bastará o convencimento (a existir) noutra pessoa de que os dados pertencem a alguém que de facto não é o seu titular, só porque este não o nega. É necessária uma conduta ativa que se mostre adequada a convencer outra pessoa de que assim é, através da astúcia do agente, facilitada pelos meios informáticos hoje disponíveis. Já não é elemento, contudo, "b) - o erro ou engano da vítima devido ao emprego da astúcia", uma vez que o resultado não é de verificação necessária. Pela mesma razão, também não constitui, nexo causal[139] entre a atuação do agente e o resultado, tão só, elemento subjetivo especial do tipo, mas disso falaremos no ponto três. A falta de consentimento do titular dos dados é elemento essencial deste crime, pois é aquilo que torna a apropriação indevida. Se o titular consentir o uso dos dados, nos termos do art.38º do CP, não existe nenhum uso de dados não autorizado, logo não existe crime. Enquanto titular de dados, é me possível autorizar o uso desses dados, para fins contratuais, por exemplo. No entanto, esta autorização é dada para fins específicos – recordamos que o direito à autodeterminação informacional inclui não só o direito de escolher dispor ou não dos meus dados, como de escolher de que maneira e

[137] Ac. do TRE de 20 de Maio de 2014, Proc. 1915/13.1TASTB.E1, Rel. Alberto João Borges.

[138] Ao exigir que o erro ou engano que determina a acção do ofendido seja astuciosamente provocado pelo agente, o legislador parece, numa primeira análise, ter excluído a possibilidade de omissão, aparentemente incompatível com a conduta activa que a descrição típica enuncia. Esse procedimento astucioso ou fraudulento faltará completamente quando a conduta imputável ao agente seja precisamente a falta de acção, ou, por outras palavras, o aproveitamento de um estado de erro do ofendido não provocado por actos «positivos» do agente." – Ac. do STJ de 18 de Junho de 2008, Proc. 08P901, Rel. Maia Costa.

[139] Tal como no crime de Burla "a acção enganadora (astúcia do agente) tem de ser a causa do erro (engano)" – Ac. do TRP de 19 de Fevereiro de 2014, Proc. 529/11.5TABGC.P1, Rel. José Carreto. Diferentemente da Burla, aqui não existe um duplo nexo causal, pois o resultado da conduta é a mera ilusão da outra parte de que os dados estão a ser usados pelo seu titular, não sendo exigido aqui um fim específico a atingir através do engano, como o prejuízo patrimonial.

para que finalidades são utilizados -, sendo que todo o uso que extrapole os fins contratados ou acordados, já será tido como sem consentimento[140].

A utilização de dados pode ser feita de qualquer forma ou por qualquer meio (correio eletrónico; chamada telefónica; *sms*; redes sociais), não havendo nenhuma vinculação na ação. Importante é que esse uso seja o meio para o agente se fazer passar pelo titular dos dados. A palavra utilização significa tornar algo útil, sendo aqui os dados a ferramenta (utilidade) que dá credibilidade à apropriação indevida de identidade. O conceito de dados pessoais será aquele que integra o conceito de ciberidentidade tal como definido no ponto 2 do Capítulo I. De forma clara e resumida, este conceito coincide com o do RGPD – "informação relativa a uma pessoa singular identificada ou identificável" – por imperativo do art.35º da CRP que introduz expressamente o bem jurídico autodeterminação informacional e remete a definição do que são dados pessoais para esta lei. São, portanto, dados pessoais para a CRP, para o RGPD e o que nos interessa nesta formulação legal, quaisquer dados, independentemente da sua natureza, que sejam reconduzíveis a uma certa pessoa[141]. Não releva o suporte originário dos dados, físico ou informático, desde que a apropriação seja feita em meio digital, através do uso desses dados. Segundo a definição do art.2º, alínea b) da LC, dados informáticos serão todos aqueles suscetíveis de processamento num sistema informático, pelo que independentemente da origem, importante é que estes estejam integrados no mundo digital, tendo uma representação visível para qualquer destinatário. Os dados serão sempre de terceiro, de alguém[142] que não o agente da atuação criminosa. Isto significa que no caso de alguém que usa os seus dados, criando uma personalidade diferente ou que cria uma *persona* completamente fictícia, com atributos inventados, não estaremos perante apropriação indevida de identidade[143]. Podemos estar perante algum tipo de comportamento fraudulento, quando o recetor desta "identidade" fictícia for enganado a revelar informações ou tiver certas atitudes motivadas pelo convencimento de que está a contactar com certa pessoa que

[140] "(...) o consentimento – muitas vezes uma "ficção" – está limitado pelo princípio da finalidade.", "Desta forma, um tratamento que invada elementos externos à finalidade, ou que não defina finalidades precisas padece de ilicitude (...)" – SOUSA PINHEIRO – Ob. cit., p. 943.

[141] Já dizia MARIA RIBEIRO DE FARIA, a propósito da anterior Lei de Proteção dos Dados Pessoais, "cabem assim neste conceito de dados pessoais, dados ou elementos informativos da mais variada natureza (sinais ou elementos de natureza não convencional ou convencional, como é o caso do nome da pessoa, dados de natureza biométrica, de que fazem parte a identificação de retina, das impressões digitais, e de geometria da mão, fotografias, entre tantos outros) que possibilitem a identificação da pessoa a vários níveis, ou sob vários aspectos (referentes à sua solvabilidade, saúde, costumes, personalidade). – MIRANDA/ MEDEIROS– Ob. cit., p. 786.

[142] Tal como no crime de furto, onde as coisas que não pertencem a ninguém (*res nullius*), não se subsumem no conceito de coisa "alheia", também aqui, os dados têm de pertencer a alguém, a uma pessoa real e concreta, para poderem ser apropriadas.

[143]Concordamos, pois, com a já referida decisão FLORES-FIGUEROA *v.* UNITED STATES, porquanto não pode haver este crime se os dados não fizerem parte de uma identidade real.

na verdade não existe, mas não será nunca apropriação indevida de identidade, pois que esta exige que os dados utilizados sejam de um terceiro real, alguém identificado ou identificável.

O tipo objetivo termina com o elemento decisivo para que se trate de uma apropriação indevida de identidade: a apresentação como sendo o legitimo titular dos dados. Este elemento é essencial para delimitar os casos que se subsumem a este tipo legal. A não existir esta delimitação, sempre que alguém usa o cartão bancário de outrem ou os dados desse cartão, estaria a praticar um crime. Não é assim porque quem o faz não está, só por isso, a adotar a identidade da pessoa a quem pertence o cartão. Com efeito, para além de ser necessária a utilização de dados alheios, é também necessário que essa utilização sirva o propósito de identificar o agente como legitimo titular desses dados, estando assim o ardil completo. Não significa isto, consideramos, contrariamente ao que foi afirmado pela STS nº1045/2011, de 14 de Outubro[144], que o agente incorpore totalmente a personalidade ou várias facetas da pessoa cujos dados utiliza, mas sim que, ao usar os dados, o faça sempre com a intenção de passar a aparência de que é o titular dos dados. Assim achamos por razões processuais e de contemporaneidade. Por razões processuais, porque nos parece arriscado e injusto pedir que seja feita prova de algo tão abstrato e complexo como o ato de adotar completamente a identidade de outrem. Por razões de contemporaneidade, no sentido em que já não é essa a atuação típica de que pratica este ato criminoso. Tendo em conta a sociedade em constante evolução em que vivemos, não se justifica adotar a identidade de alguém por completo quando se pode adotar a identidade de várias pessoas. As atuações criminosas no mundo digital são voláteis e rápidas, porque os meios técnicos assim o permitem. Usar a identidade/dados de alguém durante muito tempo representa um risco desnecessário, razão pela qual este crime sofreu mutações. A facilidade de conseguir os dados faz com que qualquer identidade seja "descartável". Por isso, defendemos que o simples uso de dados de terceiro (com intenção de provocar engano e sem consentimento) - mesmo que só uma vez, numa situação circunscrita - como seus, é apropriação indevida de identidade, não sendo necessário adotar várias facetas da pessoa a quem pertencem os dados. Até porque, relembramos, o bem aqui em causa é a autodeterminação informacional, cuja proteção recai sobre os dados pessoais, não a identidade como um todo.

Desta análise resulta que o simples uso de dados para efetuar compras online, sem o consentimento do titular do método de pagamento, já será subsumível a este tipo legal. Da mesma forma, o envio de um email com dados alheios – seja esse dado o próprio email ou

[144] *Vide* pg. 35.

só o nome da pessoa com um email criado de origem de forma a parecer o dessa pessoa – também será um exemplo válido. O *vishing* ou *smishing* com uso de dados reais de outrem – seja o seu nome, seja a aparência do seu número no ecrã do destinatário, seja um dado de informação que convença o destinatário da chamada ou *sms* da veracidade do contacto – também se enquadra. Alguns destes exemplos, note-se, configuram apropriação indevida de identidade, mas não configuram falsidade informática, por exemplo, como explicámos já, por não existir geração de dados informáticos falsificados. Sendo este um crime que não exige resultado e bastando-se com o uso de dados e respetiva intenção de enganar o destinatário com esses dados, a tutela torna-se mais ampla, abarcando casos que, de contrário, ficariam (e ficam) sem proteção.

Resta-nos dizer que, seja qual for o tipo legal que venha (se vier) a existir no futuro, este terá sempre de ser ajustado e adaptado ao longo do tempo, para que seja possível acompanhar as evoluções tecnológicas e aquilo que estas possibilitam em termos de condutas criminosas. Ao contrário dos crimes tradicionais, crimes como este e outros em meio digital terão de ser acompanhados de perto e alterados amiúde. Aquilo que se pode fazer hoje em dia não era possível há dez anos atrás e aquilo que será possível fazer daqui a dez anos, está muita para lá da imaginação de todos nós.

2. Eventuais agravações

O nº2 do tipo legal contempla as duas possíveis agravações deste crime, tendo sido escolhidas, de acordo com o estudo feito sobre a atuação típica neste tipo de fenômeno e com os direitos mais facilmente afetados por este tipo de atuações. Em qualquer uma destas hipóteses, a conduta criminosa torna-se suscetível de provocar danos superiores ou de se tornar mais perigosa.

A primeira agravação, relaciona-se com um dos resultados possíveis da conduta típica – causar prejuízo patrimonial. Esta agravação é motivada pelo facto de este ser o resultado mais frequente da apropriação indevida de identidade. De facto, causar prejuízo patrimonial é o resultado mais procurado pelos agentes deste crime, o que está provado pelos dados já apresentados por estudos internacionais no que diz respeito às perdas anuais relacionadas com utilização indevida de dados de terceiros[145]. Para além de ser o resultado mais procurado, a agravação justifica-se, também, pelo que já explicámos no ponto a especial necessidade de

[145] *Vide* Capítulo II, ponto 2.

intervenção do direito penal no contexto digital, sendo a facilidade maior e o risco menor nas atuações cometidas através de meio informático, o prejuízo patrimonial possivelmente provocado é muito superior (assim escolha o agente) ao que seria existente num crime não digital. O bem jurídico protegido, aqui, é o património.

A segunda agravação, tem, também, que ver com o resultado da apropriação indevida de identidade, ainda que de forma distinta. Neste caso, o que releva não é só o resultado – divulgação de dados de terceiro – mas, especialmente, o conteúdo específico desse resultado. De facto, não basta revelar dados, estes têm de ser relacionados com a intimidade da vida privada e familiar do titular ou de terceiro. O direito à reserva sobre a intimidade da vida privada é constitucionalmente reconhecido no art.26º, n1 da CRP e é também, um bem jurídico já protegido por várias normas do nosso CP (veja-se o Livro II - Parte especial, Título I - Dos crimes contra as pessoas Capítulo, VII – *Dos crimes contra a reserva da vida privada*) Sendo que o meio digital consegue atingir uma imensidão de pessoas, este é, não só o meio preferido dos criminosos para expor conteúdos íntimos da vida de alguém, como o meio que pode, potencialmente, provocar mais danos. Esta agravação funcionará tanto nos casos em que o agente revela conteúdos íntimos com um intuito de vingança (caso do *revenge porn*[146]), como nos casos em que o agente o faz para dar mais credibilidade ao facto de ser o titular dos dados que está a usar – pense-se num caso de *catfishing* em que é criada uma página no *facebook* usando dados de terceiro, com o objetivo de obter informações de outrem ou meramente fingir ser essa pessoa. É perfeitamente possível nestes casos que o falso titular revele informações íntimas do verdadeiro titular (quer na página de *facebook*, quer no *messenger*, por exemplo), para convencer a outra parte da veracidade da sua identidade.

No que toca à extensão do conceito intimidade da vida privada e familiar citado o Parecer 121/80 (23 de Julho de 1981) da PGR "a intimidade da vida privada de cada um, que a lei protege, compreende aqueles aspectos que, não sendo secretos em si mesmos, devem subtrair-se à curiosidade pública por naturais razões de resguardo e melindre, como os sentimentos e afectos familiares, os costumes da vida e as vulgares práticas quotidianas, a vergonha da pobreza e as renúncias que ela impõe e até, por vezes, o amor da simplicidade,

146 "*Nonconsensual pornography refers to sexually explicit images disclosed without consent and for no legitimate purpose. The term encompasses material obtained by hidden cameras, consensually exchanged within a confidential relationship, stolen photos, and recordings of sexual assaults*". - FRANKS, Mary Anne - **Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators**, p.3.

a parecer desconforme com a natureza dos cargos e a elevação das posições socias. Em suma, tudo: sentimentos, ações e abstenções"[147].

3. O tipo subjetivo

Para que haja apropriação indevida de identidade a conduta do agente tem de ser praticada com dolo. É necessária "uma atitude íntima do agente contrária ou indiferente ao Direito e às suas normas"[148], tem de haver uma intenção direta e clara do agente pela apropriação da identidade de outrem. Não nos interessa aqui discorrer sobre certas teorias penais, bastando perceber que a este crime se aplicarão as regras gerais do Código Penal, em especial, nesta matéria, o art.13º e 14º. São também aplicáveis as causas de exclusão de culpa dos artigos 16º e 17º e as inimputabilidades dos artigos 19º e 20º. Não estando prevista a forma negligente, porquanto não se vislumbra um dever de cuidado associado ao bem jurídico autodeterminação informacional, o facto praticado com negligência não é punido.

Parece-nos importante salientar o art.14º/2 que diz agir com dolo quem representa a realização de um facto como consequência necessária para chegar à conduta que quer atingir. Este critério tem especial sentido no fenómeno em estudo. Como já explicamos acima, a apropriação indevida de identidade será, muitas vezes, um crime meio para atingir um crime fim. Muitas vezes, o agente só usará dados de terceiro por ser a única forma de atingir o objetivo final em mente – veja-se o exemplo de alguém que recorre a *catfishing* ou usa o email de terceiro, com o objetivo de chegar a alguém de confiança do real titular dos dados. Nestes casos, o verdadeiro objetivo não é a apropriação da identidade do titular dos dados, contudo a apropriação é vista como necessária para chegar ao fim visado. Por aplicação do art.14º/2 do CP serão de considerar estas condutas dolosas e, portanto, preenchendo o (eventual) tipo legal.

No que toca à intenção de provocar engano esta configura um elemento subjetivo especial do tipo, por ser caracterizador deste delito. Contrariamente aos elementos especiais dos tipos de culpa dolosos, a intenção de provocar engano não constitui exigência adicional para que o agente seja punido a titulo de dolo, mas sim um elemento que "serve ainda a definição de uma certa espécie de delito e se refere, por esta via, ao bem jurídico protegido, ou se visa ainda caracterizar o objeto da ação, a forma da sua lesão, ou uma qualquer

[147] *Apud* FIGUEIREDO DIAS, Jorge de (dir.) – **Comentário conimbricense…**Ob. cit. Tomo I, p. 728.
[148] FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p. 529.

tendência relevante para o ilícito"[149]. Esta intenção é o que justifica, também, que este crime só seja punido a titulo doloso[150], sendo que na negligencia, não existe uma intenção de enganar, sendo que a negligência se reflete numa "atitude interna de descuido ou leviandade perante o Direito e as suas normas"[151] e não numa atitude consciente e diretamente contrária ao Direito.

4. <u>O grau de lesão do bem jurídico exigido</u>

Finalmente, resta-nos perceber qual é o grau de lesão do bem-jurídico exigido, por outras palavras, se este delito se classifica como um crime de dano ou de perigo e, também, se se trata de um crime simples ou complexo.

Na diferença entre crime de dano – aquele que gera uma lesão efetiva no bem jurídico – e crime de perigo – não é preciso lesar o bem jurídico, basta colocá-lo em perigo[152] -, classificamos este crime como um crime de perigo. Poder-se-ia dizer que, a mera utilização de dados alheios, já constituiria uma lesão, no entanto a questão não é assim tão simples. Relembrando o que dissemos no Capítulo III, ponto 1, a caracterização da autodeterminação informacional como bem jurídico e direito fundamental autónomo, deve-se ao facto de o acesso a dados alheios permitir a formação de um perfil dessa pessoa, levando a restrição da sua liberdade e à lesão de bens jurídicos conexos (imagem, intimidade da vida privada, entre outros). Portanto, a ofensa deste bem jurídico, exige a efetiva perda de controlo do titular, em relação aos seus dados, perda essa que acontece, quando outra pessoa é tida, erroneamente, como titular dos dados, agindo e sendo reconhecida como tal. Ora, com este crime, tal como o configurámos, aquilo que se pretende é antecipar a tutela, para o momento em que há utilização dos dados, mas onde ainda não se exige que o agente seja, de facto, reconhecido como titular dos dados usados – o momento de tutela não é, ainda, o da lesão do bem jurídico. Dentro da classe de crimes de perigo, há ainda que fazer a distinção entre

[149] FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p. 380.
[150] Em conformidade com a análise jurisprudencial feita para o crime de falsidade informática (art.3º da LC) que tem este mesmo elemento típico: "Do ponto de vista subjetivo, o tipo legal supõe o dolo, sob qualquer das formas previstas no artigo 14º do Código Penal, exigindo, enquanto elemento subjetivo especial do tipo, a intenção de provocar engano nas relações jurídicas, bem como, relativamente á produção de dados ou documentos não genuínos, a particular intenção do agente de que tais dados ou documentos sejam considerados ou utilizados para finalidades juridicamente relevantes como se fossem genuínos." – Ac. do TRE de 19 de Maio de 2015, Proc. 238/12.8PBPTG.E1, Rel. António Latas;
Da mesma forma, no que toca ao crime de burla, LEAL-HENRIQUES, Manuel de Oliveira/ SIMAS SANTOS, Manuel José Carrilho de - **Código penal anotado, p. 540** – "A burla só é censurada a título de dolo. A negligência é necessariamente excluída pela exigência de que o erro ou engano sejam astuciosamente provocados ou aproveitados. Não existe o crime sem a vontade consciente dirigida neste sentido".
[151] FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p. 896.
[152] FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p. 309.

perigo concreto e abstrato. Para haver um crime de perigo concreto, é necessário que esse perigo seja parte integrante do tipo legal[153], no crime de perigo abstrato o perigo é o que motiva a norma, mas não parte integrante da mesma[154]. Dentro desta classificação, é nossa opinião, que estamos perante um crime de perigo abstrato, não havendo uma necessidade expressa de colocar o bem jurídico em perigo. O uso de dados é um comportamento apto a comprometer a autodeterminação informacional, mas a perigosidade efetiva desse comportamento não tem de ser demonstrada.

Há quem tenha levantado questões de constitucionalidade no que toca aos crimes de perigo abstrato, por pensar que estes representam uma violação do princípio da legalidade ao antecipar demasiado a tutela dos bens jurídicos[155]. Como resposta a este problema surgiu o chamado direito penal do risco, que defende uma intervenção mais vincada do direito penal em áreas em que os perigos de atuação são exponenciais, como os relacionados com a tecnologia, indústria, manipulação genética, questões nucleares e ambientais. Para haver proteção contra estes perigos seria necessária uma ação preventiva, sempre acompanhada de uma análise delicada entre o que se quer proteger e aquilo que terá de se restringir. Cremos, que esta tutela se justifica especialmente nos crimes informáticos, em conformidade com o que é defendido por ROVIRA DEL CANTO quando nos fala da necessidade de adaptar o direito penal à nova realidade trazida pelos meios informáticos, através da criação de um "Direito Penal Global do Risco Informático e da Informação, que seria composto por um "conjunto de normas penais reguladoras dos ilícitos vinculados aos riscos derivados do uso de meios informáticos e telemáticos, os dados e a informação em si mesma"[156]. O centro deste mundo digital é a informação[157] e a transação desta sem controlo, razão pela qual acreditamos ser tão importante a incriminação do uso de dados, desde já, de forma a dar uma resposta atempada e adequada à realidade.

---

153 "Nos crimes de perigo concreto o perigo faz parte do tipo, isto é, o tipo só é preenchido quando o bem jurídico tenha efetivamente sido posto em perigo." – FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p. 309.

154 "Nos crimes de perigo abstrato o perigo não é elemento do tipo, mas simplesmente motivo da proibição. Quer dizer, neste tipo de crimes são tipificados certos comportamentos em nome da sua perigosidade típica para um bem jurídico, mas sem que ela necessite de ser comprovada no caso concreto" – FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p. 309.

155 FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., pp. 309 e 310.

156 DIAS, Vera Elisa Marques – Ob. cit., pp. 28 e 29.

157 "O objecto desta protecção reforçada é a informação e os dados em si mesmos, como bens de valor económico-social e a segurança e fiabilidade colectiva da sociedade nos sistemas e redes informáticas e de telecomunicações. A diferença existente entre os crimes informáticos e os crimes tradicionais impõe a adequação e transformação das medidas a tomar para combater os primeiros, o que leva a uma mudança de paradigma" DIAS, Vera Elisa Marques – Ob. cit., p. 29.

No que diz respeito ao número de bens jurídicos protegidos, este é um crime simples, uma vez que, como já visto, tutela somente um bem jurídico: a autodeterminação informacional. Contrariamente, o exemplo típico de um crime complexo é o do crime de roubo (210º), que tutela tanto a propriedade como a integridade física e liberdade individual de decisão e ação[158].

[158] FIGUEIREDO DIAS, Jorge de – **Direito Penal…** Ob. cit., p.312.

Conclusão

O mundo tal como o conhecemos mudou, drasticamente, nos últimos anos. O surgimento dos novos meios de comunicação e, em especial, da Internet, criaram novos costumes e modos de vida e levaram ao aparecimento de novos conceitos e a formas inovadoras de encarar conceitos já conhecidos. A identidade, um conceito por nós reconhecido desde a Antiguidade, apresenta-se agora de forma distinta. Temos, como novo elemento integrador da identidade, a ciberidentidade, constituída por todos os dados de informação pessoal reconduzíveis a uma pessoa real e concreta, identificada ou identificável. A importância deste tema, em concreto, torna-se clara quando somos confrontados com os artigos 26º e 35º da CRP, que reconhecem a identidade pessoal e a autodeterminação informacional como direitos fundamentais. Juntas, estas duas normas, esclarecem o conceito de identidade pessoal moderno.

Com um conceito jurídico alargado de identidade surgem novas formas de ataque a este direito. A Internet, como meio primordial de armazenamento e passagem de informação, torna-se uma ferramenta cada vez mais usada pelas entidades estatais e privadas e, correspondentemente, pelos agentes criminosos. Perante a sociedade de informação, torna-se mais fácil que nunca antes na História, interromper os fluxos de informação e obter dados pessoais de terceiros. O fenómeno a que apelidamos de apropriação indevida de identidade cresce em número e em danosidade, à medida que a tecnologia o possibilita. Vimos, ao longo deste trabalho, o crescimento significativo desse mesmo fenómeno que tem havido, não só em Portugal, como, especialmente, noutros países. Como resposta, os EUA, Espanha e México, têm normas próprias para a sua criminalização e a Alemanha, sob um pensamento algo distinto, embora claramente com este fenómeno em mente, decidiu-se pela criminalização autónoma do *phishing*, sendo esta a forma de obtenção de dados mais usada atualmente. Como foi evidenciado desde o inicio, o nosso ordenamento jurídico ainda não consagrou um crime autónomo, contudo, dispõe de tipos legais aos quais são subsumíveis algumas atuações prévias ou posteriores – a falsidade informática (art.3º da LC); o dano relativo a programas pu outros dados informáticos (art.4º da LC); o acesso ilegítimo (art.6º da LC); a interceção ilegítima (art.7º da LC); a burla (art217º do CP) – e até, atuações que já se podem classificar como apropriação indevida de identidade – a falsificação de documentos (art.256º do CP); o uso de documento de identificação ou de viagem alheio (art.261º do CP); a falsificação informática, se forem usados dados de terceiro. No entanto, há ainda várias

atuações desprotegidas, especialmente no contexto digital, falamos aqui no *catfishing* ou no *phshing* através do uso de um email real por alguém que não o seu titular, por exemplo.

Aliando a análise comparada com outros ordenamentos jurídicos e a análise do nosso ordenamento, que parece, na nossa opinião, ainda não estar totalmente a par dos desenvolvimentos tecnológicos recentes e das novas possibilidades que estes trouxeram às condutas criminosas, cremos haver espaço para uma criminalização autónoma da apropriação indevida de identidade. Criminalização essa que terá por base o bem jurídico autodeterminação informacional, como concretização e complemento do nosso direito fundamental à identidade pessoal. Por isso mesmo, após determinar a existência de um bem jurídico-penal e a carência penal desta atuação, deixámos aqui uma sugestão de redação do tipo legal, que nos parece adequada ao nosso ordenamento e, ao mesmo tempo, contemporânea. Este possível tipo legal teria agravações relacionadas com o património e a reserva da intimidade da vida privada e familiar, porquanto estes são os bens jurídicos que acreditamos serem mais visados pelos agentes e cujos danos, através do uso da Internet como difusor e da apropriação de identidade como fonte de credibilidade, se tornam potencialmente desastrosos. Deixámos ainda a nota, importante, de que este, como muitos outros crimes em meio digital terão de ser constantemente atualizados e revistos, à medida que a própria tecnologia evoluiu. Não nos restam dúvidas que o direito, hoje, terá de ser adaptável e que essas adaptações terão de acontecer a um ritmo sem precedentes.

O novo paradigma social remete-nos para uma sociedade do conhecimento e para a realidade de vivermos em tempos exponenciais, e, como tal acreditamos que o Direito tem aqui uma palavra importante a dizer, acompanhando as mudanças tecnológicas e de comportamento que levam a novas formas de pensar crimes já antes definidos e propondo novos enquadramentos legais capazes de fazer face a esta nova realidade.

Referências Bibliográficas

ÁLVAREZ, Rogelio Barba – El robo de identidade en México. **Revista de investigación en Derecho, Criminología y Consultoría Jurídica** [*online*]. Nº22 (2017), pp. 245-260. [Última Consulta 4 de Jan. 2019]. Disponível em http://www.apps.buap.mx/ojs3/index.php/dike/article/view/532.

ALVES, Jones Figueirêdo – **Identidade pessoal na sociedade de informação: dimensões de autodeterminação e ilicitude civil**. Universidade de Lisboa, Faculdade de Direito, 2015. Dissertação de Mestrado.

CARNEIRO DA SILVA, Flávio Manuel – **A Usurpação da Ciberidentidade** [*online*], Universidade Católica Portuguesa, Centro Regional do Porto, Escola de Direito, 2014. Dissertação de Mestrado. [Última Consulta 4 de Jan. 2019]. Disponível em http://repositorio.ucp.pt/bitstream/10400.14/16422/1/A%20usurpa%C3%A7%C3%A3o%20da%20ciberidentidade.pdf

CHOU, Neil [et al.] – **Client-side defense against web-based identity theft**[*online*]. Trabalho no âmbito do Network and Distributed System Security Symposium (NDSS). California, EUA, 2004. [Última Consulta 4 de Jan. 2019]. Disponível em https://theory.stanford.edu/~jcm/papers/spoofguard-ndss.pdf

CURTIS, George –**The Law of Cybercrimes and their Investigations**. Boca Raton: CRC Press, 2011. ISBN 978-1-4398-5832-5

DIAS, Vera Elisa Marques– **A problemática da investigação do cibercrime** [*online*]. Universidade de Lisboa, Faculdade de Direito/ IDPCC, 2010. Trabalho académico no âmbito do I Curso de Pós-Graduação de Aperfeiçoamento em Direito da Investigação

Criminal e da Prova. [Última Consulta 4 de Jan. 2019]. Disponível em http://www.verbojuridico.net/doutrina/2011/veradias_investigacaocibercrime.pdf

DUQUE, Jorge Rafael V. Reis – **A prova digital e o phishing como caso de estudo**, Universidade Lisboa, Faculdade de Direito, 2007. Relatório de mestrado para a cadeira de Direito Processual Penal.

FIGUEIREDO DIAS, Jorge de – **Direito Penal: Parte Geral**. 2ª ed. Coimbra: Coimbra Editora, 2007. ISBN 978-972-32-1523-6

FIGUEIREDO DIAS, Jorge de (dir.) –**Comentário conimbricense do código penal: parte especial**. Coimbra: Coimbra Editora, 1999 – Tomo II. ISBN 978-972-32-2061-2

FRANKS, Mary Anne - **Drafting an Effective 'Revenge Porn' Law: A Guide for Legislators** [*online*]. Universidade de Miami, Faculdade de Direito, 2015. [Última Consulta 4 de Jan. 2019]. Disponível em https://ssrn.com/abstract=2468823

GERALDES, Ana Vaz – *Phishing*: fraude online, **Revista da Faculdade de Direito da Universidade de Lisboa**, Coimbra Editora. Vol. 54, nº1(2013), pp. 87-102

HOGAN, Bernie –The presentation of self in the age of social media: distinguishing performances and exhibitions online. **Bulletin of Science Technology & Society** [*online*]. Vol. 30, nº6 (2010), pp. 377-386. [Última Consulta 4 de Jan. 2019]. Disponível em http://bst.sagepub.com/content/30/6/377b

IRSHAD, Shareen/ SOOMRO, Tariq Rahim - Identity Theft and Social Media. **IJCSNS International Journal of Computer Science and Network Security** [*online*]. Vol.18, nº1 (2018), pp. 43-55. [Última Consulta 4 de Jan. 2019]. Disponível em http://paper.ijcsns.org/07_book/201801/20180106.pdf

LEAL-HENRIQUES, Manuel de Oliveira/ SIMAS SANTOS, Manuel José Carrilho de - **Código penal anotado.** 3ª ed., Lisboa: Rei dos Livros, 2000-2002 – 2 Vols. ISBN 972-51-0954-6

LYNCH, Jennifer - Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks. **Berkeley Technology Law Journal**[*online*]. Vol. 20, nº1 (2005), pp.259-300. [Última Consulta 4 de Jan. 2019]. Disponível em https://doi.org/10.15779/Z38M67D

MIRANDA, Jorge/ MEDEIROS, Rui – **Constituição Portuguesa Anotada.** 2ª ed. Coimbra: Wolters Kluwer - Coimbra Editora, 2010 – Tomo I. ISBN 972-32-1307-9

NETO, Luísa/ LEÃO, Anabela, coord. **–Constituição anotada: obra colectiva de estudantes da Faculdade de Direito da Universidade do Porto no âmbito das comemorações dos 10 anos da Faculdade e dos 30 anos da Constituição da República Portuguesa de 1976**. [S.l.:s.n.], 2006

OLIVEIRA ASCENSÃO, José de– Criminalidade Informática. In **Direito da Sociedade da Informação**. Coimbra: Coimbra Editora, 2001. ISBN 972-32-0994-2. Vol. 2, pp. 203-228

PEREIRA, Victor de Sá/ LAFAYETTE, Alexandre **–Código penal anotado e comentado, Legislação conexa e complementar**. 2ª edição, Lisboa: QuidJuris? – Sociedade Editora Ld.ª, 2014. ISBN 978-972-724-675-5

PINTO, Ana - **Investigação criminal com recurso a meios telemáticos: em especial, as buscas online e o agente infiltrado online** [*online*]. Universidade de Lisboa, Faculdade

de Direito, 2016. Dissertação de Mestrado. [Última Consulta 4 de Jan. 2019]. Disponível em http://repositorio.ul.pt/handle/10451/23473

PROCURADORIA-GERAL DA REPÚBLICA – GABINETE CIBERCRIME – **Nota prática nº 5/2015 27 de Agosto de 2015: Jurisprudência sobre cybercrime** [*online*]. Lisboa, 2015. [Última Consulta 4 de Jan. 2019]. Disponível em http://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/nota_pratica_5_jurispridencia_penal.pdf

ROMANOSKY, Sasha –Do Data Breach Disclosure Laws Reduce Identity Theft?. **Journal of Policy Analysis and Management** [*online*]. Vol. 30, Nº 2 (2011), pp. 256-286. [Última Consulta 4 de Jan. 2019]. Disponível em https://ssrn.com/abstract=1268926

SOUSA PINHEIRO, José Alexandre Guimarães de – **Privacy e protecção de dados pessoais: a construção dogmática do direito à identidade informacional**. Lisboa: [s.n.], 2011. Universidade de Lisboa, Faculdade de Direito. Tese de Doutoramento

TEIXEIRA, Guilherme da Fonseca – Identidade e autodeterminação informacional no novo Regulamento Geral da Proteção de Dados: a inevitável privatização dos deveres estatuais de proteção. **Católica Law Review**. ISSN 2183-9336. Vol. 2, nº 1 (2018), pp. 11-38

VENÂNCIO, Pedro Dias – **Lei do Cibercrime: Anotada e Comentada.** 1ª ed. Coimbra: Coimbra Editora, 2011. ISBN 978-972-32-1906-7

WALL, David S./ Williams, Mathew L. – **Policing Cybercrime: Networked and Social Media Technologies and the Challenges for Policing**. 1ª ed. Oxfordshire: Routledge - Taylor & Francis Group, 2014. ISBN 13:978-1-138-02527-1

WANG, Wenjie/ YUAN, Yufei/ ARCHER, Norm -A Contextual Framework for Combating Identity Theft. **IEEE Security and Privacy Management** [*online*]. Vol. 4, nº2, pp.30-38. [Última Consulta 4 de Jan. 2019]. Disponível em https://www.researchgate.net/publication/3437785_A_Contextual_Framework_for_Combating_Identity_Theft

WHITE, Michael D. / FISHER, Christopher - Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Effort. **Criminal Justice Policy Review** [*online*]. Vol. 19, nº1 (2008), pp. 3-24. [Última Consulta 4 de Jan. 2019]. Disponível em http://cjp.sagepub.com/cgi/content/abstract/19/1/3

Referências Jurisprudenciais

Nacionais

Ac. do STJ de 20 de Março de 2003, Proc. 03P241, Rel. Simas Santos, disponível em www.dgsi.pt

Ac. do STJ de 4 de Junho de 2003, Proc.03P1528, Rel. Henriques Gaspar, disponível em www.dgsi.pt

Ac. do STJ de 18 de Junho de 2008, Proc. 08P901, Rel. Maia Costa, disponível em www.dgsi.pt

Ac. do STJ de 27 de Abril de 2011, Proc. 456/08.3GAMMV, Rel. Henriques Gaspar, disponível em www.dgsi.pt

Ac. do TC de 13 de Fevereiro de 2001, Proc. 166/2001, disponível em www.dgsi.pt

Ac. do TC de 23 de Dezembro de 2008, Proc. 977/2008, Rel. Maria Lúcia Amaral, disponível em www.dgsi.pt

Ac.do TRL de 10 de julho de 2012, Proc. 7876/10.1JFLSB.L1-5, Rel. Luís Gominho, disponível em www.dgsi.pt

Ac.do TRP de 21 de novembro de 2012, Proc. 1001/11.9JAPRT.P1, Rel. Borges Martins, disponível em www.dgsi.pt

Ac. do TRP de 19 de Fevereiro de 2014, Proc. 529/11.5TABGC.P1, Rel. José Carreto, disponível em www.dgsi.pt

Ac. do TRP de 10 de Maio de 2017, Proc. 135/14.2GAVFR.P1, Rel. Manuel Soares, disponível em www.dgsi.pt

Ac. do TRE de 20 de Maio de 2014, Proc. 1915/13.1TASTB.E1, Rel. Alberto João Borges, disponível em www.dgsi.pt

Ac. do TRE de 19 de Maio de 2015, Proc. 238/12.8PBPTG.E1, Rel. António Latas, disponível em www.dgsi.pt

Ac. do TRC de 11 de Março de 2009, Proc. 36/03_3GCTCS.C1., Rel. Fernando Ventura, disponível em www.dgsi.pt

Ac. do TRC de 17 de Janeiro de 2013, Proc. 282/11.2TTCVL.C1, Rel. Jorge Loureiro, disponível em www.dgsi.pt

Internacionais

STS nº635/2009, 15 de Junho de 2009, Proc. 1721/2008, Rel. Joaquin Delgado Garcia, disponível em https://supremo.vlex.es/vid/-76463551

STS no1045/2011, de 14 de Outubro de 2011, Proc. 10365/2011, Rel. Juan Ramon Berdugo Gomez de la Torre, disponível em https://supremo.vlex.es/vid/-331657506

STS no331/2012, de 4 de Maiode 2012, Proc. 11221/2011, Rel. Jose Ramon Soriano, disponível em https://supremo.vlex.es/vid/375393930

FLORES-FIGUEROA *v.* UNITED STATES, Nº08–108. *Argued* February 25, 2009 - *Decided* May 4, 2009, disponível em https://caselaw.findlaw.com/us-supreme-court/556/646.html

ANEXOS

Anexo I – A evolução do "roubo de identidade"

Table 1: Evolution of Identity Theft

Era	Type of Identity Theft
1800-1918	The outlaws of this era killed people to assume their identities
1919-1921	Identities were stolen to cast votes multiple times
1922-1930	The smugglers created their own version of witness protection programs and murdered people to attain legal documents to create new identities
1931-1959	Youngsters created fake IDs to buy alcohol
1960-1969	Introduction of credit cards gave criminals new ways of identity theft
1970-1989	Frank Abagnale the famous con artist stole identities to cash cheques
1990-1998	Technology advancement increased cases of identity crimes
1999-2000	Introduction of Internet and search engines like Google led people to give away personal information
2001-2003	The credit reporting agencies were instructed to provide credit reports to customers to prevent fraudulent accounts being opened
2004-2015	The National Crime Victimization Survey was updated to include new forms of Identity Theft
2016	Identity Theft was the most popular consumer complaint for 15 consecutive years
2017	American banks increased their security causing criminals to use other platforms for stealing identities
2018-2020	Technology is evolving and new apps are being introduced; so that thieves are gaining more and more access to personal information through these new apps

IRSHAD, Shareen/ SOOMRO, Tariq Rahim - Identity Theft and Social Media, p.43

Anexo II - Identity Theft and Assumption Deterrence Act (EUA)

105th CONGRESS
2d Session

H. R. 3601

To amend chapter 47 of title 18, United States Code, relating to **identity fraud**, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

March 30, 1998

Mr. Shadegg (for himself, Mr. Clement, Mrs. Myrick, Mr. Tiahrt, Mr. Calvert, Mr. Martinez, Mr. Filner, Mr. Coburn, Mr. Hostettler, Mr. Hoekstra, Mr. Engel, Mr. Ackerman, Mr. Hayworth, and Mr. Solomon) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committee on Transportation and Infrastructure, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To amend chapter 47 of title 18, United States Code, relating to identity fraud, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ``Identity Theft and Assumption Deterrence Act of 1998".

SEC. 2. CONSTITUTIONAL AUTHORITY TO ENACT THIS LEGISLATION.

The constitutional authority upon which this Act rests is the power of Congress to regulate commerce with foreign nations and among the several States, set forth in article I, section 8 of the United States

Constitution.

SEC. 3. IDENTITY FRAUD.

(a) Establishment of Offense.--

(1) In general.--Chapter 47 of title 18, United States Code, is amended by adding at the end the following:

``Sec. 1036. Identity fraud

``(a) Definitions.--In this section--

``(1) the term `communication facility' has the meaning given that term in section 403(b) of the Controlled Substances Act (21 U.S.C. 843(b));

``(2) the term `means of identification' means any name or number that may be used, alone or in conjunction with any other information, to assume the identity of an individual, including any--

``(A) personal identification card (as that term is defined in section 1028); or

``(B) access device, counterfeit access device, or unauthorized access device (as those terms are defined in section 1029);

``(3) the term `personal identifier' means--

``(A) a name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, or any access device (as that term is defined in section 1029);

``(B) any unique biometric data, such as a fingerprint, voice print, retina or iris image, or other unique physical representation;

``(C) any unique electronic identification number, address, or routing code; or

``(D) any other means of identification not lawfully issued to the user;

``(4) the term `identification device' means any physical, mechanical, or electronic representation of a personal identifier or any personal information or data; and

``(5) the term `personal information or data' means any information that, when used in conjunction with a personal identifier or identification device, would facilitate a misrepresentation or assumption of the identity of another.

``(b) Prohibition.--Whoever in interstate or foreign commerce, or through the use of a communication facility, knowingly, with intent to defraud, and in order to receive payment or any other thing of value the aggregate value of which is equal to or greater than $1,000--

``(1) receives, acquires, obtains, purchases, sells, transfers, traffics in, or steals, or attempts to receive, acquire, obtain, purchase, sell, transfer, traffic in, or steal, or otherwise causes or solicits another to do the same, any personal identifier, identification device, personal

information or data, or other document or means of identification of any entity or person;

``(2) possesses or uses, or attempts to possess or use, or otherwise causes or solicits another to do the same, any personal identifier, identification device, personal information or data, or other document or means of identification of any entity or person; or

``(3) assumes, adopts, takes, acquires, or uses, or attempts to assume, adopt, take, acquire, or use, or otherwise causes or solicits another to do the same, the identity of any entity or person;

shall be fined under this title, imprisoned not more than 15 years, or both.

``(c) Conspiracy.--Whoever is a party to a conspiracy of 2 or more persons to commit an offense described in subsection (b), if any of the parties engages in any conduct in furtherance of the offense, shall be fined in an amount not to exceed the amount of the fine to which that person would be subject for that offense under subsection (b), imprisoned not more than 7.5 years, or both.".

(2) Investigative authority.--In addition to any other agency having such authority, the United States Secret Service may investigate any offense under section 1036 of title 18, United States Code (as added by this subsection), except that the exercise of investigative authority under this paragraph shall be subject to the terms of an agreement, which shall be entered into by the Secretary of the Treasury and the Attorney General.

(3) Sentencing enhancement.--Pursuant to its authority under section 994(p) of title 28, United States Code, the United States Sentencing Commission shall amend the Federal sentencing guidelines to provide for sentencing enhancements under chapter 2 of the Federal sentencing guidelines for a defendant who is convicted of an offense under section 1036 of title 18, United States Code, in connection with an offense under section 513, 514, 1028, 1029, 1341, 1342, 1343, 1344, or 1708 of title 18, United States Code, as follows:

(A) A sentencing enhancement of--

(i) 1 level, if the offense involves not more than 1 victim;

(ii) 2 levels, if the offense involves not less than 2 and not more than 4 victims; or

(iii) 3 levels, if the offense involves 5 or more victims.

(B) An appropriate sentencing enhancement, if the offense involves stealing or destroying a quantity of undelivered United States mail, in violation of section 1702, 1703, 1708, 1709, 2114, or 2115 of title 18, United States Code.

(C) An appropriate sentencing enhancement based on the potential loss (as opposed to the actual loss) that could have resulted from an identity theft offense

(i.e. the line of credit of the access device, etc.).

(4) Clerical amendment.--The analysis for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

``1036. Identity fraud.".

(b) Forfeiture of Contraband.--Section 80302(a) of title 49, United States Code, is amended--

(1) in paragraph (5), by striking ``or'' at the end;

(2) in paragraph (6), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

``(7) an identification document, false identification document, or a document-making implement (as those terms are defined in sections 1028 and 1029 of title 18) involved in a violation of section 1028 or 1029 of title 18;

``(8) a counterfeit access device, device-making equipment, or scanning receiver (as those terms are defined in sections 1028 and 1029 of title 18); or

``(9) a means of identification (as that term is defined in section 1036) involved in a violation of section 1036.".

(c) Restitution.--Section 3663A of title 18, United States Code, is amended--

(1) in subsection (c)(1)(A)--

(A) in clause (ii), by striking ``or'' at the end;

(B) in clause (iii), by striking ``and'' at the end and inserting ``or''; and

(C) by adding at the end the following:

``(iv) an offense described in section 1036 (relating to identity fraud); and''; and

(2) by adding at the end the following:

``(e) Identity Fraud.--Making restitution to a victim under this section for an offense described in section 1036 (relating to identity fraud) may include payment for any costs, including attorney fees, incurred by the victim--

``(1) in clearing the credit history or credit rating of the victim; or

``(2) in connection with any civil or administrative proceeding to satisfy any debt, lien, or other obligation of the victim arising as a result of the actions of the defendant.".

(d) Identity Fraud Information and Study; Inclusion in Suspicious Activity Reports.--

(1) Definitions.--In this subsection--

(A) the term ``financial institution'' has the same meaning as in section 20 of title 18, United States Code; and

(B) the term ``identity fraud'' means an offense described in section 1036 of title 18, United States Code (as added by subsection (a) of this section).

(2) Identity fraud information.--Beginning not later than

60 days after the date of enactment of this Act, the United States Secret Service of the Department of the Treasury and the Federal Bureau of Investigation of the Department of Justice, in consultation with financial institutions and other interested private entities, shall collect and maintain information and statistical data relating to--

(A) the number of identity fraud offenses investigated;

(B) the number of prosecutions and convictions for identity fraud; and

(C) any information provided by State and local law enforcement agencies relating to the investigation of identity fraud.

(3) Identity fraud study.--Not later than 18 months after the date of enactment of this Act, the Secretary of the Treasury, the Chairman of the Federal Trade Commission, the Attorney General, and the Postmaster General shall--

(A) conduct a comprehensive study of--

(i) the nature, extent, and causes of identity fraud; and

(ii) the threat posed by identity fraud to--

(I) financial institutions and payment systems; and

(II) consumer safety and privacy; and

(B) based on the results of that study, submit to Congress a report including an evaluation of the effectiveness of the provisions of this Act and the amendments made by this Act and, if necessary, specific recommendations for legislation to address the problem of identity fraud.

(4) Suspicious activity reports.--Not later than 90 days after the date of enactment of this Act, the Secretary of the Treasury shall promulgate such regulations as may be necessary to include identity fraud as a separate characterization of suspicious activity for purposes of reports by financial institutions of suspicious transactions under section 5318(g) of title 31, United States Code.

In https://www.congress.gov/bill/105th-congress/house-bill/3601/text [Última Consulta 4 de Jan. 2019]

Anexo III - UNITED STATES CODE, Title 18 (Crimes and Criminal Procedure) – Chapter 47 (Fraud and False Statements)

18 U.S. Code § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information

(a) Whoever, in a circumstance described in subsection (c) of this section—

(1)

knowingly and without lawful authority produces an identification document, authentication feature, or a false identification document;

(2)

knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority;

(3)

knowingly possesses with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents;

(4)

knowingly possesses an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States;

(5)

knowingly produces, transfers, or possesses a document-making implement or authentication feature with the intent such document-making implement or authentication feature will be used in the production of a false identification document or another document-making implement or authentication feature which will be so used;

(6)

knowingly possesses an identification document or authentication feature that is or appears to be an identification document or authentication feature of the United States or a sponsoring entity of an event designated as a special event of national significance which is stolen or produced without lawful authority knowing that such document or feature was stolen or produced without such authority;

(7)

knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any

unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law; or

(8)

knowingly traffics in false or actual authentication features for use in false identification documents, document-making implements, or means of identification;

shall be punished as provided in subsection (b) of this section.

(b) The punishment for an offense under subsection (a) of this section is—

(1)except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 15 years, or both, if the offense is—

(A)the production or transfer of an identification document, authentication feature, or false identification document that is or appears to be—

(i)

an identification document or authentication feature issued by or under the authority of the United States; or

(ii)

a birth certificate, or a driver's license or personal identification card;

(B)

the production or transfer of more than five identification documents, authentication features, or false identification documents;

(C)

an offense under paragraph (5) of such subsection; or

(D)

an offense under paragraph (7) of such subsection that involves the transfer, possession, or use of 1 or more means of identification if, as a result of the offense, any individual committing the offense obtains anything of value aggregating $1,000 or more during any 1-year period;

(2)except as provided in paragraphs (3) and (4), a fine under this title or imprisonment for not more than 5 years, or both, if the offense is—

(A)

any other production, transfer, or use of a means of identification, an identification document,,[1] authentication feature, or a false identification document; or

(B)

an offense under paragraph (3) or (7) of such subsection;

(3)a fine under this title or imprisonment for not more than 20 years, or both, if the offense is committed—

(A)

to facilitate a drug trafficking crime (as defined in section 929(a)(2));

(B)

in connection with a crime of violence (as defined in section 924(c)(3)); or

(C)

after a prior conviction under this section becomes final;

(4)

a fine under this title or imprisonment for not more than 30 years, or both, if the offense is committed to facilitate an act of domestic terrorism (as defined under section 2331(5) of this title) or an act of international terrorism (as defined in section 2331(1) of this title);

(5)

in the case of any offense under subsection (a), forfeiture to the United States of any personal property used or intended to be used to commit the offense; and

(6)

a fine under this title or imprisonment for not more than one year, or both, in any other case.

(c) The circumstance referred to in subsection (a) of this section is that—

(1)

the identification document, authentication feature, or false identification document is or appears to be issued by or under the authority of the United States or a sponsoring entity of an event designated as a special event of national significance or the document-making implement is designed or suited for making such an identification document, authentication feature, or false identification document;

(2)

the offense is an offense under subsection (a)(4) of this section; or

(3)either—

(A)

the production, transfer, possession, or use prohibited by this section is in or affects interstate or foreign commerce, including the transfer of a document by electronic means; or

(B)

the means of identification, identification document, false identification document, or document-making implement is transported in the mail in the course of the production, transfer, possession, or use prohibited by this section.

(d) In this section and section 1028A—

(1)

the term "authentication feature" means any hologram, watermark, certification, symbol, code, image, sequence of numbers or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified;

(2)

the term "document-making implement" means any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement;

(3)

the term "identification document" means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a sponsoring entity of an event designated as a special event of national significance, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;

(4)the term "false identification document" means a document of a type intended or commonly accepted for the purposes of identification of individuals that—

(A)

is not issued by or under the authority of a governmental entity or was issued under the authority of a governmental entity but was subsequently altered for purposes of deceit; and

(B)

appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a sponsoring entity of an event designated by the President as a special event of national significance, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization;

(5)the term "false authentication feature" means an authentication feature that—

(A)

is genuine in origin, but, without the authorization of the issuing authority, has been tampered with or altered for purposes of deceit;

(B)

is genuine, but has been distributed, or is intended for distribution, without the authorization of the issuing authority and not in connection with a lawfully made identification document, document-making implement, or means of identification to which such authentication feature is intended to be affixed or embedded by the respective issuing authority; or

(C)

appears to be genuine, but is not;

(6)the term "issuing authority"—

(A)

means any governmental entity or agency that is authorized to issue identification documents, means of identification, or authentication features; and

(B)

includes the United States Government, a State, a political subdivision of a State, a sponsoring entity of an event designated by the President as a special event of national significance, a foreign government, a political subdivision of a foreign government, or an international government or quasi-governmental organization;

(7)the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

(A)

name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(B)

unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(C)

unique electronic identification number, address, or routing code; or

(D)

telecommunication identifying information or access device (as defined in section 1029(e));

(8)

the term "personal identification card" means an identification document issued by a State or local government solely for the purpose of identification;

(9)

the term "produce" includes alter, authenticate, or assemble;

(10)

the term "transfer" includes selecting an identification document, false identification document, or document-making implement and placing or directing the placement of such identification document, false identification document, or document-making implement on an online location where it is available to others;

(11)

the term "State" includes any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession, or territory of the United States; and

(12)the term "traffic" means—

(A)

to transport, transfer, or otherwise dispose of, to another, as consideration for anything of value; or

(B)

to make or obtain control of with intent to so transport, transfer, or otherwise dispose of.

(e)

This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States, or any activity authorized under chapter 224 of this title.

(f)ATTEMPT AND CONSPIRACY.—

Any person who attempts or conspires to commit any offense under this section shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy.

(g)FORFEITURE PROCEDURES.—

The forfeiture of property under this section, including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the provisions of section 413 (other than subsection (d) of that section) of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853).

(h)FORFEITURE; DISPOSITION.—

In the circumstance in which any person is convicted of a violation of subsection (a), the court shall order, in addition to the penalty prescribed, the forfeiture and destruction or other disposition of all illicit authentication features, identification documents, document-making implements, or means of identification.

(i)RULE OF CONSTRUCTION.—

For purpose of subsection (a)(7), a single identification document or false identification document that contains 1 or more means of identification shall be construed to be 1 means of identification.

In https://www.law.cornell.edu/uscode/text/18/1028 [Última Consulta 4 de Jan. 2019]

18 U.S. Code § 1028A - Aggravated identity theft

(a)OFFENSES.—

(1)IN GENERAL.—

Whoever, during and in relation to any felony violation enumerated in subsection (c), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years.

(2)TERRORISM OFFENSE.—

Whoever, during and in relation to any felony violation enumerated in section 2332b(g)(5)(B), knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person or a false identification document shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 5 years.

In https://www.law.cornell.edu/uscode/text/18/1028A [Última Consulta 4 de Jan. 2019]

Section 152a
Counterfeiting of debit cards, etc, cheques, and promissory notes

(1) Whosoever for the purpose of deception in legal commerce or to facilitate such deception

1. counterfeits or alters domestic or foreign payment cards, cheques or promissory notes; or

2. procures for himself or another, offers for sale, gives to another or uses such counterfeit cards, cheques, or promissory notes

shall be liable to imprisonment not exceeding five years or a fine.

(2) The attempt shall be punishable.

(3) If the offender acts on a commercial basis or as a member of a gang whose purpose is the continued commission of offences under subsection (1) above the penalty shall be imprisonment from six months to ten years.

(4) Payment cards within the meaning of subsection (1) above are cards

1. which are provided by a credit or financial services institution, and

2. which are specially protected against imitation through design or coding.

(5) Section 149 to the extent that it refers to the counterfeiting of stamps and section 150(2) shall apply mutatis mutandis.

In https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1422 [Última Consulta 4 de Jan. 2019]

Section 202b
Phishing

Whosoever unlawfully intercepts data (section 202a(2)) not intended for him, for himself or another by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility, shall be liable to imprisonment not exceeding two years or a fine, unless the offence incurs a more severe penalty under other provisions.

Section 202c
Acts preparatory to data espionage and phishing

(1) Whosoever prepares the commission of an offence under section 202a or section 202b by producing, acquiring for himself or another, selling, supplying to another, disseminating or making otherwise accessible

1. passwords or other security codes enabling access to data (section 202a(2)), or

2. software for the purpose of the commission of such an offence,

shall be liable to imprisonment not exceeding one year or a fine.

(2) Section 149(2) and (3) shall apply mutatis mutandis.

In https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1757 [Última Consulta 4 de Jan. 2019]

ANEXO V - Código Penal (Espanha)

TÍTULO XVIII De las falsedades

CAPÍTULO I De la falsificación de moneda y efectos timbrados

Artículo 386. 1. Será castigado con la pena de prisión de ocho a doce años y multa del tanto al décuplo del valor aparente de la moneda: 1.º El que altere la moneda o fabrique moneda falsa. 2.º El que introduzca en el país o exporte moneda falsa o alterada. 3.º El que transporte, expenda o distribuya moneda falsa o alterada con conocimiento de su falsedad. 2. Si la moneda falsa fuera puesta en circulación se impondrá la pena en su mitad superior. La tenencia, recepción u obtención de moneda falsa para su expedición o distribución o puesta en circulación será castigada con la pena inferior en uno o dos grados, atendiendo al valor de aquélla y al grado de connivencia con el falsificador, alterador, introductor o exportador. 3. El que habiendo recibido de buena fe moneda falsa la expenda o distribuya después de constarle su falsedad será castigado con la pena de prisión de tres a seis meses o multa de seis a veinticuatro meses. No obstante, si el valor aparente de la moneda no excediera de 400 euros, se impondrá la pena de multa de uno a tres meses. 4. Si el culpable perteneciere a una sociedad, organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de estas actividades, el juez o tribunal podrá imponer alguna o algunas de las consecuencias previstas en el artículo 129 de este Código. 5. Cuando, de acuerdo con lo establecido en el artículo 31 bis, una persona jurídica sea responsable de los anteriores delitos, se le impondrá la pena de multa del triple al décuplo del valor aparente de la moneda.

Artículo 387. A los efectos del artículo anterior, se entiende por moneda la metálica y el papel moneda de curso legal y aquella que previsiblemente será puesta en curso legal. Se equipararán a la moneda nacional las de otros países de la Unión Europea y las extranjeras. Se tendrá igualmente por moneda falsa aquella que, pese a ser realizada en las instalaciones y con los materiales legales, se realiza incumpliendo, a sabiendas, las condiciones de emisión que hubiere puesto la autoridad competente o cuando se emita no existiendo orden de emisión alguna.

Artículo 388. La condena de un Tribunal extranjero, impuesta por delito de la misma naturaleza de los comprendidos en este capítulo, será equiparada a las sentencias de los Jueces o Tribunales españoles a los efectos de reincidencia, salvo que el antecedente penal haya sido cancelado o pudiese serlo con arreglo al Derecho español.

Artículo 389. El que falsificare o expendiere, en connivencia con el falsificador, sellos de correos o efectos timbrados, o los introdujera en España conociendo su falsedad, será castigado con la pena de prisión de seis meses a tres años. El adquirente de buena fe de sellos de correos o efectos timbrados que, conociendo su falsedad, los distribuyera o utilizara será castigado con la pena de prisión de tres a seis meses o multa de seis a veinticuatro meses. No obstante, si el valor aparente de los sellos o efectos timbrados no excediera de 400 euros, se impondrá la pena de multa de uno a tres meses.

CAPÍTULO II De las falsedades documentales

Sección 1.ª De la falsificación de documentos públicos, oficiales y mercantiles y de los despachos transmitidos por servicios de telecomunicación

Artículo 390. 1. Será castigado con las penas de prisión de tres a seis años, multa de seis a veinticuatro meses e inhabilitación especial por tiempo de dos a seis años, la autoridad o funcionario público que, en el ejercicio de sus funciones, cometa falsedad: 1.º Alterando un documento en alguno de sus elementos o requisitos de carácter esencial. 2.º Simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad. 3.º Suponiendo en un acto la intervención de personas que no la han tenido, o atribuyendo a las que han intervenido en él declaraciones o manifestaciones diferentes de las que hubieran hecho. 4.º Faltando a la verdad en la narración de los hechos. 2. Será castigado con las mismas penas a las señaladas en el apartado anterior el responsable de cualquier confesión religiosa que incurra en alguna de las conductas descritas en los números anteriores, respecto de actos y documentos que puedan producir efecto en el estado de las personas o en el orden civil.

Artículo 391. La autoridad o funcionario público que por imprudencia grave incurriere en alguna de las falsedades previstas en el artículo anterior o diere lugar a que otro las cometa, será castigado con la pena de multa de seis a doce meses y suspensión de empleo o cargo público por tiempo de seis meses a un año.

Artículo 392. 1. El particular que cometiere en documento público, oficial o mercantil, alguna de las falsedades descritas en los tres primeros números del apartado 1 del artículo 390, será castigado con las penas de prisión de seis meses a tres años y multa de seis a doce meses. 2. Las mismas penas se impondrán al que, sin haber intervenido en la falsificación, traficare de cualquier modo con un documento de identidad falso. Se impondrá la pena de

prisión de seis meses a un año y multa de tres a seis meses al que hiciere uso, a sabiendas, de un documento de identidad falso. Esta disposición es aplicable aun cuando el documento de identidad falso aparezca como perteneciente a otro Estado de la Unión Europea o a un tercer Estado o haya sido falsificado o adquirido en otro Estado de la Unión Europea o en un tercer Estado si es utilizado o se trafica con él en España.

Artículo 393. El que, a sabiendas de su falsedad, presentare en juicio o, para perjudicar a otro, hiciere uso de un documento falso de los comprendidos en los artículos precedentes, será castigado con la pena inferior en grado a la señalada a los falsificadores.

Artículo 394. 1. La autoridad o funcionario público encargado de los servicios de telecomunicación que supusiere o falsificare un despacho telegráfico u otro propio de dichos servicios, incurrirá en la pena de prisión de seis meses a tres años e inhabilitación especial por tiempo de dos a seis años. 2. El que, a sabiendas de su falsedad, hiciere uso del despacho falso para perjudicar a otro, será castigado con la pena inferior en grado a la señalada a los falsificadores.

Sección 2.ª De la falsificación de documentos privados

Artículo 395. El que, para perjudicar a otro, cometiere en documento privado alguna de las falsedades previstas en los tres primeros números del apartado 1 del artículo 390, será castigado con la pena de prisión de seis meses a dos años.

Artículo 396. El que, a sabiendas de su falsedad, presentare en juicio o, para perjudicar a otro, hiciere uso de un documento falso de los comprendidos en el artículo anterior, incurrirá en la pena inferior en grado a la señalada a los falsificadores.

Sección 3.ª De la falsificación de certificados

Artículo 397. El facultativo que librare certificado falso será castigado con la pena de multa de tres a doce meses.

Artículo 398. La autoridad o funcionario público que librare certificación falsa con escasa trascendencia en el tráfico jurídico será castigado con la pena de suspensión de seis meses a dos años. Este precepto no será aplicable a los certificados relativos a la Seguridad Social y a la Hacienda Pública.

Artículo 399. 1. El particular que falsificare una certificación de las designadas en los artículos anteriores será castigado con la pena de multa de tres a seis meses. 2. La misma pena se impondrá al que hiciere uso, a sabiendas, de la certificación, así como al que, sin haber intervenido en su falsificación, traficare con ella de cualquier modo. 3. Esta disposición es aplicable aun cuando el certificado aparezca como perteneciente a otro Estado de la Unión Europea o a un tercer Estado o haya sido falsificado o adquirido en otro Estado de la Unión Europea o en un tercer Estado si es utilizado en España.

Sección 4.ª De la falsificación de tarjetas de crédito y débito y cheques de viaje

Artículo 399 bis. 1. El que altere, copie, reproduzca o de cualquier otro modo falsifique tarjetas de crédito o débito o cheques de viaje, será castigado con la pena de prisión de cuatro a ocho años. Se impondrá la pena en su mitad superior cuando los efectos falsificados afecten a una generalidad de personas o cuando los hechos se cometan en el marco de una organización criminal dedicada a estas actividades. Cuando de acuerdo con lo establecido en el artículo 31 bis una persona jurídica sea responsable de los anteriores delitos, se le impondrá la pena de multa de dos a cinco años. Atendidas las reglas establecidas en el artículo 66 bis, los jueces y tribunales podrán asimismo imponer las penas recogidas en las letras b) a g) del apartado 7 del artículo 33. 2. La tenencia de tarjetas de crédito o débito o cheques de viaje falsificados destinados a la distribución o tráfico será castigada con la pena señalada a la falsificación. 3. El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito o cheques de viaje falsificados será castigado con la pena de prisión de dos a cinco años.

CAPÍTULO III Disposiciones generales

Artículo 400. La fabricación, recepción, obtención o tenencia de útiles, materiales, instrumentos, sustancias, datos y programas informáticos, aparatos, elementos de seguridad, u otros medios específicamente destinados a la comisión de los delitos descritos en los Capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 400 bis. En los supuestos descritos en los artículos 392, 393, 394, 396 y 399 de este Código también se entenderá por uso de documento, despacho, certificación o **documento de identidad falsos** el uso de los correspondientes documentos, despachos, certificaciones o documentos de identidad auténticos realizado por quien no esté legitimado para ello.

CAPÍTULO IV De la usurpación del estado civil

Artículo 401. El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años.

CAPÍTULO V De la usurpación de funciones públicas y del intrusismo

Artículo 402. El que ilegítimamente ejerciere actos propios de una autoridad o funcionario público atribuyéndose carácter oficial, será castigado con la pena de prisión de uno a tres años.

Artículo 402 bis. El que sin estar autorizado usare pública e indebidamente uniforme, traje o insignia que le atribuyan carácter oficial será castigado con la pena de multa de uno a tres meses.

Artículo 403. 1. El que ejerciere actos propios de una profesión sin poseer el correspondiente título académico expedido o reconocido en España de acuerdo con la legislación vigente, incurrirá en la pena de multa de doce a veinticuatro meses. Si la actividad profesional desarrollada exigiere un título oficial que acredite la capacitación necesaria y habilite legalmente para su ejercicio, y no se estuviere en posesión de dicho título, se impondrá la pena de multa de seis a doce meses. 2. Se impondrá una pena de prisión de seis meses a dos años si concurriese alguna de las siguientes circunstancias: a) Si el culpable, además, se atribuyese públicamente la cualidad de profesional amparada por el título referido. b) Si el culpable ejerciere los actos a los que se refiere el apartado anterior en un local o establecimiento abierto al público en el que se anunciare la prestación de servicios propios de aquella profesión.

In
https://www.boe.es/legislacion/codigos/codigo.php?id=038_Codigo_Penal_y_legislacion_complementaria&modo=1 [Última Consulta 4 de Jan. 2019]

Anexo VI – Código Penal Para el Distrito Federal (México)

CAPÍTULO III USURPACIÓN DE IDENTIDAD Artículo 211 Bis. - Al que por cualquier medio usurpe, con fines ilícitos, la identidad de otra persona, u otorgue su consentimiento para llevar a cabo la usurpación en su identidad, se le impondrá una pena de uno a cinco años de prisión y de cuatrocientos a seiscientos días multa. Se aumentaran en una mitad las penas previstas en el párrafo anterior, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito establecido en el presente artículo.

In http://www.aldf.gob.mx/archivo-d261f65641c3fc71b354aaf862b9953a.pdf [Última Consulta 4 de Jan. 2019]