# A USURPAÇÃO DA CIBERIDENTIDADE

**FLÁVIO MANUEL CARNEIRO DA SILVA**

PORTO

2014

UNIVERSIDADE CATÓLICA PORTUGUESA
CENTRO REGIONAL DO PORTO
ESCOLA DE DIREITO

# A USURPAÇÃO DA CIBERIDENTIDADE

**FLÁVIO MANUEL CARNEIRO DA SILVA**

*Dissertação de Mestrado em Direito Criminal, realizada sob a orientação do Exmo. Senhor Professor Doutor José M. Damião da Cunha*

Porto
2014

*À minha madrinha*

*A coragem é a primeira das qualidades humanas porque garante todas as outras.*
Aristóteles

# AGRADECIMENTOS

*Tudo parece impossível até que seja feito.*
Nelson Mandela

Agradeço ao Senhor Professor José Manuel Damião da Cunha por ter aceitado orientar esta dissertação, o que fez com grande profissionalismo e com contagiante vigor, e por me ter lembrado, no momento certo, que importa mais ao Direito como ele deve ser e menos como ele é.

À minha patrona, Senhora Dra. Poliana Pinto Ribeiro, pela amizade, pela paciência e pelo apoio que demonstrou e demonstra todos os dias, em todos os desafios a que me proponho.

Ao meu avô, que é o meu reduto protetor e a razão elementar para que o sonho fosse objetivo, e o objetivo realidade.

Aos meus pais, que acreditam incondicionalmente em mim e que me fazem perceber, a todo o momento, a importância da responsabilidade.

À Ana Lu, pela força e incentivo inesgotáveis que me transmitiu e principalmente pelo carinho e dedicação sentidos e vividos.

# RESUMO

Esta dissertação problematiza o fenómeno da usurpação da identidade virtual – ou *ciberidentidade* -, numa perspetiva jurídico-penal.

Constatou-se que é fácil utilizar a identidade virtual de outra pessoa sem o seu consentimento, violando assim um direito fundamental, de caracter eminentemente pessoal.

Perante a verificação que o Direito Penal não defende, de *iure condendo*, a ciberidentidade enquanto bem jurídico autónomo, apresentamos argumentos favoráveis e desfavoráveis à autonomização do crime de usurpação da ciberidentidade, culminando com uma proposta dogmática do (futuro?) tipo legal de crime.

**Palavras-Chave:** ciberidentidade, usurpação, Internet, criminalidade informática.

# ABSTRACT

This dissertation discusses the phenomenon of online identity (ciberidentity) theft from a criminal perspective.

It was noted how easy is to use the virtual identity of another person, without their consent, thereby violating a fundamental right, whose nature is eminently personal.

According to the fact that Criminal Law does not protect the ciberidentity, as an autonomous legal right, we introduce both favorable and unfavorable arguments for the criminalization of ciberidentity theft, and we present a dogmatic proposal of the (future?) crime.



**Keywords:** ciberidentity, theft, Internet, cybercrime.

# ABREVIATURAS

| | |
|---|---|
| **Ac.** | Acórdão |
| **Art(s).** | Artigo(s) |
| **BI** | Bilhete de Identidade |
| **CC** | Código Civil |
| **Cfr.** | Confira, confronte |
| **consult.** | Consultada |
| **CP** | Código Penal |
| **CRP** | Constituição da República Portuguesa |
| **FDUNL** | Faculdade de Direito da Universidade Nova de Lisboa |
| **IP** | *Internet Protocol* |
| **Ob.** | Obra |
| **p.** | Página |
| **pp.** | Páginas |
| **ROA** | Revista de Ordem dos Advogados |
| **RPCC** | Revista Portuguesa de Ciência Criminal |
| **últ.** | Última |

# ÍNDICE

# INTRODUÇÃO

*Think about what people are doing on Facebook today. They're keeping up with their friends and family, but they're also building an image and identity for themselves, which in a sense is their brand. They're connecting with the audience that they want to connect to. It's almost a disadvantage if you're not on it now.*

Mark Zuckerberg

A dissertação que aqui se apresenta problematiza a (ir)responsabilidade penal pela usurpação da identidade virtual. Com rigor, indagaremos sobre a dignidade penal de um bem jurídico autónomo e pessoal - a identidade virtual ou *ciberidentidade* -, e a consequente (des)necessidade de criminalização dos comportamentos que o violam.

Finda a primeira década do século XXI, afigura-se ultrapassada a discussão em torno da carência e capacidade do Direito na regulação social *online*, impondo-se reflexão e ação na prossecução desse fim. Afinal vivemos numa Sociedade de Informação e a Internet não é uma mera rede aberta de comunicações mundial, é a digitalização da sociedade em todas as suas dimensões.

Por inerência o problema da usurpação da identidade estende-se ao ciberespaço, assumindo aí contornos dissemelhantes e porventura proporções mais gravosas, e como tal, colocando em crise as soluções clássicas da problemática.

No Capítulo I começaremos por concetualizar juridicamente a *ciberidentidade* e indagar sobre a sua consagração como bem jurídico-penal pessoal e autónomo, com acolhimento jurídico-constitucional. Efetuaremos, ainda, uma brevíssima súmula da evolução histórica da ciberidentidade, em pouco mais de 20 anos de Internet em Portugal.

No Capítulo II analisaremos o fenómeno da usurpação da ciberidentidade, onde procuraremos identificar o problema e abordar as suas implicações fenomenológicas e jurídicas, através da exposição das diferentes condutas que lhe são subsumíveis e das consequências típicas desse comportamento ilícito.

Perante a constatação que a usurpação da ciberidentidade *tout court* não é um ilícito criminal autónomo, o Capítulo III fica reservado à análise da generosidade dessa solução legal, através de apresentação de argumentos favoráveis e desfavoráveis à criminalização do comportamento.

Ainda sem revelar a nossa opinião quanto à necessidade de criminalização, no Capítulo IV avançamos com uma proposta dogmática de um tipo de crime que tutele a identidade virtual, tecendo considerações quanto ao bem jurídico a proteger e os elementos objetivos e subjetivos do tipo de ilícito, que a existir, deverão constar, *de iure constituendo*, do crime de usurpação da ciberidentidade.

Culminaremos esta dissertação com a nossa visão quanto à (des)necessidade de criminalização autónoma do fenómeno, enfatizando que o principal propósito do presente trabalho é introduzir na literatura jurídica portuguesa a discussão sobre um tema atual e muito pouco explorado.

# CAPÍTULO I

## A CIBERIDENTIDADE

### 1. Uma aproximação ao conceito jurídico da Ciberidentidade

No âmbito do estudo aqui apresentado, importa definir, antes de tudo o mais, o que é a ciberidentidade para a ciência estrita do direito penal, torno-a um conceito operante na aplicação do direito.

A identidade pessoal tem vindo a ser definida como "*aquilo que caracteriza cada pessoa enquanto unidade individualizada que se diferencia de todas as outras pessoas por uma determinada vivência pessoal*" (**1**).

Em defesa do princípio geral do respeito pela dignidade e personalidade humanas, o artigo 26.º, n.º 1 da CRP postula o direito à identidade pessoal que visa "*garantir aquilo que identifica cada pessoa como indivíduo, singular e irredutível*" (**2**). Este direito abrange o direito ao nome – art. 72.º do CC -, que engloba o *direito a ter um nome, de não ser privado dele, de o defender e de impedir que outrem o utilize, sem prejuízo dos casos de homonímia* (**3**).

No plano infra-constitucional, a identidade civil traduz-se no conjunto de dados pessoais individualizadores de cada cidadão (*cfr.* art. 1.º, n.º 1 da Lei 33/99, de 18 de Maio), onde certamente se incluí o nome, a filiação, a data de nascimento, a naturalidade, o sexo, a residência, a fotografia e a assinatura (**4**).

---

[1] JORGE MIRANDA e RUI MEDEIROS, *Constituição da República Portuguesa Anotada*, p. 609.

[2] CANOTILHO, J. J. GOMES e MOREIRA, VITAL, *Constituição da República Portuguesa Anotada*, p. 462.

[3] *Ibidem*.

[4] *Cfr.* art. 5.º da Lei 33/99, de 18 de Maio (Elementos identificadores do BI).

Naturalmente que enquanto direito de personalidade, a identidade pessoal se estende à Internet, que é um importante meio de relacionamento económico, cultural e social caracterizador da Sociedade de Informação em que vivemos.

No entanto, dadas as vastas implicações jurídicas da utilização da informática ([5]), as considerações clássicas sobre a identidade pessoal relevam-se insuficientes ([6]) para responder à questão: **para o direito, o que é a ciberidentidade?**

SHERRY TURTLE, pioneira nos estudos sobre a identidade na Internet, identificou três importantes características da ciberidentidade: *multiplicidade*, *invisibilidade* e *anonimato* ([7]).

A multiplicidade refere-se à maneira pela qual cada um pode manifestar várias instâncias de si mesmo no ciberespaço ([8]). Por outras palavras, a multiplicidade traduz-se na possibilidade de uma mesma pessoa criar um número plural de identidades, também designadas por *máscaras* ([9]).

A invisibilidade alude à possibilidade de qualquer pessoa escolher e se autoidentificar na Internet com características que podem não ter reflexo na vida real ([10]).

Por seu turno, o anonimato exprime a "*não identificabilidade da pessoa física do utilizador que acede à Internet*" ([11]).

---

[5] *Cfr.* ISABEL REIS GARCIA, "Do direito da informática a um anteprojecto de lei de proteção de dados pessoais", pp. 979-1003. A Autora chega a defender a criação de um novo ramo do direito.

[6] JOHN PERRY BARLOW *in A Declaration of Independence of Cyberspace*, proclamou: "*legal concepts of property, expression, identity, movement and context do not apply to us. They are based on matter. There is no matter here*".

[7] SHERRY TURTLE, *Life on the Screen: Identity in the Age of the Internet*, p. 14 *apud* MARK FRANCIS GROVER, *A theory of unified online identity*, p. 16.

[8] *Cfr.* MARK FRANCIS GROVER, *op. cit.*, p. 48.

[9] Termo avançado por DORIAN WISZNIEWSKI e RICHARD COYNE na ob. *Mask and Identity: The Hermeneutics of Self-Construction*.

[10] SHERRY TURTLE, *Constructions and Reconstructions of the Self in Virtual Reality*, *Cyber Reader: Critical Writings For the Digital Era*, p. 212 *apud* MARK FRANCIS GROVER, *op. cit.*, p. 22.

De um ponto de vista estritamente jurídico dificilmente alguma destas características enformará o conceito que procuramos, na medida em que [essas características] espelham a possível desconexão entre a identidade pessoal e a identidade virtual.

Em rigor, estas particularidades permitem percecionar um verdadeiro *direito ao anonimato* coexistente com o direito à identidade pessoal na Internet.

O anonimato na Internet é a consequência lógica da identificação *online* ser efetuada pelo *IP – Internet Protocol*, que é um protocolo de comunicação que identifica um computador na Internet, mas não a concreta pessoa que a está a *navegar* nesse computador (**12**).

Esta possibilidade de não ser reconhecido, de não se identificar e de não ser identificado na Internet constitui um direito inalienável (**13**), enquanto manifestação do direito à reserva da intimidade da vida privada (**14**) (**15**), constitucionalmente acolhido no n.º 1 do artigo 26.º da Lei Fundamental.

---

11 JOÃO FACHANA, *A responsabilidade civil pelos conteúdos ilícitos colocados e difundidos na Internet*, p. 67.

12 De uma forma genérica, todos os computadores ligados à internet possuem um endereço de IP (e.g.: 123.45.67.89) que os identifica de forma única, assim permitindo a comunicação com outros computadores através da emissão e receção de dados.

13 *Cfr.* JOEL TIMÓTEO PEREIRA, *Direito da Internet e Comércio Eletrónico*, p. 20. O Autor refere que no Parecer n.º 13/96 do Conselho Consultivo da Procuradoria Geral da República, publicado no DR, II, n.º 286, de 12.12.97, p. 15247 ss, se sustentou que: "*No cruzamento do direito à identidade pessoal, que inclui fundamentalmente o direito à intimidade da vida privada, poder-se-á extrair uma proteção constitucional do anonimato*".

14 Este direito tem também consagração 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.

15 Segundo GOMES CANOTILHO e VITAL MOREIRA, op. cit. p. 181, o direito à reserva da intimidade da vida privada e familiar inclui dois direitos menores: o direito a impedir o acesso de estranhos a informações sobre a vida privada e familiar; e o direito a que ninguém divulgue as informações que tenha sobre a vida privada e familiar de outrem.

Muito recentemente o Tribunal de Justiça da União Europeia abriu caminho para o acolhimento do *direito a ser esquecido na Internet* (**16**). A Comissão Europeia propôs, em 2012, uma reforma global na regulamentação da proteção de dados, onde incluiu o direito ao esquecimento na Internet, nos termos do art. 17.º Proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Entretanto o Parlamento Europeu já aprovou, com alterações, a proposta apresentada pela Comissão (**17**).

Estamos em posição para concluir que a identidade virtual se manifesta empiricamente de forma tão variada e flexível que pode mesmo traduzir-se na não identificabilidade pessoal do utilizador.

Uma tal conceção jurídica da ciberidentidade – que chega a englobar o próprio anonimato - não se adequa às funcionalidades próprias da dogmática jurídico-penal e inviabiliza as suas finalidades prático-normativas.

Desde logo, tornou-se para nós claro que o *anonimato* não pode ser uma manifestação da ciberidentidade, mas antes o seu oposto.

Ora, 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.

Definimos, assim, ciberidentidade, no âmbito do presente trabalho, como o **conjunto de elementos físicos, fisiológicos, psíquicos, económicos, culturais e sociais de um utilizador, constantes na Internet, que correspondem à identidade real da própria pessoa.**

---

16 Informação disponível em http://www.bit.pt/tribunal-europeu-defende-direito-ser-esquecido/ (últ. vez consult. em 22 de Maio de 2014).

17 De acordo com a informação disponibilizada em http://www.europarl.europa.eu/news/pt/news-room/content/20140307IPR38204/html/Parlamento-Europeu-refor%C3%A7a-prote%C3%A7%C3%A3o-dos-dados-pessoais-dos-cidad%C3%A3os (últ. vez consult. em 22 de Maio de 2014).

## **2.** Proteção Constitucional da Ciberidentidade

A Constituição da República Portuguesa, enquanto lei fundamental da sociedade portuguesa, estabelece os direitos, liberdades e garantias que devem ser respeitados no recurso às "novas" tecnologias, *maxime* a Internet.

O *supra* mencionado art. 26.º da Lei Fundamental (Outros Direitos Pessoais) consagra nove direitos, de entre os quais o direito à identidade pessoal e o direito à reserva da intimidade da vida privada e familiar.

A Ciberidentidade como a definimos – uma extensão da identidade pessoal na Internet -, encontra neste preceito constitucional uma invariável proteção. Ou seja, qualquer ato atentatório do direito à ciberidentidade será *a priori* ilícito.

O direito ao nome, corolário do direito à identidade pessoal, está bem patente na realidade virtual, porquanto é possível a uma instituição, empresa ou pessoa identificar-se na Web através do registo e utilização de *nomes de domínio*.

Sinteticamente, o sistema de domínios na web (Domain Names System) faz corresponder a um determinado *IP* um nome alfanumérico (e. g. tribunalconstitucional.pt), facilitando a memorização do endereço e consequentemente a navegação na web. No fundo, este sistema evita a necessidade dos utilizadores memorizarem a cadeia de dígitos de um IP, tarefa insofismavelmente morosa e de difícil concretização (**[18]**).

Contudo, a proteção da ciberidentidade não se esgota com o direito ao nome, antes se estende a um conjunto de dados pessoais informatizados.

[18] Algumas implicações jurídicas da atribuição de nomes de domínio foram sintetizadas por JOEL TIMÓTEO RAMOS PEREIRA, *op. cit.*, p. 13.

O art. 35.º da CRP consagra um direito à autodeterminação informativa que visa "*evitar intromissões abusivas na vida privada das pessoas através da recolha e tratamento de dados pessoais informatizados*" (**19**).

Segundo ALBERTO MARTINS, a autodeterminação informacional é o direito de cada cidadão "*decidir autónoma e livremente, quando, e dentro de que limites, os dados da sua vida pessoal são suscetíveis de informatização ou publicidade*" (**20**).

De acordo com GOMES CANOTILHO e VITAL MOREIRA, o art. 35.º CRP elenca uma série de direitos fundamentais com vista à "*defesa contra o tratamento informático de dados pessoais*" (**21**): o direito ao controlo dos dados pessoais (n.º 1); o direito à não difusão dos dados (n.º 2) e o direito ao não tratamento informático de certos dados (n.º 3). Finalmente, o n.º 5 da norma constitucional proíbe a atribuição de um número nacional único que "*funciona como garantia daqueles direitos, dificultando o tratamento informático de dados pessoais e a sua interconexão, que seria facilitada com um identificador comum*" (**22**).

Ainda segundo estes autores, a proibição de tratamento informático de dados referentes à vida privada (art. 35.º, n.º 3 CRP) funciona como garantia do direito à reserva da intimidade da vida privada (**23**), não obstante o seu "*âmbito de proteção parecer mais extenso do que o do art. 26.º*" (**24**).

Todavia, a Lei Fundamental não define o que se deve entender por dados pessoais, apesar de consagrar a sua proteção. De acordo com a Convenção para a Proteção de Pessoas relativamente ao

---

19 JORGE MIRANDA e RUI MEDEIROS, *op. cit.*, p. 783.

20 ALBERTO MARTINS, Proteção de dados pessoais informatizados na Constituição da República Portuguesa, p. 431.

21 GOMES CANOTILHO e VITAL MOREIRA, *op. cit.*, anotação a este dispositivo.

22 *Ibidem*, p. 216.

23 *Ibidem*, p. 181.

24 HELENA MONIZ, Notas sobre a proteção de dados pessoais perante a informática, p. 245. Segundo a autora, esta diferente abrangência dos preceitos impõe a distinção entre dados sensíveis (colocados no âmbito da *intimidade da vida privada*) e dados pessoais (integrados no domínio da reserva da *vida privada*).

tratamento automatizado de dados de carácter pessoal, dado de carácter pessoal é "*qualquer informação relativa a uma pessoa singular identificada ou suscetível de identificação (titular dos dados)*" – art. 2.º, n.º 2.

No ordenamento jurídico nacional a Lei n.º 67/98, de 26 de Outubro (Lei da Proteção de Dados Pessoais) ([25]) define dados pessoais como "*qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ('titular dos dados')*", indicando que "*é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social*".

Segundo JOEL TIMÓTEO PEREIRA, estes dados "*são pessoais porque relativos à esfera não pública da vida – cfr. art. 181.º do CP -, com exceção dos dados íntimos que estão interditos de tratamento informático (origem racial, tendência sexual, doenças de carácter reservado, conceção política, religioso ou filosófica)*". Acrescenta que "*estes elementos não podem constar dos formulários existentes na Internet para registo em qualquer site ou para a prestação de qualquer serviço por esse site*" ([26]).

Partilhamos da opinião de PAULO GONÇALVES TEIXEIRA quando afirma que "*a proteção legal da identidade privilegia o ser humano (físico) que lhe dá corpo*" ([27]), mas sem que razões de economia expositiva nos permitam centrar no problema do tratamento jurídico da ciberidentidade das pessoas coletivas, acreditamos que as

---

[25] Este diploma legal transpôs para a ordem jurídica portuguesa a Diretiva n.º 95/46/CE, do PE e do Conselho, 24/10/95, relativa à proteção das pessoas singulares no que diz respeito ao tratamento dados pessoais e à livre circulação desses dados.

[26] JOEL TIMÓTEO PEREIRA, op. cit., p. 23.

[27] PAULO GONÇALVES TEIXEIRA, *O fenómeno do phishing - enquadramento jurídico-penal*, p. 27.

considerações tecidas nesta dissertação lhes são, *mutatis mutandis*, aplicáveis.

## **3.** CiberIdentidade: *Statu Quo*

A identidade no ciberespaço pode ser revelada de diversas formas, nomeadamente, através da biografia, de fotografias, ou informações pessoais.

Sempre que um cidadão se integra em redes sociais como o *Facebook* ou o *Twitter*, envia e recebe *e-mails*, frequenta *chats*, cria um *blog*, participa num fórum ou *newsletter*, ou simplesmente procede ao registo num *site* da web, pode manifestar a sua ciberidentidade (o que geralmente acontece).

Todos esses conceitos, plataformas e espaços sociais virtuais já não são novidade e imiscuíram-se tão profundamente na nossa vida que dispensam um trabalho de concetualização. Mais interesse desperta a evolução da relação entre a identidade real e a identidade virtual, e portanto, o progresso da ciberidentidade em pouco mais de vinte anos de Internet em Portugal.

Sendo certo que 1991 foi o ano zero da Internet entre nós (**28**), em meados de 1996 já se registavam 15 776 endereços de IP e 512 nomes de domínio (**29**), e no final de 2011 contavam-se mais de 2 800 000 endereços de IP diferentes (**30**). O número de utilizadores em Portugal e

---

28 Portugal ligou-se à Internet no Outono de 1991 como resultado do projeto "Serviço IP da RCCN", conduzido pela FCCN, então designada Fundação para o Desenvolvimento dos Meios Nacionais de Cálculo Científico.

29 *Cfr.* MARTINS, JOSÉ LEGATHEAUX, Evolução Tecnológica da Internet em Portugal, pp. 70 a 78.

30 Informação avançada por Akamai technologies, inc., *in* Status of Internet Report – Q4 of 2011.

no Mundo aumentou descontroladamente até hoje ([31]), e tudo indica que a tendência continuará a ser essa.

A massificação do uso da Internet é causa e consequência da evolução tecnológica e naturalmente a história da Internet relata a readaptação de serviços, a criação de novas funcionalidades e a mudança de tendências e popularidade na utilização de plataformas e *sites* na Web.

A forma como a ciberidentidade se manifesta nas diferentes plataformas *online* depende necessariamente da lógica de funcionamento desses serviços. Isto é, se um sistema de registo de utilizadores num *site* não admite a possibilidade de identificação visual, então forçosamente nenhum utilizador poderá ser identificado por uma determinada fotografia nesse espaço em concreto. Como é óbvio, cabe ao utilizador escolher que plataformas vão de encontro à sua preferência: desde uma rede social onde é possível verter em pleno a sua ciberidentidade a um *chat* de comunicação anónima.

No final dos anos noventa e nos primeiros anos do novo milénio, o Internet Relay Chat (IRC) tornou-se um dos principais protocolos de comunicação utilizado na Internet em Portugal. Milhares de utilizadores concentravam-se diariamente na primeira e principal rede portuguesa de IRC – A PTnet. O IRC é uma plataforma de comunicação em tempo real (*chat*), onde os utilizadores podem encetar conversações em canais abertos ou fechados com vários outros utilizadores em simultâneo, ou em privado com apenas outro utilizador.

Os utilizadores são identificados no IRC através de um *nickname* que pode ser registado (a partir da designação de *password*) para uso

---

[31] Entre a infindável quantidade de notícias que corroboram esta nossa afirmação, *vide*
http://tek.sapo.pt/noticias/telecomunicacoes/numero_de_utilizadores_de_banda_larga_movel_e_1351149.html;
http://www.marktest.com/wap/a/n/id~165b.aspx;
http://www.marktest.com/wap/a/n/id~1a70.aspx (últ. vez consult. em 22 de Maio de 2014).

exclusivo de determinada pessoa. Este sistema de identificação pelo *nickname* não cabe, nos termos atrás descritos, no conceito jurídico de ciberidentidade, sem detrimento da opção de cada um em divulgar os seus dados pessoais a outros utilizadores, que passam a associar aquele *nickname* a uma pessoa humana.

Em todo o caso, o IRC é um protocolo de comunicação que utiliza texto simples, não admitindo pois o emprego de fotografias ou avatares ([32]), nem a visualização de multimédia, além de ser relativamente fácil ser importunado por utilizadores mal intencionados e completamente anónimos.

Com o advento do MSN Messenger, nomeadamente por ser um *software* já incorporado nos sistemas operativos Windows, o IRC entrou em decadência. O *Messenger* trouxe novas funcionalidades, como a conversação áudio e vídeo, a integração com o serviço de *e-mail*, e proporcionava uma convivência social *online* circunscrita a amigos e conhecidos, circunstância que terá tido uma crucial importância para o aumento da confiança dos utilizadores na exposição da sua identidade. Aí os elementos enformadores da ciberidentidade empubesceram, constando do perfil dos utilizadores não só o *e-mail*, como a imagem, o nome, a voz, etc.

Presentemente, a esmagadora maioria dos utilizadores da Internet está integrado numa rede social virtual.

"*Uma rede social é uma estrutura social composta por pessoas ou organizações, conectadas por um ou vários tipos de interesses e que partilham valores e objetivos. Estas redes tendem a estar articuladas com as Novas Tecnologias de Informação podendo assentar numa*

---

[32] "*Em informática, avatar é um cibercorpo inteiramente digital, uma figura gráfica de complexidade variada que empresta sua vida simulada para o transporte identificatório de cibernautas para dentro dos mundos paralelos do ciberespaço*", *in* Wikipédia. Disponível em http://pt.wikipedia.org/wiki/Avatar_(realidade_virtual) (últ. vez consult. em 22 de Maio de 2014).

*plataforma online onde se estruturam estas relações sociais entre utilizadores".* (**33**)

São exemplos de redes sociais virtuais o *Facebook*, o *Twitter*, o *Google+*, o *MySpace*, o *LinkedIn*, o *Orkut*, entre muitos outros.

Pertencer a uma comunidade *online* é fácil, gratuito e contagiante. Utilizando o caso paradigmático do *Facebook*, que é a rede social mais utilizada em Portugal e no Mundo (**34**), é possível criar um perfil com todos os dados pessoais, profissionais, culturais e sociais, adicionar outros utilizadores como nossos amigos, publicar fotografias, vídeos, músicas e mensagens, comentar as publicações de amigos, conhecidos e desconhecidos, compartilhar publicações de outros utilizadores, conversar em tempo real, trocar ficheiros, utilizar a conversação via áudio e vídeo, criar grupos privados, páginas profissionais, recreativas e de lazer, enfim.

Se nos primórdios da Internet em Portugal, as comunidades virtuais eram utilizadas de forma anónima, quase anónima ou circunscrita a "verdadeiros" amigos e conhecidos, nas redes sociais é possível ter milhares de amigos virtuais, e é certamente comum ter uma rede de amizades com centenas de pessoas.

Como à partida tudo o que é publicado pelo utilizador, desde a data da criação da conta até ao momento atual, fica registado e acessível, a ciberidentidade assumiu uma abrangência completamente diferente. Deixou de se exteriorizar como elementos pessoais avulsos ou incompletos e tornou-se numa representação extensíssima do ser existencial.

---

33 http://pt.wikipedia.org/wiki/Rede_social (últ. vez consult. em 22 de Maio de 2014).

34 Estatísticas consultadas em http://siteanalytics.compete.com/facebook.com/ (últ. vez consult. em 22 de Maio de 2014).

# CAPÍTULO II

## A USURPAÇÃO DA CIBERIDENTIDADE

### **4.** Questão prévia: terminologia adotada

Usurpação, furto e roubo de (ciber)identidade são diferentes terminologias reportadas à mesma realidade e como tal pretendem identificar o mesmo problema pelas diferentes ciências que o estudam. Somos da opinião que a terminologia aqui adotada oferece maior rigor jurídico, por três ordens de razão.

*Prius*, e partindo de um argumento histórico, por referência ao artigo 38.º do Lei 12/91, de 21 de Maio (Lei da Identificação Civil e Criminal), já revogada pela Lei 33/99, de 18 de Maio, cuja epígrafe era "*Usurpação de Identidade*" (**35**), e que, como veremos, é uma norma relevante neste trabalho.

*Secundu*, porque a ciberidentidade não deve ser considerada uma *coisa móvel* (**36**), suscetível de deslocação espacial, e a sua apropriação por outrem pode não pressupor uma *subtração,* enquanto elemento objetivo do crime de furto (art. 203.º C.P) e roubo (art. 210.º C.P). A subtração acarreta, num primeiro momento, a "*eliminação do domínio de facto que outrem detinha*" (**37**), sem o seu consentimento, e em segundo lugar "*a criação pelo agente de um novo domínio sobre a*

---

35 Dispunha o mencionado artigo que: "*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*".

36 Como afirma JOSÉ DE FARIA COSTA *in* Comentário Conimbricense do Código Penal, Parte Especial, Tomo II, p. 43: "*informação é uma categoria epistemológica que se diferencia, quer da matéria, quer da energia*".

37 JOSÉ DE FARIA COSTA, *Ibidem*.

*coisa*" ([38]). O que se verifica na usurpação da ciberidentidade é a criação de um novo domínio sobre a identidade virtual de outrem, por parte do agente, sem que isso implique necessariamente a quebra do domínio anterior, e sem que a apropriação ocorra por qualquer meio de constrangimento que esvazie a liberdade da vítima – requisito essencial para a consumação de um crime de roubo.

*Tertius*, como sustenta OLIVEIRA ASCENÇÃO, a usurpação tem sido entendida como "*a apresentação como próprio do que é alheio*" ([39]), o que no nosso entender define com suficiente abrangência e rigor concetual, a conduta desvaliosa objeto do nosso estudo.

## **5.** O problema da usurpação da ciberidentidade

A usurpação da ciberidentidade ocorre **quando alguém utiliza como sua a ciberidentidade de outrem, sem o seu consentimento** ([40]) ([41]).

A Organização para a Cooperação e Desenvolvimento Económico (OCDE) propôs em 2008 uma diferente definição, que enfatiza a intenção criminosa da conduta: "*identity theft occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes*".

A usurpação da ciberidentidade manifesta-se de variadas formas: quando alguém acede (sem autorização) a um *site* com as credenciais

---

[38] CUNHA, JOSÉ DAMIÃO, *Dos Crimes contra o Património*, p. 26.

[39] JOSÉ DE OLIVEIRA ASCENÇÃO, *Direito Penal de Autor*, p. 19.

[40] Temos por certo que a aquiescência de tal utilização afasta a ilicitude da conduta.

[41] Também a definição avançada pelo Centro de Prevenção de Fraude do Reino Unido (CIFAS) vem ao encontro da nossa: "*Identity theft (also known as impersonation fraud) is the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent*".

pessoais de outrem (utilizando o *login* e *password*) – na conta de *e-mail*, na página do banco, na conta do *Facebook* -, e aí age como se fosse o verdadeiro titular, por exemplo, enviando um e-mail, fazendo operações bancárias *online* como transferências, ou colocando um comentário na rede social; ou quando alguém cria um perfil, um domínio, um *site* (etc.) de forma a copiar a identidade de uma pessoa ou entidade já constante na Internet, fazendo-se passar pelo verdadeiro titular dessa identidade.

Este é um problema sério, que vem assumindo contornos mais globalizantes e atinge números preocupantes em todo o mundo (**42**).

Como qualquer outra atividade ilícita praticada *online*, o número de casos de usurpação da ciberidentidade aumenta numa relação direta ao incremento do número de utilizadores da Internet e à evolução tecnológica.

Como afirma R. GELMAN, "*o ciberespaço torna possível a qualquer um recolher informações pessoais sobre outros*" (**43**). De facto, se o *furto de identidade* envolve uma aproximação física entre o agente e a vítima, isso não corresponde à realidade na situação vertente.

Desde logo, a usurpação da identidade *online* pode ser perpetrada sem que a vítima se aperceba atempadamente da situação a que foi sujeita, muitas vezes desconhecendo-se o autor da conduta, o *locus deliti* e a envergadura do dano causado. Nas palavras de JOÉL TIMÓTEO PEREIRA, "*É difícil reconstruir o percurso das informações entre o ponto emissor e o ponto recetor, em virtude de os*

---

42 Essa realidade agudiza-se de dia para dia, tendo a Organização Mundial da Propriedade Intelectual (OMPI) registado em 2012 um aumento de 5% do número de casos de "roubo de ciberidentidade".
Notícia disponível em: http://www.ecofinancas.com/noticias/onu-indica-recorde-casos-roubo-identidade-internet-2012 (últ. vez consult. em 22 de Maio de 2014).

43 *Cfr.* R. GELMAN, *Protecting Yourself Online, The Definitive Resource on Safety, Freedom and Privacy in Cyberspace* (tradução livre nossa).

*atos na Internet serem praticados em diversos pontos, sabendo que os infratores, em regra, dissimulam o efetivo ponto emissor*" (**44**).

Importa reter, que o fenómeno em estudo pode ser sistematizado em três momentos sequenciais:

a) Obtenção de dados pessoais informatizados da vítima;

b) Usurpação da ciberidentidade (*tout court*);

c) Prática de atos juridicamente relevantes durante a utilização da ciberidentidade.

## **6.** Obtenção *ilícita* de dados pessoais informatizados: *modus operandi*

Os dados pessoais informatizados podem ser obtidos de variadas formas ilícitas, assumindo preponderância o *Hacking*, a utilização de *Malware* e o *Phishing* (**45**).

O *hacking* consiste no acesso não autorizado a um sistema informático, explorando as suas vulnerabilidades.

Esta prática nem sempre é mal intencionada. Aliás, é essencialmente em função da motivação ética da conduta que se distinguem os *hackers* dos *crackers*.

O *hacker*, como afirma JOSÉ ALVES DE MATOS, "*apenas utiliza os seus conhecimentos para demonstrar que existem lacunas nos programas e nos sistemas de segurança considerados infalíveis*" (**46**). Por seu turno, o *cracker* é alguém que "*ilegalmente, entra, altera, apaga ou introduz informação distinta, programas ou vírus, em sistemas de*

---

44 JOÉL TIMÓTEO PEREIRA, *op. cit.*, p. 239.

45 De acordo com a OCDE (2011), que incluí entre estes meios de obtenção de dados pessoais também o *spam*. *Apud* RAND Europe, *Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report*, p. 22.

46 JOSÉ ALVES DE MATOS, *Dicionário de Informática e Novas Tecnologias*, p. 173 *apud* PEDRO DIAS VENÂNCIO, *Lei do Cibercrime Anotada e Comentada*, p. 63.

*segurança*" ([47]). Segundo JOSÉ ALVES DE MATOS, a quebra de códigos de segurança pode ser motivada pelo proveito próprio, a intenção de prejudicar alguém ou simplesmente pelo desafio ([48]).

O *hacking* é criminalmente punido enquanto crime de acesso ilegítimo. Este tipo legal de crime está previsto na Lei do Cibercrime, concretamente no seu art. 6.º, que dispõe: "*1- Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias; 2 – Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior*".

Ora, como salienta PEDRO DIAS VENÂNCIO, "*o termo acesso ilegítimo abrange basicamente as infrações relativas às ameaças à segurança (confidencialidade, integridade e disponibilidade) dos sistemas informáticos*" ([49]).

Compreende-se que o acesso ilegítimo a um sistema informático seja um meio idóneo à obtenção de dados pessoais informatizados, informações essas que poderão culminar na usurpação da ciberidentidade, por exemplo, através da utilização de credenciais de acesso (login e password) de um *e-mail*.

Impõe-se, a este ponto, um esclarecimento: partindo da nossa definição de ciberidentidade, nem toda a utilização ilegítima das credenciais de acesso de outrem são, em si, uma usurpação da ciberidentidade. Se através das credenciais de acesso o utilizador não puder ser identificado a partir dos seus dados pessoais reais, então a conduta não é verdadeiramente

[47] JOEL TIMOTÉO PEREIRA, *op. cit.*, p. 474.
[48] *Cfr.* JOSÉ ALVES DE MATOS, ibidem, p. 97 *apud* PEDRO DIAS VENÂNCIO, *ibidem*.
[49] PEDRO DIAS VENÂNCIO, *op.cit.*, p. 59.

uma usurpação da identidade *online*. Exemplificando, se A utilizar a *password* de B para aceder ao *nickname* pela qual B é conhecido no IRC, A não está a usurpar a ciberidentidade de B. Já se A utilizar o *login* e a *password* de B, para aceder a um blog, onde B se identificou com o seu nome, e-mail, fotografia, e fizer uma publicação, aí A já está a apropriar-se dos elementos reais identificativos de B, e logo, a usurpar a ciberidentidade deste.

*Malware* é um termo genérico utilizado para qualificar um programa ou "*software destinado a infiltrar-se ilicitamente num sistema informático, com o intuito de causar danos, alterações ou roubo de informações*" (**50**). Vírus, *spyware*, *worms*, *trojans*, *exploits*, backdoors, *rootkits* são exemplos de programas maliciosos. A utilização de *Malware* também é penalmente punida através dos diferentes Crimes Informáticos, previstos na Lei 109/99, de 15 de Setembro (Lei do Cibercrime) – falsidade informática (art. 3.º), dano relativo a programas ou outros dados informáticos (art. 4.º), sabotagem informática (art. 5.º), acesso ilegítimo (art. 6.º) e interceção ilegítima (art. 7.º) (**51**). Geralmente este tipo de *software* malicioso é um instrumento por excelência de um *cracker*.

Sobre o *Phishing*, PEDRO VERDELHO escreve: "*esta atividade é faticamente complexa e traduz-se na remessa massiva de mensagens de correio eletrónico (utiliza portanto a técnica de spam). Tais mensagens incluem um link para uma página na WWW. Esta página será normalmente a reprodução aproximada de uma outra (esta autêntica), por exemplo de um banco ou de uma entidade emissora de cartões de crédito. Conterá elementos identificadores da entidade autêntica e imagens a ela referentes. Porém, será falsa, por ser construída e gerida por terceiros, sem autorização da entidade cujos sinais pretende imitar. Se a vítima usar o link para aceder à página falsa,*

[50] Definição disponível em http://pt.wikipedia.org/wiki/Malware (últ. vez consult. em 22 de Maio de 2014).

[51] Não consignamos o crime de reprodução ilegítima de programa protegido (art. 8.º da Lei do Cibercrime) por não se relacionar diretamente com a utilização de Malware.

*deparar-se-á com uma página parecida com a do seu banco, ou da entidade gestora do seu cartão de crédito (ou de qualquer outro sítio na Internet que permita a realização de pagamentos online). Será pedido à vítima que se identifique, introduzindo os seus códigos confidenciais, referentes às sua conta bancária ou ao seu cartão, que permitirão aceder às contas bancárias das vítimas, transferindo o dinheiro que aí houver para contas suas. Ou utilizar os respetivos cartões de crédito em seu proveito"* (**52**).

Uma nova modalidade de *phishing*, denominada de *Pharming* consiste numa *"técnica que utiliza os métodos de difusão de vírus que têm formato de verme – os worms. Passa pela difusão, por via de spam – portanto de correio eletrónico. – de ficheiros ocultos, que igualmente de forma oculta se auto-instalam nos computadores ou sistemas informáticos das vítimas. Uma vez alojados, estes ficheiros alteram de forma oculta, sem o conhecimento do dono do computador, os arquivos do sistema, designamente os ficheiros contendo os populares favoritos e o registo de cookies. Por via desta alteração, quando o dono do computador acede ao seu habitual site bancário, o sistema, ardilosamente alterado, redirige-o para um outro site, construído e disponibilizado online com métodos idênticos aos do phishing. Nestes casos torna-se muito difícil reconhecer a fraude, mesmo para utilizadores avançados"* (**53**).

A doutrina salienta o difícil enquadramento do *phishing* num determinado tipo legal de crime, atendendo às múltiplas formas de execução do crime (**54**). Seguimos de perto o trabalho de PAULO GONÇALVES TEIXEIRA (**55**), que indica vários tipos legais de crime associados ao fenómeno.

---

52 PEDRO VERDELHO, *Phishing e outras formas de defraudação nas redes de comunicação*, p. 413.

53 PEDRO VERDELHO, *ibidem*, pp. 415 e 416.

54 Neste sentido, entre outros, JOÃO BARBOSA DE MACEDO, *Algumas considerações acerca dos crimes informáticos em Portugal*, pp. 237 e 238.

55 *Cfr.* PAULO GONÇALVES TEIXEIRA, *op. cit.*, pp. 19 a 58.

Não deixa de ser curioso, e de relevante interesse nesta dissertação, constatar que o *Phishing* pode ser, simultaneamente, um meio de obtenção de dados pessoais e uma conduta em si subsumível à usurpação da ciberidentidade, *maxime* quando o agente envia um *e-mail* com os elementos identificadores de uma entidade para induzir a vítima em erro.

Bem vistas as coisas, o agente que cria um *e-mail* similar ao endereço eletrónico de outrem (pessoa singular ou uma pessoa coletiva), e se identifica como sendo essa pessoa (seja através da indicação do nome, seja utilizando a imagem corporativa de uma empresa), nem sequer necessita de obter ilicitamente dados pessoais relevantes para usurpar a identidade virtual.

Aqui deparamos com o verdadeiramente elementar: **para ser possível usurpar a ciberidentidade, basta que a vítima tenha, em algum momento, colocado na Internet um ou vários elementos da sua identidade.** Tão somente isso.

## **7.** O caso especial da criação de perfis falsos nas redes sociais

De todos os casos específicos que poderíamos abordar na temática da usurpação da ciberidentidade, escolhemos a criação e utilização de perfis falsos nas redes sociais virtuais porquanto se apresenta como o *modus operandi* mais simples e fundamental do fenómeno, e como tal, facilita a perceção do comportamento ilícito, além de suportar cabalmente a conclusão avançada no ponto anterior.

Empregando o exemplo paradigmático do *Facebook* idealizemos a seguinte situação: A, cria uma conta, com o nome Mickael Carreira

(cantor português), e constrói o seu perfil indicando os dados pessoais (data de nascimento, fotografia, cidade de residência, por exemplo) e profissionais (músico/cantor). Todos esses dados estão disponíveis na Internet, portanto a sua obtenção não proveio de nenhum meio ilícito (**56**). O perfil vai sendo melhorado de forma a torná-lo mais realista, e A convence jovens a despirem-se perante uma *webcam*.

Esta hipótese é verídica!

Em Abril de 2013 foi publicada uma notícia (**57**) segundo a qual "*Um homem de 64 anos usou durante mais de dois anos o nome de Mickael Carreira para convencer jovens a despirem-se em frente a uma webcam*". No corpo da notícia lê-se: "*As jovens eram contactadas através dos perfis nas redes sociais (MSN e Facebook) e assediadas a mostrar o corpo e fazer poses eróticas perante a câmara. Quando começavam a desconfiar da identidade do agressor as vítimas eram intimidadas pelo agressor, que ameaçava divulgar as imagens já registadas*".

Nisto se traduz a criação e utilização de perfis falsos nas redes sociais.

Naturalmente que a designação "perfil falso" reporta-se à incongruência entre os dados virtuais e os dados reais do utilizador. Como já se explanou no Capítulo I, a utilização de um perfil falso só é uma conduta subsumível à usurpação se o perfil usado corresponder à ciberidentidade de outra pessoa. Foi esse o caso.

De certa forma, poder-se-á dizer que as figuras públicas são um alvo privilegiado deste tipo de comportamento. O que não significa que as pessoas com maior notoriedade sejam as únicas vítimas (**58**).

---

56 Aliás, embora sejam dados pessoais, dificilmente poderão ser considerados dados pessoais privados, quando foi o próprio a torna-los públicos na Internet. Como tal, não estarão à partida protegidos pelo art. 35.º da CRP nem pelo crime de devassa da vida privada (art. 193.º do CP).

57 http://tek.sapo.pt/noticias/internet/mickael_carreira_usado_para_fazer_despir_mulh_1311880.html (últ. vez consult. em 22 de Maio de 2014).

58 Identificamos no caso múltiplas vítimas: as jovens e o próprio cantor Mickael Carreira.

Parafraseando JOANA VERÍSSIMO, MARIA MACIAS e SOFIA RODRIGUES ([59]), *"Todos estamos vulneráveis a este tipo de situações, 24 sobre 24 horas, 7 dias por semana. E vários são os casos em que são criados perfis falsos em nome de alguém com o objetivo de ofender a sua honra e o seu bom nome"*.

A "proteção não jurídica" dada à criação e utilização de perfis falsos é uma tarefa da administração das plataformas. Cada utilizador é livre de denunciar um perfil falso ou mesmo conteúdos difundidos na rede social. Perante uma denúncia legítima, cabe aos responsáveis do serviço retirar o conteúdo ou eliminar o perfil falso. A autorregulação das redes sociais constitui um autêntico dever jurídico, como confirma uma decisão judicial de um tribunal brasileiro do Rio de Janeiro, em 2011, que condenou a Google no pagamento de uma indemnização de €5.400 a um jovem vítima de difamação na rede social Orkut ([60]). Apesar de importante, a proteção dada pelos responsáveis dos *sites*, que funcionam como verdadeiros fiscalizadores, só é virtualmente capaz de impedir a continuação da atividade ilícita.

## **8.** Finalidades abusivas da usurpação da ciberidentidade

São inúmeras as finalidades abusivas da usurpação da ciberidentidade, que podem, em todo o caso, ser agrupadas em três motivações genéricas: a obtenção indevida de vantagem patrimonial, o encobrimento da prática de outros crimes, e a provocação de danos relevantes nas vítimas.

---

[59] JOANA VERÍSSIMO, MARIA MACIAS e SOFIA RODRIGUES, *Implicações jurídicas das redes sociais na Internet: um novo conceito de privacidade?*, p. 4.

[60] http://tek.sapo.pt/noticias/negocios/google_obrigada_a_indemnizar_jovem_difamado_n_1169562.html (últ. vez consult. em 22 de Maio de 2014).

A obtenção indevida de ganhos económicos é abundantemente referenciada como o principal desígnio deste ato ilícito. Assume especial relevância neste campo ([61]), a burla informática concretizada através do serviço de *homebanking* ([62]), muitas vezes com recurso ao *phishing* e *pharming* ([63]) ([64]).

O nosso ordenamento jurídico-penal prevê e pune o crime de Burla informática e nas comunicações (art. 221.º CP) ([65]).

A utilização de uma identidade virtual alheia sem o consentimento do titular como forma de encobrimento de outros crimes é uma realidade que dispensa grandes considerações. Os crimes praticados sob uma ciberidentidade alheia podem ser todos quantos a imaginação criminógena permite conceber, revestindo singular importância e preocupação a pedofilia e o tráfico de menores.

Por fim, a usurpação da ciberidentidade é um meio idóneo à prática de crimes contra a honra – difamação (art. 180.º CP), contra a privacidade – devassa da vida privada (art. 193.º CP) e gravações e

---

61 De acordo com os dados avançados pelo Diário Económico, o valor das fraudes *online* chegou aos 1,8 milhões de euros nos primeiros meses de 2009, valor que representa uma subida de 20% relativamente a idêntico período de 2008. Notícia disponível em http://tek.sapo.pt/noticias/internet/burlas_na_internet_crescem_20_1010055.html (últ. vez consult. em 22 de Maio de 2014).

62 O *homebanking* consiste num contrato em que o banco disponibiliza ao cliente um serviço através do qual lhe confere a possibilidade de efetuar um conjunto de atividades no âmbito da atividade bancária, através da Internet ou do telefone.

63 Sobre a responsabilidade contratual do próprio banco - *cfr.* Acórdão do Supremo Tribunal de Justiça, de 18/12/2013, processo n.º 6479/09.8TBBRG.G1.S1. Disponível em www.dgsi.pt.

64 Com interesse, uma recente notícia de um desvio de 243 mil euros de 111 contas bancárias, disponível em http://expresso.sapo.pt/76-acusados-por-phishing-acederam-a-111-contas=f858214 (últ. vez consult. em 22 de Maio de 2014).

65 Estabelece o art. 221.º, n.º 1 do CP, que: "*Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa*".

fotografias ilícitas (art. 199.º CP), ou contra a liberdade pessoal – ameaça (art. 153.º CP) e coação (art. 154.º CP).

Aqui chegados, importa reconhecer que a usurpação da ciberidentidade não é um fenómeno desconhecido do legislador nem lacunoso no que concerne à tutela jurídico-penal. O Direito Penal intervém nesta problemática como vimos *supra*, seja através da tutela dos sistemas informáticos e dos dados informáticos (Lei do Cibercrime) seja pela proteção conferida ao fim criminoso visado com a usurpação propriamente dita (difamação, obtenção ilegítima de vantagem patrimonial, prejuízo patrimonial para a vítima, *etc*).

Na literatura jurídica portuguesa, a usurpação da identidade *online* tem sido tratada como um fenómeno ligado a outros problemas, como o *phishing* e a privacidade nas redes sociais virtuais. Em todo o caso, até ao momento só logramos obter uma simples constatação: **a usurpação da ciberidentidade *tout court* (o simples ato de utilizar a identidade virtual de outrem sem o seu consentimento) não é autonomamente punível pelo sistema jurídico-penal**.

Assim afirma PAULO TEIXEIRA, "*em nosso entender é clara a lacuna legislativa neste campo, dado que a lei portuguesa não prevê e consequentemente não sanciona a situação de quem cria e usa um endereço de correio-electrónico que pretende parecer o de outrem*" (**66**). Também JOANA VERÍSSIMO, MARIA MACIAS E SOFIA RODRIGUES escrevem: "*criar um perfil falso de alguém que não existe, só para preservar a sua identidade durante os relacionamentos na internet, sem que esta prática tenha causado qualquer dano, não é crime. Todavia pode levar o criador a ter de remover o seu perfil, ou por infração dos Termos de Uso estipulados pelo website, ou caso exista alguma denúncia e, aí, poderá ter de suportar uma indemnização, no caso de existirem meios de prova que comprovem a violação for criado através de uma pessoa real, o facto de utilizar a imagem e a personalidade de*

[66] PAULO GONÇALVES TEIXEIRA, *op. cit.*, p. 27.

*outra pessoa, escrever declarações falsas com fim de a prejudicar, ou alterar a verdade sobre determinado facto juridicamente relevante, pode levar o responsável a incorrer no crime de roubo de identidade online - um crime ainda não tipificado em Portugal"* (**67**).

[67] JOANA VERÍSSIMO, MARIA MACIAS e SOFIA RODRIGUES, *op. cit.*, p. 15.

# CAPÍTULO III

## A (NÃO) CRIMINALIZAÇÃO DO FENÓMENO

Aqui chegados, fica patente a facilidade da prática da usurpação da ciberidentidade em contraponto com a potencialidade das suas consequências. Por outras palavras, torna-se demasiado fácil prejudicar alguém com este ato ilícito que viola um bem jurídico constitucionalmente protegido.

A constatação desta fragilidade do Direito na resposta ao problema está no âmago da questão crucial neste estudo: Deverá ou não ser a usurpação da ciberidentidade objeto de criminalização, independentemente da finalidade do comportamento?

De *iure condendo*, já sabemos, a por nós chamada usurpação da ciberidentidade *tout court* não é um ilícito criminal autónomo.

Consideramos, porém, pertinente colocar em crise esta solução normativa, a partir de uma análise dialética de argumentos favoráveis e desfavoráveis à criminalização do comportamento, que potencie na literatura jurídica uma discussão mais profunda do problema.

### **9.** Argumentos desfavoráveis

O primeiro argumento desfavorável à autonomização do crime de usurpação da ciberidentidade invoca considerações de ordem sistemática. Na Lei 12/91, de 21 de Maio (Lei da Identificação Civil e Criminal) previa-se e punia-se o crime de usurpação da identidade. O art. 38.º do diploma dispunha que: "*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"*. Este tipo legal de crime viria a desaparecer do ordenamento jurídico português, com a revogação daquele diploma, que foi substituído pela Lei 33/99, de 18 de Maio (Regula a identificação civil e a emissão do bilhete de identidade de cidadão nacional).

Da opção legislativa de não transpor para a Lei 33/99 o crime de usurpação de identidade parece resultar a ideia de que a utilização de uma identidade alheia assume relevância penal em cinco diferentes situações: quando se comete o crime de uso de documento de identificação alheio (art. 261.º CP), quando se comete o crime de falsificação de documentos (art. 256.º CP) ([68]), ao cometer o crime de falsificação de estado civil (art. 248.º CP), no cometimento do recente ([69]) crime de falsas declarações (art. 348.º-A CP) ou quando através da usurpação se causa um prejuízo económico a outrem (e. g. o crime de burla – art. 217.º e ss. CP).

Nos quatro primeiros casos, a relevância penal pode resultar diretamente da utilização de uma identidade alheia, embora não seja a identidade (virtual) o concreto bem jurídico protegido. No último caso, essa utilização só é penalmente relevante enquanto "*meio de erro ou engano*" (elemento objetivo do tipo de ilícito da burla).

Na esmagadora maioria dos casos dignos da intervenção penal, a usurpação da identidade é, pois, tutelada pelo elenco dos crimes previstos no Código Penal.

Pois bem, autonomizar um tipo legal de crime que tutele a usurpação da ciberidentidade, quando inexiste no direito um tipo legal que puna a usurpação da identidade, tornar-se-ia sistematicamente incoerente.

---

[68] Referência específica ao preenchimento típico da alínea e), n.º 1 do art. 256.º CP – "*Usar documento a que se referem as alíneas anteriores*".

[69] O art. 348.º-A CP foi aditado pela Lei n.º 19/2013, de 21 de Fevereiro, e entrou em vigor em 24-03-2013.

Um dos principais argumentos desfavoráveis à autonomização do crime de usurpação da ciberidentidade invoca os princípios da subsidiariedade e fragmentariedade jurídico-penais.

Não colocando em crise o "direito penal do bem jurídico", podemos afirmar que a dignidade jurídico-penal de um bem jurídico deriva da sua "*concretização enquanto valor constitucional expressa ou implicitamente ligado aos direitos e deveres fundamentais e à ordenação social, política e económica*" (**70**). No entanto, a intervenção penal não pode ser aferida tão-só pela existência de um bem jurídico-penal, exigindo-se um outro critério para que a criminalização seja legítima: o da necessidade ou carência de tutela penal (**71**). Este princípio diz-nos que "*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*" (**72**). Daqui deriva a natureza subsidiária – de *ultima ratio* – do Direito Penal, desde logo, em respeito do princípio constitucional da proporcionalidade em amplo sentido (art. 18.º, n.º 2 CRP).

A tutela subsidiária de bens jurídico-penais pressupõe, ainda, que um fenómeno social complexo e desvalioso, não seja ele todo criminalizado, mas só os comportamentos limite em que o bem jurídico já não seja suficientemente protegido pela intervenção dos meios civis e administrativos - princípio da fragmentariedade da intervenção jurídico-penal.

Ora, partindo da divisão em três momentos do fenómeno vertente (*Capítulo II, ponto 5*), temos por certo que o nosso sistema jurídico-penal dá resposta às situações de obtenção ilícita de dados pessoais informatizados, através da previsão e punição dos Crimes Informáticos constantes na Lei 109/99, de 15 de Setembro (Lei do Cibercrime) –

---

70 JORGE DE FIGUEIREDO DIAS, *Direito Penal*, Parte Geral, Tomo I, p. 120.
71 *Ibidem*, p. 127.
72 *Ibidem*, p. 128.

falsidade informática (art. 3.º), dano relativo a programas ou outros dados informáticos (art. 4.º), sabotagem informática (art. 5.º), acesso ilegítimo (art. 6.º) e interceção ilegítima (art. 7.º).

Em segundo lugar, o *ius puniendi* oferece já uma ampla tutela das consequências desvaliosas da apropriação da identidade virtual alheia. Pense-se na difamação (art. 180.º CP), na devassa da vida privada (art. 193.º CP), na burla informática (art. 221.º, n.º 1 CP), na coação (art. 154.º CP), entre outros.

Perante o exposto, aparenta ser obliterável uma alteração do sistema jurídico-penal, justamente pela desnecessidade de punição da simples utilização da ciberidentidade de outrem, sem o seu consentimento.

## **10.** Argumentos favoráveis

O primeiro argumento favorável à tipificação do crime de usurpação da ciberidentidade é o próprio fenómeno de *patologia social* presente neste comportamento, que exige a definição de uma estratégia de controlo social da realidade humana.

Cabe à política criminal "*definir, quer no plano do direito constituído, quer do direito constituindo, os limites da punibilidade*" (**73**), de forma a atingir a finalidade de combate aos problemas de relação comunitária *através* do direito penal. Isto é, *a aplicação do direito penal fica dependente da teleologia, das valorações e das proposições político-criminais imanentes do sistema jurídico-constitucional* (**74**).

---

73 JORGE DE FIGUEIREDO DIAS, *op. cit.*, p. 41.

74 Neste sentido, JORGE DE FIGUEIREDO DIAS, *ibidem*, pp. 35 a 38.

Se não considerarmos nem os meios pelos quais a usurpação ocorre nem os danos provocados com a utilização de uma identidade virtual alheia, ainda assim este fenómeno atinge a identidade pessoal no seu núcleo essencial, que mais do que um direito constitucionalmente consagrado, e logo, bem jurídico fundamental para o indivíduo e para a sociedade, é um valor básico muito anterior à ideia de Estado e transcendente à própria conceção social do Homem: é o último reduto da sua individualidade e da sua dignidade.

Inquirindo-se o sistema jurídico-constitucional em que assenta o discurso legitimador da criminalização, dever-se-á concluir que o direito constituído não privilegia os direitos de personalidade na Internet como limites intransponíveis da liberdade na cibersociedade, antes abraça uma atitude de passividade perante a construção de um sistema nefasto à projeção autêntica de cada ser humano na Internet.

A partir daqui dever-se-á defender o alargamento da sempre subsidiária tutela do Direito Penal, criminalizando-se a usurpação da ciberidentidade enquanto tal, de forma a ultrapassar a insuficiente intervenção penal neste fenómeno, essencialmente destinada a proteger os sistemas informáticos, o acesso a dados informáticos e o escopo económico, - e não a identidade virtual dos cidadãos.

Tal solução seria encarada como uma medida tanto profilática como consciencializadora, capaz de cumprir a função do direito penal e principalmente adaptar a sensibilidade axiológica da sociedade à plena consagração da Sociedade de Informação.

Naturalmente que mais do que um argumento, esta consideração de política criminal consubstancia uma verdadeira tomada de posição quanto à questão central deste estudo e simultaneamente se apresenta como o primeiro passo metodológico para a procura de uma solução justa e adequada para este problema, que é já trabalho da dogmática jurídico-penal.

A intervenção dos meios civis na tutela da ciberidentidade não se apresenta uma solução suficiente para acautelar o fenómeno da

usurpação. A natureza do processo civil não permite a obtenção de meios de prova eficazes quanto à identificação do verdadeiro autor do comportamento, porquanto não está na disponibilidade de um cidadão comum obter e apresentar a juízo provas irredutíveis da sua pretensão. O princípio da investigação e a preciosa intervenção do Ministério Público no processo penal, reforçam o papel do Direito Penal na tutela dos atos ilícitos praticados na Internet. Isto porque, não raras vezes, a única forma de presumir o autor da conduta é a partir do *IP* do computador que foi utilizado. Ora, só os fornecedores de serviços de internet têm cabal acesso a esses dados, e somente os disponibilizam por ordem judicial.

JOÃO FACHANA, relativamente à responsabilidade civil pelos conteúdos ilícitos colocados e difundidos na Internet, chega à seguinte conclusão: "*Por não ser possível associar o IP a um determinado sujeito em particular, mas apenas ao computador do qual provém o acto ilícito, bem como, pelos mecanismos que existem para ocultar o verdadeiro IP, teremos forçosamente de concluir pela impraticabilidade da responsabilidade civil dos autores do acto ilícito, por via de regra*" (**75**).

O sistema jurídico-penal brasileiro pune a adoção de uma falsa identidade. Estabelece o art. 307.º do Código Penal Brasileiro que "*a atribuição própria ou a terceiro de falsa identidade com o intuito de obter um benefício próprio ou alheio, ou de causar um dano a outrem, é punível com detenção de três meses a um ano, ou multa, se o facto não constituir elemento de crime mais grave*".

Nas palavras de LUÍZ REGIS PRADO, "*no art. 307.º o Código prevê uma forma de falsidade não mais documental, nem mesmo material ou ideológica mas pessoal: ilude alguém a respeito da própria identidade*

[75] JOÃO FACHANA, p. 69.

*ou da identidade de terceiro, para obter vantagem ou causar-lhe dano*" (**76**).

Tem sido entendimento maioritariamente acolhido pela doutrina brasileira que o tipo legal da falsa identidade descreve a conduta de modo genérico alcançando as mais variadas características da pessoa (nome, idade, estado civil, profissão, sexo, filiação, condição social, etc) (**77**).

LUÍZ PRADO explica que "*a falsa atribuição pode ser tanto verbal quanto por escrito, devendo, entretanto, ter idoneidade para ludibriar (…), bem como potencialidade para causar dano*" (**78**).

Não se nos afiguram razões para rejeitar a aplicação deste tipo legal de crime à usurpação da ciberidentidade no Brasil, como se não afigurariam razões para afastar a aplicabilidade, em Portugal, do art. 38.º da Lei 12/91, de 21 de Maio (usurpação da identidade) a esse fenómeno, não fosse o facto de ter sido revogado.

Não obstante, convém não esquecer que quer o art. 307.º do CP Brasileiro, quer o revogado art. 38.º da Lei 12/91, enfatizam a manobra fraudulenta – a falsidade enquanto meio de engano -, e como tal, pretendem proteger a segurança nas relações jurídicas e não o direito à identidade pessoal.

Esta nossa conclusão é derradeiramente sustentada pela posição de JÚLIO FABBRINI MIRABETE que afirma (relativamente ao art. 307.º do CP Brasileiro): "*a primeira conduta é atribuir-se ou atribuir a outrem a falsa identidade, ou seja, fazer-se passar ou a terceiro por outra pessoa existente ou imaginária*" (**79**). Ou seja, importa no crime de falsa identidade o engano perpetrado pela utilização da identidade real ou fabricada. Esta subsunção da possibilidade de criação de uma

---

76 LUÍZ REGIS PRADO, Curso de Direito Penal brasileiro – Volume 4 (Parte Especial), 2º Edição – Editora Revista dos Tribunais – pág. 278.

77 Neste sentido, cfr. NÉLSON HUNGRIA, Comentários ao Código Penal, p. 306; e MAGALHÃES NORONHA, Direito Penal, p. 196.

78 LUÍZ REGIS PRADO, *Curso de Direito Penal Brasileiro*, p. 280.

79 JÚLIO FABBRINI MIRABETE, *Código Penal interpretado*, p. 1664.

identidade que não é a de ninguém ao crime de falsa identidade, excluí da sua *ratio legis* a proteção da identidade de outrem apesar de poder garantir essa tutela indiretamente. Invariavelmente, está também excluída do seu fundamento a proteção da ciberidentidade como a definimos.

Ainda no domínio do Direito Comparado, é curioso constatar que, nos Estados Unidos da América, o "furto de identidade" é objeto de tutela jurídico-penal em todos os Estados (**80**). Mas também aí o crime de *identity theft* revela essencialmente preocupações de ordem económico-financeira. Por exemplo, no Estado de Connecticut a usurpação da identidade é perpetrada quando o agente usa conscientemente informações pessoais de outrem para obter dinheiro, crédito, bens, serviços, propriedade ou serviços médicos sem consentimento (**81**).

Do exposto parece resultar a necessidade de tutelar a identidade virtual, através de uma alteração do sistema penal, *maxime* com a criminalização da usurpação da ciberidentidade *tout court*.

Independentemente da nossa opinião, que ainda não revelámos, cabe agora avançar com uma proposta concreta de construção dogmática do tipo legal de crime de usurpação da ciberidentidade. Por vezes o modo de concretização de uma ideia permite esbater o extremar de posições, além de permitir ultrapassar uma questão que terá de ser, *ad arbitrium*, respondida pelo político-legislador (criminalizar ou não) e abraçar uma outra, que implica uma concretização do jurista-legislador (como criminalizar).

---

80 http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx (últ. vez consult. em 22 de Maio de 2014).

81 *Cfr.* http://www.jud.ct.gov/JI/criminal/part10/10.3-1.htm (últ. vez consult. em 22 de Maio de 2014). Na página pode ler-se: "*a person commits identity theft when (he/she) knowingly uses personally identifying information of another person to obtain [or attempt to obtain] (money / credit / goods / services / property / medical information1) without the consent of such other person*".

# CAPÍTULO IV

## UMA PROPOSTA DOGMÁTICA DO TIPO LEGAL DE CRIME

### **11.** Bem jurídico

De *iure constituendo*, a autonomização do crime de usurpação da ciberidentidade deverá fundamentar-se na proteção da ciberidentidade, enquanto bem jurídico pessoal. Do nosso ponto de vista, a razão essencial para a consagração deste crime autónomo deverá ser inequivocamente a violação do direito à identidade pessoal na Internet. Aplaudimos a previsão de um crime de falsa identidade no ordenamento jurídico brasileiro mas não abraçamos a sua construção dogmática, na medida em que pretende evitar a violação da segurança no tráfico jurídico em virtude da utilização de uma falsa identidade. Fosse esse o escopo da criminalização, e os argumentos contrários à mesma seriam dificilmente superados.

### **12.** O tipo objetivo de ilícito

A factualidade típica do ilícito deverá traduzir-se na **utilização da ciberidentidade de outrem, sem o seu consentimento**.

A estrutura da conduta típica não necessita, neste momento, de grandes considerações, porquanto que ao longo deste trabalho já fomos adensando o alcance hermenêutico dos seus elementos nucleares, mas não nos escusamos a tecer os seguintes esclarecimentos:

a) A utilização da ciberidentidade não é a conduta através da qual se obtêm dados pessoais da vítima, mas sim o ato material de usar como seus os elementos caracterizadores de outra pessoa enquanto indivíduo singular e irredutível (nome, filiação, data de nascimento, fotografia, residência, sexo, e-mail) que o identificam como tal na Internet.
b) O facto de ser empiricamente impossível privar totalmente alguém da sua ciberidentidade, permite que o consentimento da vítima afaste o tipo incriminador, não obstante a natureza irrenunciável dos direitos de personalidade, e logo, do direito à identidade pessoal na Internet.

A conduta pode ser cometida por qualquer pessoa (crime comum) e traduz-se num ato positivo – uma **ação** – por parte do agente. É importante que o preenchimento da factualidade típica configure um **dano** causado no direito de cada um a não sofrer intromissões abusivas na projeção de si próprio (a identidade) na Internet – **crime de dano** -, em que ocorra uma **lesão efetiva** da ciberidentidade a ponto da vítima **perder o controlo absoluto dos atos que são praticados com a sua identidade virtual**.

Não deverá ser necessário nenhum *plus* típico específico quanto aos atos praticados com a ciberidentidade de outrem (ao contrário do que se verifica no exemplo demonstrado no Estado do Connecticut). Todavia, dever-se-á configurar indispensável **a suscetibilidade de perturbação relevante nas relações jurídicas e/ou sociais**. Isto é, muito embora não deva ser necessário a verificação de uma consequência adicional, a conduta terá de imprimir uma danosidade social traduzida na suscetibilidade de transgressão da barreira da confiança jurídica. Desta forma, operar-se-ia uma redução da área de tutela típica, naturalmente reforçando a fragmentaridade da intervenção penal, excluindo-se aquelas situações que jamais deverão consubstanciar uma prática criminosa, e simultaneamente precavendo a *diabolica probatio*

de qualquer *plus* típico, justamente num fenómeno em que pode ser difícil ou impossível demonstrar judicialmente o que o agente fez durante a usurpação (perda de controlo absoluto).

Ilustremos o que acabou de ser sustentado: A aproveita que o e-mail de B está aberto, e sem que este saiba, envia uma mensagem eletrónica a C (seu irmão) a dizer, "hoje não janto em casa", e assina em nome de B. Aqui, há inequivocamente uma situação de usurpação da ciberidentidade, que não assume relevância penal típica porque não se configura a suscetibilidade de perturbação relevante nas relações jurídicas e/ou sociais.

Se A tem de alguma forma acesso à utilização do *e-mail* de B durante algum tempo (uma semana, por exemplo), e B não tem forma de saber que mensagens eletrónicas foram enviadas, ou sequer se foi alguma enviada, ocorre uma usurpação da ciberidentidade, que assume relevância penal típica, uma vez que o decurso do tempo durante o qual a vítima perdeu o controlo absoluto da sua identidade virtual é susceptivel de perturbação relevante nas relações jurídicas e/ou sociais.

Outra *fattispecie*: Se C aproveita que D está conectado no *Twitter*, e faz uma publicação em seu nome dizendo: "eu sou racista e odeio ciganos", está a usurpar a identidade online de D e a praticar um ato suscetível de responsabilidade penal (difamação), e portanto, mais que a suscetibilidade, fica patente a efetiva perturbação relevante nas relações jurídicas e sociais, e C deveria ser responsabilizado penalmente pela usurpação da ciberidentidade. Por fim, se Z cria um perfil no Facebook de forma a copiar o perfil de Y, está a usurpar a identidade virtual de forma a ser susceptivel a perturbação nas relações sociais, já que passam a existir dois Y aos olhos de incontáveis utilizadores, e então, Z seria responsabilizado penalmente.

## **13.** O tipo subjetivo de ilícito

Naturalmente que o crime em estudo exigiria **dolo** relativamente à ação, em qualquer das suas formas.

Rejeitamos, porém, a exigência de uma dupla componente subjetiva que implique a comprovação da intenção de realizar finalidades criminosas ou pelo menos ilícitas. A *praxis* judicial mostra-nos a dificuldade da condenação do agente que pratica condutas subsumíveis a tipos legais de crime que exigem um elemento subjetivo especial, ao mesmo tempo que não seria coerente desconsiderar a previsão de um *plus* na conduta típica para a consumação do crime mas exigir a demonstração de uma qualquer intenção nesse sentido, quando o crime é perpetrado "atrás de uma máquina". Perante a difícil demonstração da dupla componente subjetiva, principalmente em matéria de criminalidade informática, não se nos afigura justificada essa exigência.

## **14.** Concurso

Defendemos, por fim, que a incriminação da usurpação da ciberidentidade *tout court*, a existir, não deverá consignar uma relação de subsidiariedade expressa, como no art. 307.º do CP Brasileiro – "*se pena mais grave lhe não couber por força de outra disposição legal*" -, antes se devendo estabelecer também uma agravação nos limites da pena, dessa maneira se precavendo a possibilidade das consequências da usurpação serem mais gravosas que a violação do direito à identidade virtual, e ao mesmo tempo, considerando que os crimes praticados com a identidade virtual de outrem transpiram um maior desvalor da ação e do resultado: "*se pena mais grave lhe não couber por força de outra disposição legal, caso em que esta será elevada de*

*um [terço, quinto, quarto] nos seus limites mínimo e máximo [ou no seu limite máxima, ou no seu limite mínimo]"* (**82**).

[82] Seguimos a posição de AMÉRICO TAIPA DE CARVALHO *in Comentário Conimbricense do Código Penal*, Tomo I, p. 529, que criticando a solução legal da subsidiariedade expressa do crime de violência doméstica (art. 152.º CP), apresenta esta proposta, que quanto a nós, faz todo o sentido.

# CONCLUSÃO

Ao longo deste trabalho procuramos evidenciar a dinâmica inerente ao problema da usurpação da identidade virtual chamando à colação a ciência conjunta do Direito Penal, quanto à fenomenologia criminógena e as prementes reflexões de política criminal, culminando com uma possível solução dogmática para a criminalização autónoma do problema.

Foram formuladas opiniões e desenvolvidos pontos de vista sobre um tema praticamente "virgem" na literatura jurídica portuguesa, circunstância que, esperamos, cumprirá o principal objetivo proposto: despertar a atenção para a problemática e potenciar um trabalho doutrinal por parte de quem dedica a sua vida à investigação científico-jurídica. Certamente que todas as conclusões por nós formuladas são criticáveis, e se críticas houver, então, modestamente, sentiremos que a missão foi cumprida, e a dialética está a satisfazer a sua função científica.

Por isso mesmo, não nos escusamos à formulação da nossa visão quanto à autonomização do crime, apesar de chegados aqui, ainda não nos termos comprometido com uma posição. Foi nosso intento apresentar considerações objetivas e, na medida do possível, isentas até à conclusão do trabalho.

Pessoalmente, julgamos que quando o clímax coincide com o desfecho, o interesse empubesce. É esse o efeito pretendido.

Entendemos que a usurpação da ciberidentidade justifica alterações no sistema jurídico-penal. Apreciamos que o legislador não instrumentalize o Direito Penal a seu bem prazer, e propugnamos que este meio de controlo social, o seja enquanto solução de *ultima ratio*, para que não se perca na tradição jurídica portuguesa um notável trabalho de legitimação e fundamentação de um ramo do Direito que

pressupõe a aplicação das mais gravosas consequências jurídicas. Ao mesmo tempo, concebemos a Internet como um espaço de liberdade, o que só num mundo ideal dispensa a hétero regulação, e portanto, a intervenção jurídica. Somos sensíveis à insuficiência da intervenção dos meios civilísticos para responder cabalmente aos fenómenos cibernáuticos que violam bem jurídicos eminentemente pessoais, por uma razão muito simples: os danos sofridos por alguém no ambiente virtual, são, no ciberespaço, praticamente incontroláveis e insuscetíveis de restituição natural ou avaliação patrimonial (por serem geralmente incalculáveis), além de transbordarem para a vida real da vítima.

O que particularmente nos surpreendeu quando efetuamos a pesquisa para esta dissertação foi a total desconsideração da identidade virtual como um bem jurídico pessoal que merece ser tutelado. O que realmente transparece é que nos países onde o "furto de identidade" *online* é alvo de maior discussão, como na cultura jurídica anglo-saxónica, a preocupação gira em torno do prejuízo patrimonial decorrente dos atos praticados por alguém utiliza a identidade virtual que não é sua. Bem sabemos que também no quadro do nosso sistema penal, é mais severamente punido quem furtar um bem de um cofre fechado (**83**) do que quem agredir a integridade física de outrem (**84**), mas somos da opinião que o legislador português é especialmente atento às patologias sociais eminentemente ligadas à pessoa enquanto tal.

Acreditamos que a proposta conjunta apresentada no Capítulo IV pode ser uma solução equilibrada (**85**), porque não enquadra o problema vertente como um comportamento bagatelar, e ao mesmo tempo permite a aplicação objetiva de um crivo hermenêutico, que excluí da área de tutela, as situações limite.

---

83 art. 204.º, n.º 1, alínea e) do CP.

84 art. 143.º do CP.

85 Seguimos de perto a máxima de Aristóteles, segundo o qual, a moderação é a maior das virtudes.

Quanto à inexistência de um crime de usurpação da identidade, e da consequente incoerência sistemática que daí pode advir, cabem as considerações sobre a fragmentariedade jurídico-penal. Convenhamos, a usurpação da identidade não é um problema novo, e na realidade, prever a sua criminalização só iria dar premente resposta à questão vertida neste trabalho: a defesa da ciberidentidade. Ora, ao admitir a criminalização da usurpação da identidade, onde se consignasse também uma solução ao problema da usurpação da ciberidentidade, estar-se-ia a *tomar o todo pela parte*, aí sim, atingindo os princípios essenciais da intervenção jurídico-penal.

Tanto quanto julgamos, a nossa solução apresenta-se simultaneamente profilática e consciencializadora, e principalmente, coerente face às premissas dogmáticas que são substrato do nosso sistema penal. A proposta exposta é, todavia, um produto inacabado, que resulta de um modesto impulso doutrinal – o nosso. O estado embrionário da discussão em torno deste tema, não nos permitiu avançar mais na construção do tipo legal de crime, nomeadamente quanto à pena a aplicar. Foi sempre nossa intenção trazer à colação propostas que permitam acolher os argumentos favoráveis à autonomização do crime de usurpação da ciberidentidade, ultrapassando da melhor forma, as críticas que se lhe podem apontar.

Tudo considerado, esperamos ter oferecido um contributo oportuno para a análise crítica do tema vertido.

*Flávio M. Carneiro da Silva*

Maio de 2014

# BIBLIOGRAFIA


*Monografias*

ASCENÇÃO, JOSÉ DE OLIVEIRA, *Direito Penal de Autor*, Lex Edições, 1993.

CANOTILHO, J. J. GOMES E MOREIRA, VITAL, *Constituição da República Portuguesa Anotada*, Vol. I, 4.ª edição, Coimbra Editora, 2007.

CARVALHO, AMÉRICO TAIPA, *in Comentário Conimbricense ao Código Penal*, Parte Especial, Tomo I, 2.ª Edição, Coimbra Editora, 2012.

COSTA, JOSÉ DE FARIA, *in Comentário Conimbricense do Código Penal*, Parte Especial, Tomo II, Coimbra Editora, 1999.

CUNHA, JOSÉ DAMIÃO DA, *Dos Crimes contra o Património*, Direito Penal Patrimonial – Texto de Apoio ao Mestrado em Ciências Jurídico-Criminais, 2012/2013.

DIAS, JORGE DE FIGUEIREDO, *Direito Penal*, Parte Geral, Tomo I, 2.ª Edição, Coimbra Editora, 2007.

DIAS, JORGE DE FIGUEIREDO, *Comentário Conimbricense do Código Penal*, Parte Especial, Tomo I, 2.ª Edição, Coimbra Editora, 2012.

DIAS, JORGE DE FIGUEIREDO, *Comentário Conimbricense do Código Penal*, Parte Especial, Tomo II, Coimbra Editora, 1999.

FACHANA, JOÃO, *A responsabilidade civil pelos conteúdos ilícitos colocados e difundidos na Internet*, Dissertação de Mestrado, UCP, 2011. Disponível em http://goo.gl/z0rdoj (últ. vez consult. em 22 de Maio de 2014).

GARCIA, ISABEL REIS, *Do direito da informática a um anteprojecto de lei de protecção de dados pessoais*, ROA, ano 49 (1989), vol. III.

GELMAN, R., *Protecting Yourself Online, The Definitive Resource on Safety, Freedom and Privacy in Cyberspace,* Harper Edge, 1998.

GROVER, MARK FRANCIS, *A theory of unified online identity*, 2009. Disponível em http://goo.gl/j9LvZp (últ. vez consult. em 22 de Maio de 2014).

HUNGRIA, NÉLSON, Comentários ao Código Penal, Vol. 9, ed., Edições Forense, 1959.

MARTINS, ALBERTO, *Proteção de dados pessoais informatizados na Constituição da República Portuguesa*, Documentação e Direito Comparado, n.º 47 e 48, Julho-Dezembro, 1991

MARTINS, JOSÉ LEGATHEAUX, *Evolução Tecnológica da Internet em Portugal*, Ingenium – Revista da Ordem dos Engenheiros, 2.ª Série, n.º 17.

MIRABETE, JÚLIO FABBRINI, *Código Penal interpretado*, Editora Atlas, 1999.

MIRANDA, JORGE e MEDEIROS, RUI, *Constituição da República Portuguesa Anotada*, Tomo I, 2.ª ed., Coimbra Editora, 2010.

MONIZ, HELENA, *Notas sobre a proteção de dados pessoais perante a informática (o caso especial dos dados pessoais relativos à saúde)*, RPCC 7, Coimbra Editora, 1997.

NORONHA, MAGALHÃES, *Direito Penal*, Vol. 4, Saraiva Editora, 1962.

PRADO, LUÍZ REGIS, *Curso de Direito Penal Brasileiro,* Volume 4, 2º Edição, Brasil: Editora Revista dos Tribunais.

PEREIRA, JOEL TIMÓTEO, *Direito da Internet e Comércio Eletrónico*, Lisboa: Quid Juris, 2001.

RAND Europe, *Comparative Study on Legislative and Non Legislative Measures to Combat Identity Theft and Identity Related Crime: Final Report*, 2011. Disponível em http://goo.gl/LzBGiV (últ. vez consult. em 22 de Maio de 2014).

TEIXEIRA, PAULO GONÇALVES, *O fenómeno do phishing - enquadramento jurídico-penal*, Dissertação Mestrado em Direito, Universidade Autónoma de Lisboa, 2011.
Disponível em http://goo.gl/AwmwXP (últ. vez consult. em 22 de Maio de 2014).

VENÂNCIO, PEDRO DIAS, *Lei do Cibercrime Anotada e Comentada*, Coimbra Editora, 2011.

VERDELHO, PEDRO, *Phishing e outras formas de defraudação nas redes de comunicação*, Direito da Sociedade de Informação, Volume VIII, Coimbra Editora, 2009.

VERÍSSIMO, JOANA, MACIAS, MARIA, RODRIGUES, SOFIA, *Implicações jurídicas das redes sociais na Internet: um novo conceito de privacidade?,* Dissertação de Mestrado em Direito da Comunicação, FDUNL, 2012. Disponível em http://goo.gl/H2PkHm (últ. vez consult. em 22 de Maio de 2014).

WISZNIEWSKI, DORIAN e COYNE, RICHARD, *Mask and Identity: The Hermeneutics of Self-Construction, The Information Age in Building Virtual Communities: Learning and Change in Cyberspace*, Ed. Renninger et al., New York: Cambridge University Press, 2002.

*Comunicados, artigos de imprensa e outras páginas na Internet*

BARLOW, John Perry, *A Declaration of the Independence of Cyberspace*, 1996. Disponível em http://goo.gl/WuuHqr (últ. vez consult. em 22 de Maio de 2014).

http://expresso.sapo.pt/76-acusados-por-phishing-acederam-a-111-contas=f858214

http://pt.wikipedia.org/wiki/Avatar_(realidade_virtual)

http://pt.wikipedia.org/wiki/Malware

http://pt.wikipedia.org/wiki/Rede_social

http://siteanalytics.compete.com/facebook.com/

http://tek.sapo.pt/noticias/internet/burlas_na_internet_crescem_20_1010055.html

http://tek.sapo.pt/noticias/internet/mickael_carreira_usado_para_fazer_despir_mulh_1311880.html

http://tek.sapo.pt/noticias/negocios/google_obrigada_a_indemnizar_jovem_difamado_n_1169562.html

http://tek.sapo.pt/noticias/telecomunicacoes/numero_de_utilizadores_de_banda_larga_movel_e_1351149.html

http://www.bit.pt/tribunal-europeu-defende-direito-ser-esquecido

http://www.ecofinancas.com/noticias/onu-indica-recorde-casos-roubo-identidade-internet-2012

http://www.europarl.europa.eu/news/pt/news-room/content/20140307IPR38204/html/Parlamento-Europeu-refor%C3%A7a-prote%C3%A7%C3%A3o-dos-dados-pessoais-dos-cidad%C3%A3os

http://www.jud.ct.gov/JI/criminal/part10/10.3-1.htm

http://www.marktest.com/wap/a/n/id~165b.aspx

http://www.marktest.com/wap/a/n/id~1a70.aspx

http://www.ncsl.org/research/financial-services-and-commerce/identity-theft-state-statutes.aspx