COLEÇÃO FORMAÇÃO CONTÍNUA

O DOMÍNIO DO IMATERIAL: PROVA DIGITAL, CIBERCRIME E A TUTELA PENAL DE DIREITOS INTELECTUAIS

JURISDIÇÃO PENAL

MAIO 2018

CENTRO DE ESTUDOS JUDICIÁRIOS

Diretor do CEJ
João Manuel da Silva Miguel, Juiz Conselheiro

Diretores Adjuntos
Paulo Alexandre Pereira Guerra, Juiz Desembargador
Luís Manuel Cunha Silva Pereira, Procurador-Geral Adjunto

Coordenador do Departamento da Formação
Edgar Taborda Lopes, Juiz Desembargador

Coordenadora do Departamento de Relações Internacionais
Helena Leitão, Procuradora da República

Grafismo
Ana Caçapo - CEJ

Capa
Edifício do CEJ

Foto
Victor Pimenta - CEJ

Conceitos de Tempo e de Espaço estão em mutação: uma sociedade em rede, planetarizada e digitalizada, quer económica, quer culturalmente, era - há bem poucos anos - apenas ficção científica...

Hoje, mais do que uma realidade, é - para além de tudo o que consigo traz de bom e de bem - fonte de problemas para o funcionamento de uma sociedade cujas regras não estavam preparadas para estes desenvolvimentos.

A área dos direitos de Autor e a tutela penal de que necessitam é um bom exemplo.

Como o é a adaptação das regras do processo penal à recolha de prova no universo digital.

É sobre tudo isso é necessário reflectir, criar inquietações e abrir pistas de solução.

"O domínio do imaterial: prova digital, cibercrime e a tutela penal dos direitos intelectuais" junta textos e apresentações que correspondem às intervenções ocorridas em acções de formação organizadas pelo Centro de Estudos Judiciários, em 2017 e 2018, e que podem agora alimentar uma discussão que não termina, mas que permite a quem se defronta com os problemas ter mais elementos de ponderação e estudo.

Mais um e-book da "Coleção Formação Contínua" que fica disponibilizado a toda a Comunidade Jurídica, em acesso livre.

(ETL)

CENTRO
DE ESTUDOS
JUDICIÁRIOS

Ficha Técnica

Nome:
O domínio do imaterial: prova digital, cibercrime e a tutela penal de direitos intelectuais

Jurisdição Penal:
Helena Susano – Juíza de Direito, Docente do CEJ e Coordenadora da Jurisdição
José Quaresma – Juiz de Direito e Docente do CEJ
Alexandre Au-Yong de Oliveira – Juiz de Direito e Docente do CEJ
Rui Cardoso – Procurador da República e Docente do CEJ
Susana Figueiredo – Procuradora da República e Docente do CEJ
Patrícia Naré Agostinho – Procuradora da República e Docente do CEJ
Miguel Rodrigues – Procurador da República e Docente do CEJ

Coleção:
Formação Contínua

Plano de Formação 2017/2018:
Temas de Direito Penal e Processual Penal – 9 e 16 de fevereiro e 2 e 9 de março de 2018 (programa)

Plano de Formação 2016/2017:
Temas de Direito Penal e Processual Penal - Porto, 10 de fevereiro de 2017 (programa)

Conceção e organização:
Jurisdição Penal

Intervenientes:
Manuel Oehen Mendes – Advogado e Docente convidado da UCP/Porto
Alexandre Oliveira – Juiz de Direito e Docente do CEJ
David Silva Ramalho – Assistente Convidado da Faculdade de Direito da Universidade de Lisboa, investigador do Centro de Investigação de Direito Penal e Ciências Criminais e Advogado
Nuno Serdoura dos Santos – Procurador da República
Pedro Verdelho – Procurador da República
Baltazar Rodrigues – Chefe do Gabinete de Tecnologia e Informática da Polícia Judiciária

Revisão final:
Edgar Taborda Lopes – Juiz Desembargador, Coordenador do Departamento da Formação do CEJ
Ana Caçapo – Departamento da Formação do CEJ

Notas:

Para a visualização correta dos e-books recomenda-se o seu descarregamento e a utilização do programa Adobe Acrobat Reader.

Foi respeitada a opção dos autores na utilização ou não do novo Acordo Ortográfico.

Os conteúdos e textos constantes desta obra, bem como as opiniões pessoais aqui expressas, são da exclusiva responsabilidade dos/as seus/suas Autores/as não vinculando nem necessariamente correspondendo à posição do Centro de Estudos Judiciários relativamente às temáticas abordadas.

A reprodução total ou parcial dos seus conteúdos e textos está autorizada sempre que seja devidamente citada a respetiva origem.

Forma de citação de um livro eletrónico (NP405-4):

AUTOR(ES) – **Título** [Em linha]. a ed. Edição. Local de edição: Editor, ano de edição.
[Consult. Data de consulta]. Disponível na internet: <URL:>. ISBN.

Exemplo:
Direito Bancário [Em linha]. Lisboa: Centro de Estudos Judiciários, 2015.
[Consult. 12 mar. 2015].
Disponível na
internet: <URL: http://www.cej.mj.pt/cej/recursos/ebooks/civil/Direito_Bancario.pdf.
ISBN 978-972-9122-98-9.

Registo das revisões efetuadas ao e-book

Identificação da versão	Data de atualização
1.ª edição –07/05/2018	

O domínio do imaterial: prova digital, cibercrime e a tutela penal de direitos intelectuais

Índice

CENTRO
DE ESTUDOS
JUDICIÁRIOS

1.

A tutela penal do Direito de Autor e outros temas conexos

Manuel Oehen Mendes

CENTRO
DE ESTUDOS
JUDICIÁRIOS

A TUTELA PENAL DO DIREITO DE AUTOR E OUTROS TEMAS CONEXOS**

Manuel Oehen Mendes*

Sumário: *A presente intervenção pretende chamar a atenção para a razão de ser do recurso à última* ratio *do direito penal na tutela de interesses de natureza, à primeira vista, essencialmente privados. Onde a natureza imaterial dos bens protegidos permite a sua utilização ubíqua, sem desapossamento do titular, diminuindo, assim, o grau de censura ética pela sua violação. De seguida, procurámos identificar algumas características comuns aos crimes jusautorais e analisar, com mais detalhe, os quatro tipos de crime capitais: contrafacção; usurpação; violação de direitos morais e aproveitamento de obra usurpada ou contrafeita, ou de cópia não autorizada de fonograma ou videograma. Por fim - e antes de fazer um breve balanço das vantagens e desvantagens práticas do recurso à tutela penal -, abordámos a incriminação de certas condutas aptas a pôr em risco o exclusivo dos autores ou as faculdades atribuídas aos titulares dos direitos conexos, tais como, a neutralização das medidas eficazes de carácter tecnológico, a informação para a gestão electrónica dos direitos e a violação do acesso condicionado às comunicações electrónicas codificadas.*

Palavras-chave: *acesso condicionado; adaptação; bases de dados; colocação à disposição do público; contrafacção; crime público; direito penal de autor; direitos conexos; direitos morais; direitos patrimoniais; dispositivos ilícitos; distribuição; divulgação; gestão electrónica de direitos; medidas de carácter tecnológico; negligência; obra; plágio; prestação; princípio da adesão; programas de computador; reincidência; responsabilidade civil; sanções; tentativa; usurpação; utilização.*

I. Justificação

O Direito de Autor é, indiscutivelmente, direito privado e quer o qualifiquemos como um seu ramo, como sucede, por exemplo, com o Direito Comercial ou com o Direito do Trabalho, ou como um direito civil *especial*, como parece indicar a letra do artº 1303º, nº 1 do Código Civil[1], o que é facto é que este ramo do direito tem, em primeira linha, por finalidade proteger *interesses particulares* dos autores e dos titulares dos direitos conexos, bem como os *interesses privados* da indústria da cultura que, hoje em dia, é quem promove e explora economicamente as obras e as prestações protegidas.

** Texto que serviu de base à conferência proferida pelo autor no CEJ / Porto, em 3 de Fevereiro de 2017, inicialmente publicado na Revista do CEJ 2017 – I, CEJ, Almedina, 2017, pags. 189-204.

* Advogado e Docente convidado da UCP/Porto.

[1] Para o Professor Oliveira Ascensão, p. ex., o Direito de Autor seria um novo ramo do Direito Civil e não uma *especialização*, para um certo sector, dos princípios gerais do Direito Civil. Situando-se ao lado do Direito da Família, das Sucessões, etc. Seja como for, um conjunto de normas que regula um sector diferenciado da vida dos particulares. Cfr. *Direito Civil - Direito de Autor e Direitos Conexos*, Coimbra, 1992, pp. 29 s.

Não obstante, é inegável a existência de um relevante *interesse público* na promoção e estímulo à criação artística, científica e literária, o qual justifica igualmente a sua tutela jurídica e encontra, entre nós, inclusive, consagração constitucional no artº 42º *("Liberdade de criação cultural")* da CRP [2].
Por outro lado, os direitos de autor e os direitos conexos são direitos patrimoniais privados, ainda que dotados com uma vertente pessoal acentuada. Nesta dimensão, são direitos análogos aos direitos de propriedade (de onde a denominação tradicional de direitos da "propriedade intelectual") e gozam, por isso, de idêntica protecção à que é conferida pelo artº 62º da Constituição da República à propriedade sobre as coisas corpóreas [3].

Sucedendo que a tutela penal da *propriedade*, em sentido lato, é um dado adquirido pela nossa ordem jurídica, que hoje ninguém discute (artºs 203º e ss. CP).

Por fim, o reconhecimento dos *direitos pessoais* dos autores e, em certa medida, dos titulares de determinados direitos conexos[4], os ditos "direitos morais", justificariam igualmente o reforço da tutela civil através do recurso à última *ratio* do direito penal.[5]

Todas estas razões, aqui sumariamente enunciadas, sustentam a tradição europeia continental, quer do *"Droit d'auteur"*, quer do *"Urheberrecht"*, de proteger criminalmente, com uma amplitude e intensidade maior ou menor, a violação dos direitos de autor e dos direitos conexos. O direito francês, p. ex., incluiu inicialmente a violação dos direitos de autor no próprio Código Penal (artºs 425º e 428º), sendo que tais disposições apenas transitaram para a Lei do Direito de Autor em 1957 [6].

Em relação ao *copyright* anglo-saxónico, poderá sustentar-se que a tutela penal foi adoptada mais recentemente, em virtude, sobretudo, da violação em massa destes direitos, proporcionada pela digitalização das obras e prestações, pela utilização generalizada da informática e pelas novas tecnologias das telecomunicações, mas o recurso a este meio de

[2] Este *interesse público*, que não deve ser confundido com o *interesse do público* à queda no *domínio público* e ao *livre acesso* às obras protegidas, é particularmente acentuado nos sistemas anglo-saxónicos do *copyright*, como nos dá conta, p. ex., Gillian Davies, na sua obra de referência *Copyright and the Public Interest*, 2ª ed., Londres, 2002.
[3] Para uma valoração semelhante no direito alemão (art.º 14º da *Grundgesetz*), cfr., p. ex., Fromm/Nordemann, *Urheberrecht*, 11ª ed., Estugarda, 2014, anot. 11 à introdução ao § 106 UrhG.
[4] Na nossa ordem jurídico-autoral, os artistas intérpretes e executantes gozam do reconhecimento expresso de certos direitos morais, concretamente: do direito ao nome e do direito ao respeito pela integridade da prestação, nos termos do disposto nos artºs 180º e 182º, respectivamente, do CDADC.
[5] Para o Professor Oliveira Ascensão, estes direitos pessoais dos autores justificariam, por maioria de razão, a tutela penal que o CDADC decidiu consagrar para os direitos patrimoniais. Constatando-se, no entanto, segundo este Autor, uma *inversão de valores* ou a ausência de uma justificação *ética* para esta criminalização, uma vez que "as violações do direito pessoal recebem uma tutela menor", a saber: nem todas as manifestações destes direitos pessoais são criminalmente tuteladas e, ao contrário do que se verifica em relação aos direitos patrimoniais, o procedimento criminal depende de queixa. Cfr. *Direito Penal de Autor*, Lisboa, 1993, pp. 15 ss. Curiosamente, porém, no direito penal de autor alemão, que ninguém acusará, por certo, de falta de fundamento ético, a violação dos direitos morais dos autores não é, por regra, objecto de qualquer perseguição penal. Por outras palavras, a violação *exclusiva* de interesses patrimoniais privados (*maxime* da "propriedade") poderá envolver, em certas circunstâncias, um significativo conteúdo ético, suficiente para justificar uma reacção criminal. Cfr., por todos, Rehbinder/Peukert, *Urheberrecht*, 17ª ed.. Munique, 2015, p. 401, anotação à margem nº 1307; Dreier/Schulze, *Urheberrechtsgesetz - Kommentar*, 5ª ed., Munique, 2015, p. 1699, anotações à margem nºs 1 e 2. Por fim, o artº 67º, nº 2 do CDADC deixa claro que "[a] *garantia das vantagens patrimoniais (...) constitui, do ponto de vista económico, o objecto fundamental da protecção legal."*
[6] Cfr. Lucas *et al.*, *Traité de la propriété littéraire et artistique*, 4ª ed., Paris, 2012, p. 860.

defesa continua a ser bastante "marginal" ou secundário no combate quotidiano às infracções ao direito de autor e aos direitos conexos neste sistema jurídico [7].

II. Características da reacção criminal no âmbito do Direito de Autor

1. Uma das principais características do Direito Penal foi sempre a garantia conferida aos cidadãos pelo rigor da *tipicidade* das condutas criminalmente puníveis.

O direito penal de autor português introduz uma significativa derrogação deste princípio fundamental, ao recorrer a "normas incriminadoras em branco", as quais são, depois, integradas por *remissão* para os ilícitos civis relativos à violação dos direitos de autor e dos direitos conexos.

Para além disso, estas previsões legais recorrem também, com frequência, a conceitos indeterminados, tais como, p. ex., o de "quem utilizar..." (artºs 195º e 196º CDADC).

Porém, não é sequer rigoroso afirmar que, p. ex., as normas incriminadoras em branco contidas no artigo 195º CDADC podem ser integradas directamente pelas disposições que consagram os ilícitos civis correspondentes, pela simples razão de que estas normas "tipificadoras" civis não existem, enquanto tais. Com efeito, o CDADC não tipifica propriamente as condutas que constituem ilícitos civis por violação dos direitos de autor e dos direitos conexos.

O que a nossa lei faz é tão-só colocar a obra na disponibilidade *exclusiva* dos seus autores e delimitar o *conteúdo* dos poderes conferidos a esses mesmos autores para atingir aquele desiderato.

O artº 67º, nº 1 CDADC atribui aos autores o direito exclusivo de fruir e utilizar a obra; e o artº 68º, nº 2 do mesmo diploma enumera, exemplificativamente, os actos de exploração (actuais) em relação aos quais assiste ao autor "o direito exclusivo de fazer ou autorizar".

A *contrario*, estas condutas, quando incidam sobre uma obra protegida pelo DA e tenham sido levadas a cabo por um terceiro *sem autorização* do autor, serão ilícitas.

E, desta feita, por remissão, criminalmente puníveis nos termos dos artºs 195º e 199º CDADC. A falta de autorização é, portanto, o primeiro elemento objectivo deste tipo de crimes.

[7] Cfr. Gillian Davies *et al.*, *Copinger and Skone James on Copyright*, 17ª ed., Londres, 2016, pp. 1618 ss. (*"From the Copyright Act of 1709 to the end of nineteenth century, infringers were not liable to be imprisoned"*; só com a Lei de 1911, e apesar da considerável resistência do Parlamento, é que foram introduzidas sanções criminais em relação à violação do *copyright* para todas as categorias de obras protegidas); para o direito norte-americano, *vide,* p. ex., Leaffer, *Understanding Copyright Law*, 6ª ed., New Providence (NJ), 2014, pp. 479 ss. (*"In general, the government has not had a successful record of curbing criminal infringement actions, largely because of the burden of proof required in a criminal suit."*).

Um problema particular emerge a propósito das condutas de exploração económica de uma obra que *não estejam previstas* especialmente no CDADC, ou que tenham surgido como uma *nova forma* de exploração em data posterior à aprovação da sua versão em vigor.

Tendo em consideração os valores da segurança e da certeza jurídica que se destacam no direito criminal, através da adopção do *princípio da tipicidade*, não parecem restar dúvidas de que as condutas criminalmente puníveis só podem corresponder àquelas formas de exploração da obra ou prestação que estejam *suficientemente descritas* como passíveis de serem levadas a cabo pelo titular dos direitos, ou de serem autorizadas por este a terceiros. A tanto o exige também a observância do *princípio da legalidade*, consagrado no artº 29º CRP: *nullum crimen sine lege certa.*

Apesar de todas as suas especificidades, em homenagem ao princípio fundamental da *unidade da ordem jurídica*, o direito penal de autor tem de ser sempre interpretado e integrado de acordo com os princípios e regras do direito penal comum.

2. Outras características particulares dos crimes jusautorais:

A) São punidos a título de *negligência*, em qualquer das suas modalidades, ainda que só com pena de multa (nº 2 do artº 197º CDADC);

B) Poderá sustentar-se em relação a eles que a *tentativa* será punível [8], mesmo quando a moldura penal abstracta não ultrapasse os 3 anos de prisão, estabelecidos como limite excludente para a punição nesta modalidade, sem previsão expressa, pelo nº 1 do artº 23º CP, uma vez que o nº 2 do artº 197º CDADC acaba por estipular, de facto, uma pena máxima de 6 anos de prisão no caso de reincidência [9]. Devendo também ser levado em consideração o legislado para os programas de computador, que nada justifica que gozem de um regime mais favorável do que, por exemplo, aquele que usufruem as obras de arte plásticas ou do género da literatura [10];

C) São crimes públicos, que não dependem de queixa, nem admitem desistência (artº 200º CDADC), com excepção dos que envolvam *exclusivamente* a violação de direitos morais, que

[8] Com excepção da infracção ao direito de autor sobre as bases de dados criativas, como se explicita *infra* em nota.
[9] Apesar das críticas, entre outros, de Oliveira Ascensão, que considera exagerado que possa haver uma pena de 6 anos de prisão, por violação do direito de autor. *Direito Penal de Autor, in* AAVV, *Estudos em Homenagem ao Professor Doutor Manuel Gomes da Silva*, Lisboa, 2001, pp. 460 ss.
[10] No caso concreto dos programas de computador, a punição da tentativa está expressamente prevista no nº 3 do artº 8º da Lei nº 109/2009, de 15 de Setembro, uma vez que a violação dos direitos de autor sobre estas obras específicas é punida apenas com pena de prisão até 3 anos ou multa, sem agravação especial no caso de reincidência. Assimetricamente, a tentativa não será de todo punida no caso de infracção ao direito de autor sobre as bases de dados criativas, protegidas pelo Dec.-Lei nº 122/2000, de 4 de Julho, o qual não prevê essa possibilidade e limita a moldura penal aplicável a uma pena de prisão até 3 anos ou a pena de multa, sem mais. José A. Branco, *in* Paulo Pinto de Albuquerque / José Branco (coord.), *Comentário das Leis Penais Extravagantes*, Vol. II, Lisboa, 2011, anotando os artºs 195º e ss. do CDADC, entende, no entanto, que nenhum dos crimes aí previstos são passíveis de ser punidos a título de tentativa, tendo em conta a falta de previsão expressa nesse sentido e o disposto no artº 23º, nº 1 CP (cfr. pp. 258 e 260). Mas reconhecendo, ao mesmo tempo, que *"No que concerne à **pena de prisão** pode-se afirmar, linearmente, que serão os crimes punidos com prisão 'até seis anos'."* (p. 261). Por outro lado, deve ter-se presente que o regime geral da reincidência não conduz, por si só, a qualquer agravamento do limite máximo das molduras penais (artº 76º, nº 1 CP).

dependem de queixa e assumem, assim, uma natureza semipública (artºs 200º e 198º CDADC) [11];

D) O princípio da adesão é facultativo, podendo a responsabilidade civil ser exercida tanto em acção autónoma, como em conjunto com o processo crime (artº 203º CDADC);

E) A severidade das sanções, donde se destaca o limite máximo da pena de prisão, que é de 3 anos, mas que poderá ir até aos 6 anos, em caso de reincidência[12] (cfr. artºs 197º, 198º e 199º CDADC e artºs 75º e 76º CP), e o carácter *cumulativo* da pena de multa[13] que, nos termos do CDADC, pode atingir um máximo de 500 dias (cfr. artº 47º, nº 1 do CP, que estabelece, por regra, um limite máximo de 360 dias). A disposição prevendo que, em caso de reincidência, não poderá haver suspensão da pena (artº 197º, nº 3) deverá ser considerada revogada pelo nº 3 do artº 2º do Dec.-Lei nº 48/95, de 15 de Março, que aprovou o Código Penal revisto.

III. Os quatro crimes capitais

Analisando o objecto da nossa exposição mais detalhadamente, o CDADC incrimina, em particular, quatro tipos de condutas. A exploração não autorizada da obra ou da prestação de outrem. A apresentação como própria de obra alheia, vulgo *"plágio"*. A divulgação de obra "contrafeita" ou "plagiada" e a violação de certas prerrogativas pessoais dos autores e dos artistas intérpretes ou executantes. [14]

1. Comecemos pelo primeiro. O artº 195º CDADC, sob a epígrafe de "usurpação"[15], pune, no seu nº 1, quem, sem autorização do autor ou do artista, do produtor de fonograma e videograma ou do organismo de radiodifusão, utilizar uma obra ou prestação por qualquer das formas previstas no CDADC.

Como já fizemos referência, o artº 195º configura uma norma penal em branco, que apenas cumprirá os "mínimos" para a sua aceitação constitucional, por remissão para outras normas do *mesmo diploma* que permitirão que ela seja suficientemente completada. Não sem

[11] Cfr., p. ex., José A. Branco, *ob. cit.*, p. 269.
[12] A reincidência nestes crimes não será, no futuro, com certeza, uma situação muito excepcional, tendo em conta as "tentações" proporcionadas pelas facilidades do mundo digital e a utilização massiva da Internet.
[13] Admitido pelos artºs 6º e ss. do Dec.-Lei nº 48/95, de 15 de Março, que aprovou o CP revisto. Constituem excepção a este regime de cumulação os crimes resultantes da violação de direitos de autor sobre programas de computador e bases de dados criativas, regulados por legislação especial.
[14] A *falsificação*, nomeadamente no domínio das artes plásticas, que consiste na apresentação da *cópia* de uma obra, realizada por pessoa diferente do seu autor, como se ela fosse o *original* dessa mesma obra, não está contemplada no CDADC, sendo antes do domínio das previsões do Código Penal, através da aplicação dos dispositivos relativos ao crime de burla (artºs 217º e s. CP) e, porventura, à falsificação de documento (p. ex., de um certificado de autenticidade de um quadro; artº 256º CP). O CDADC proíbe, no entanto, o uso em obra própria (original) do nome de autor alheio, ainda que com autorização deste (artº 29º, nº 3 CDADC); a lei alemã do direito de autor criminaliza, inclusive, esta hipótese no § 107 UrhG. A *imitação de um estilo*, de uma *moda*, *de um género musical*, *de uma tendência estética*, etc., por mais originais ou característicos que sejam, não configura, por sua vez, qualquer violação do direito de autor. Cfr., por todos, Rehbinder / Peukert, *ob. cit.*, p. 28, anot. à margem nº 80.
[15] A qual aparece manifestamente "trocada" com a epígrafe do artº 196º ("Contrafacção"), como demonstrou na doutrina, há muitos anos, o Prof. Oliveira Ascensão, sem qualquer resultado do ponto de vista das reformas legislativas que o Código entretanto sofreu. Cfr. *Direito Penal de Autor,* Lisboa, 1993, p. 19.

dificuldades, pelas razões que já atrás mencionámos: com efeito, não existem no CDADC verdadeiros "tipos" de ilícitos civis que possam integrar *directamente* aquela norma em branco, com a segurança, suficiência e transparência requeridas.

Para além da *falta de autorização* do titular dos direitos envolvidos (autores e titulares de direitos conexos), sempre que exigível, os outros dois elementos objectivos do tipo são os conceitos indeterminados de *obra* ou *prestação* e de *utilização* em qualquer das formas previstas neste Código.

Pois bem, a noção de *obra* (protegida) terá de ser construída a partir da interpretação dos artºs 1º a 3º do CDADC e as *prestações* relevantes são aquelas que constituem o objecto dos direitos conexos consagrados nos artºs. 176º e ss. do mesmo diploma.

Quanto às *formas de utilização / exploração* que carecem de autorização, deverão ser encontradas no cotejo do disposto nos artºs. 68º e 75º (utilizações lícitas) do CDADC, o que nem sempre se tem revelado ser uma tarefa fácil. A exploração que dependa apenas do pagamento de uma *remuneração* ao titular dos direitos não deverá ser considerada entre as formas de exploração potencialmente incriminadores.

O *bem jurídico* protegido por esta norma é o conjunto das faculdades / vantagens patrimoniais que decorrem da utilização da obra ou prestação e que são atribuídas ao titular dos direitos de autor ou dos direitos conexos [16].

O artº 195º desdobra-se, no entanto, num conjunto de outros tipos de crime - autónomos ou não, é discutível -, em que os bens jurídicos protegidos nem sempre são de natureza predominantemente patrimonial.

Assim, a alínea a) do nº 2 prevê e pune a chamada violação do direito ao inédito, cujo bem jurídico é essencialmente o *direito pessoal* (ou moral) do autor à não divulgação da obra sem a sua autorização. Por esta razão, a norma em causa não prevê as *prestações* protegidas pelos direitos conexos, mas apenas as *obras* do direito de autor. A proibição mantém-se, como é óbvio, mesmo naqueles casos - os mais comuns - em que a divulgação não põe em causa a paternidade da obra, isto é, mesmo naquelas hipóteses em que a obra é divulgada com o nome do seu verdadeiro autor.

O preceito prevê, porém, que a divulgação seja *abusiva*, o que corresponde à exigência de um elemento subjectivo no tipo, qual seja o da *consciência* de que se está a cometer um abuso[17]. Seja como for, não nos podemos esquecer que este crime, tal como os demais aqui em apreço, será punido mesmo sob a forma de um comportamento negligente.

A alínea b) refere-se às colectâneas ou compilações de obras, levadas a cabo sem autorização dos autores das obras compiladas, o que já caberia na incriminação do nº 1. A compilação é uma utilização que, como qualquer outra, depende de *autorização* (cfr. artº 68º, nº 1 e, em

[16] Cfr. Valter Alves, *O crime de usurpação de direitos de autor*, Coimbra, 2014, p. 57.
[17] Cfr. Luís Menezes Leitão, *Direito de Autor*, Coimbra, 2011, p. 300.

especial, artºs 7º, nº 2 e 76º, nº 3 CDADC). O Prof. Oliveira Ascensão diz, por isso, que *"À primeira vista o preceito não se entende."* Sendo, ao fim e ao cabo, uma previsão dispensável[18].

A alínea c) volta a incluir as *prestações* cobertas pelos direitos conexos e incrimina a exploração da obra ou prestação para lá dos limites da autorização (licença) que haja sido concedida pelo titular dos direitos. O objectivo é punir a conduta descrita, não apenas como uma mera *violação do contrato* que autorizou ao agente, observados certos termos e condições, a exploração da obra ou prestação, mas como uma verdadeira *infracção ao direito de exclusivo* do autor ou ao *direito de impedir certos actos* atribuído ao titular dos direitos conexos. Esta disposição faz toda a diferença do ponto de vista do *enforcement* dos direitos de autor, face aos limites impostos aos beneficiários de contratos de licença de exploração de direitos de autor e de direitos conexos.

Por último, o nº 3 do artº 195º consagra o curioso crime do "auto-plágio", não no sentido de alguém que apresenta como sua obra de autor alheio ("plágio" em sentido estrito), mas na medida em que o autor pode ser condenado criminalmente por utilizar a sua própria obra. Por exemplo, quando tendo celebrado um contrato de edição de um livro com um determinado editor, utiliza um capítulo desse mesmo livro para integrar uma outra obra da sua autoria, ou em co-autoria, ou quando coloca esse mesmo texto à disposição do público num *site* da Internet, sem autorização do editor. A publicação múltipla da mesma obra em diferentes locais ou suportes é frequente em certas áreas científicas.

Uma vez mais, a punição criminal a sobrepor-se à mera responsabilidade civil resultante da violação do contrato (*in casu,* de edição), favorecendo não o autor, mas os *interesses económicos* de um terceiro (o editor), que constituem o bem jurídico protegido por este tipo de crime. Uma clara vantagem para a indústria da cultura, alcançada através da criminalização do incumprimento contratual, em detrimento dos interesses particulares dos autores que lhe fornecem a matéria prima.

Como nestes contratos só pode estar em causa a cessão de direitos patrimoniais, a ofensa aos mesmos - com a verificação de um prejuízo efectivo - constitui um elemento objectivo do tipo, transformando-o, assim, num crime de resultado, ao contrário do que sucede com as outras hipóteses contempladas no artº 195º CDADC [19].

Esta norma incriminadora não abrange, porém, a violação dos contratos de licença relativos às *prestações* tuteladas por meros direitos conexos.

2. O artº 196º CDADC, sob a epígrafe "Contrafacção" (leia-se "Usurpação"), tipifica o crime que consiste basicamente na exploração voluntária de uma obra ou prestação com usurpação da respectiva autoria. Fazendo-se passar o agente por autor ou criador da mesma. A exploração

[18] *Últ. ob. cit.*, p. 25.
[19] Cfr. Valter Alves, *ob. cit.*, p. 131. Autor que propõe (p. 132 ss.) uma interpretação restritiva deste nº 3 do artº 195º CDADC, que não partilhamos, excluindo aqueles casos que possam ser subsumidos à mera responsabilidade civil por incumprimento contratual do titular dos direitos de autor que foram objecto de licenciamento.

da obra cuja autoria foi usurpada pode ter lugar tal qual ela foi criada pelo seu verdadeiro autor ou sob uma forma de tal modo semelhante que não se possa atribuir-lhe qualquer individualidade própria (nº 1). O "pastiche", por exemplo, sendo normalmente criativo e transparente, não deve ser considerado como "contrafacção".

A "contrafacção" pode ser total ou parcial, isto é, pode dizer respeito tanto à obra ou à prestação completas, como apenas a uma parte delas, sendo punida da mesma forma num caso ou noutro, apesar de a parte final do nº 2 do artº 196º dizer que só se considera como contrafeita a parte da obra ou prestação que efectivamente o haja sido... Um preciosismo inútil.

A exploração da obra "contrafeita" ("utilização" ou "reprodução", no texto da lei[20]) não necessita de ser realizada pelo mesmo processo que foi utilizado pelo original, respeitando as mesmas dimensões ou o mesmo formato, isto é dizer, pode consistir, por exemplo, numa *adaptação* de um romance ao cinema ou a uma obra de teatro. Todavia, a criação de uma coreografia (bailado) a partir de um determinado texto literário (um poema, p. ex.) já não vemos como possa ser considerada uma *reprodução* desse texto, dada a enorme distância existente entre as *formas de expressão* utilizadas (obra literária *versus* obra coreográfica), ainda que recorrendo a um mesmo conteúdo ou ideia. Na nossa opinião, a coreografia implicará sempre, em relação ao texto literário, uma *individualidade criativa* tal que a afastará – quase que necessariamente – de todo e qualquer juízo de "contrafacção". Na verdade, para que esta exista em relação a uma *adaptação*, terá que estar presente na obra "contrafeita" uma boa dose da *forma de expressão* característica da obra adaptada. Pelo menos para efeitos da previsão penal, por exigência da mais elementar certeza e segurança jurídica dos envolvidos.

Tendo em conta, sobremaneira, a admissibilidade da comissão deste crime por meio da *adaptação* de uma obra a outro género diferente do da obra adaptada (p. ex., por "conversão" de um filme numa representação cénica), não se compreende bem a exigência que faz alguma doutrina de que, para haver contrafacção, terá de existir necessariamente a *produção de exemplares* da obra contrafeita (no caso, uma representação teatral!) [21].

O nº 4 da referida disposição legal dá-nos, por sua vez, alguns exemplos, mais ou menos felizes, de condutas que não constituem "contrafacção" (delimitação negativa do tipo?), de onde destacamos a eventual semelhança das traduções de uma mesma obra ou a que se verifique entre fotografias que representem o mesmo objecto, desde que cada uma delas apresente alguma individualidade própria (originalidade).

O bem jurídico tutelado parece ser, neste caso, mais complexo do que aquele que subjaz ao crime previsto e punido pelo artº 195º, uma vez que está aqui em causa a protecção

[20] Que demonstra alguma insegurança terminológica a este respeito, utilizando, como sinónimos, p. ex., as expressões "utilização" e "reprodução", ambas formas de exploração da obra que se pretende acautelar, mas com significado técnico diferente no âmbito do Direito de Autor.
[21] Cfr., p. ex., Luís Menezes Leitão, *ob. cit.*, pp. 302 s., louvando-se na opinião de Oliveira Ascensão, e José A. Branco, *ob. cit.*, p. 259.

cumulativa de direitos patrimoniais e morais dos autores, bem como dos titulares dos direitos conexos, quando for o caso [22].

3. Para além da proibição da usurpação e contrafacção de obras e prestações protegidas, o CDADC incrimina igualmente o "aproveitamento" de obras contrafeitas ou usurpadas no seu artº 199º, sob a forma da colocação à venda, venda, importação, exportação ou qualquer outro modo de distribuição ao público da obra usurpada ou contrafeita, ou da cópia não autorizada pelo produtor de fonogramas ou videogramas (artº 184º CDADC), com independência do respectivo conteúdo e do facto de os *exemplares* terem sido produzidos no País ou no estrangeiro.

Esta referência ao local da produção dos *exemplares* envolvidos na prática do crime e à sua *distribuição* ao público por qualquer modo, tem levado uma parte importante da doutrina[23] a afirmar que também aqui só haverá ilícito criminal quando existir a produção de *exemplares* da obra contrafeita ou usurpada, ou dos fonogramas ou videogramas não autorizados. Ficando, assim, de fora desta incriminação, p. ex., a *colocação* da obra, do fonograma ou do videograma *à disposição do público* na Internet, que na doutrina e jurisprudência europeia - ao contrário do que sucede nos EUA - tem sido encarada como uma forma de *comunicação ao público* e não como uma manifestação do direito exclusivo de reprodução e *distribuição* da obra ou prestação.

Com isto, a disposição do artº 199º CDADC perde muito do seu interesse actual.

Por outro lado, o aproveitamento da obra contrafeita ou usurpada, ou das cópias não autorizadas dos fonogramas ou videogramas, já estará abrangido pela previsão dos artºs 195º e 196º, pelo que pode considerar-se que o tipo legal de crime do artº 199º se encontra numa relação de concurso aparente com os primeiros [24], devendo este artº 199º aplicar-se apenas àqueles casos em que o aproveitamento dos exemplares das obras ou das cópias ilícitas dos fonogramas ou videogramas é levado a cabo por um terceiro que não esteve envolvido nas práticas de contrafacção ou usurpação. Aproveitando-se delas apenas a jusante da conduta criminosa e, necessariamente, de forma *consciente*, isto é, com conhecimento - ou com violação do dever de diligência que conduziria a esse conhecimento - do carácter ilícito dos exemplares das obras ou dos fonogramas ou videogramas em causa.

Como nota, registe-se a curiosidade de que a pena de multa, em caso de negligência, não poderá ir além dos 50 dias (nº 2 do artº 199º).

4. Por fim, a tutela penal dos direitos morais dos autores e dos artistas intérpretes ou executantes. O artº 198º, nº 1 fala-nos de obra ou *prestação*, mas, de facto, em relação a esta última, só os artistas interpretes ou executantes gozam da protecção de algumas faculdades

[22] Na verdade, no âmbito dos direitos conexos, só os artistas intérpretes e executantes gozam da protecção de direitos pessoais (artºs 180º e 182º CDADC), pelo que estes não podem constituir o elemento *dominante* do bem jurídico tutelado pelo artº 196º CDADC.
[23] Cfr. Oliveira Ascensão, *Direito Penal de Autor*, Lisboa, 1993, p. 47 (*"O objecto do tipo do artº 199º é sempre um exemplar"*), Luís Menezes Leitão, *ob. cit.*, p. 304, José A. Branco, *ob. cit.*, p. 264 s.
[24] Cfr. José A. Branco, *ob. cit*., pp. 258 e 266.

pessoais, que se encontram enunciadas nos artºs 180º (direito ao nome) e 182º (direito à integridade) do CDADC. Os organismos de radiodifusão e os produtores de fonogramas ou videogramas não têm, naturalmente, direitos pessoais reconhecidos no CDADC. O mesmo sucedendo com o direito *sui generis* do *fabricante* das bases de dados não criativas do Dec.-Lei nº 122/2000, de 4 de Julho.

Por outra parte, nem todos os direitos pessoais ou morais dos autores estão acautelados pelo artº 198º CPI. O direito ao inédito e o direito de retirada, p. ex., não estão previstos. Apenas o direito à paternidade e os direitos à genuinidade e à integridade da obra marcam presença. E quanto aos últimos, só quando o acto do agente for susceptível de desvirtuar a obra e afectar a honra ou reputação do autor.

Para os artistas intérpretes ou executantes, o direito ao nome é tutelado através da contra-ordenação prevista no artº 205º, nº 2 *in fine* do CDADC e o direito à integridade da prestação nos mesmos termos do direito de autor (artº 198º, b) *in fine*). Em virtude do regime estabelecido pelos nºs 1 e 2 do artº 180º CDADC, é duvidoso que o nosso legislador tenha querido consagrar um direito de paternidade para os artistas e que o tenha feito exclusivamente através da menção que consta na previsão penal da alínea a) do artº 198º CDADC [25].

Mesmo sendo lícita a utilização da obra ou prestação, a violação dos direitos morais dos autores ou dos artistas poderá continuar a constituir um crime, desde que estejam reunidos todos os requisitos, objectivos e subjectivos, do tipo do artº 198º CDADC.

A violação do direito de paternidade está também incluída entre os elementos objectivos do tipo do artº 196º, nº 1 ("*... quem utilizar, como sendo criação ou prestação sua ...*"), pelo que, tendo sido cometido aquele crime, o artº 198º, a) não terá aplicação. O mesmo não sucedendo, todavia, se quem se arroga falsamente a paternidade de uma obra ou prestação não chega a utilizar as mesmas. No mais, nada obsta ao concurso material do disposto no artº 198º com as previsões criminais do CDADC que se destinam a tutelar direitos patrimoniais.[26]

O bem jurídico protegido pelo artº 198º é a personalidade dos autores e dos artistas, através da atribuição aos mesmos de certos direitos pessoais, normalmente designados por direitos morais.

Como já foi referido, a violação *exclusiva* de direitos morais dos autores e dos artistas intérpretes ou executantes configura um crime semipúblico, que está dependente de queixa (artº 200º CDADC), e que é punido de acordo com o artº 197º CDADC, como, de resto, sucede com todos os demais anteriormente mencionados. O artº 202º estabelece um regime especial em relação à sanção acessória de apreensão dos exemplares em que se materialize apenas a violação de direitos morais.

[25] Com Oliveira Ascensão, *últ. ob. cit.*, pp. 45 s.
[26] Neste sentido, José A. Branco, *ob. cit.*, p. 264.

IV. Incriminações conexas

1. O direito de autor e os direitos conexos admitem que os respectivos titulares adoptem medidas de protecção de carácter tecnológico, para garantir o respeito pelos seus direitos de exclusivo (artº 217º). Neste sentido, o artº 218º CDADC considera um crime a *neutralização* não autorizada dessas medidas tecnológicas de protecção. São elementos, respectivamente, objectivos e subjectivos do tipo a *eficácia* da medida tecnológica adoptada pelo titular dos direitos e a *consciência* - ou a violação do dever de diligência que conduziria a essa mesma consciência - do agente de que, com a sua conduta, está a neutralizar, sem autorização, uma medida tecnológica de protecção eficaz. A definição do que se deve entender por uma medida eficaz de carácter tecnológico consta do nº 2 do artº 217º CDADC e é, assim, uma noção normativa.

A moldura penal deste crime é de até um ano de prisão ou multa até 100 dias. A tentativa é punível com multa até 25 dias. Ao contrário do que vimos em relação à generalidade dos crimes de direito de autor, a negligência, neste caso, não é punida.

Certos *actos preparatórios* desta infracção estão contemplados e são punidos com pena de prisão ou multa pelo artº 219º CDADC.

2. De forma idêntica, é assegurada aos autores e aos titulares de direitos conexos e do direito *sui generis* sobre as bases de dados não criativas a faculdade de adoptarem dispositivos destinados a obter a informação necessária para a gestão electrónica dos seus direitos (artº 223º CDADC).

Nesta conformidade e de acordo com o artº 224º CDADC, constitui crime punível com pena de prisão até um ano ou com pena de multa até 100 dias:

> a) A supressão ou alteração de qualquer informação destinada à gestão electrónica de direitos;
>
> b) A distribuição, importação para distribuição, comunicação ao público ou colocação à disposição do público de obras, prestações ou produções protegidas, das quais tenha sido suprimida ou alterada, sem autorização, a informação para a gestão electrónica dos direitos, sabendo o agente que, em qualquer das situações indicadas, está a provocar, permitir, facilitar ou dissimular a violação de direitos da propriedade intelectual.

Este crime é doloso e pressupõe a consciência - ou a violação de um dever de diligência: "sabendo ou tendo motivos razoáveis para saber" - do significado dos actos acima descritos. A tentativa é punível com multa até 25 dias.

Tanto o crime de neutralização de medidas eficazes de carácter tecnológico (artº 218º), como aquele que acabámos de descrever podem implicar, como pena acessória, a "perda de coisas", incluindo o lucro ilícito obtido pelo infractor (artº 225º), e a responsabilidade civil deles

decorrente é independente do procedimento criminal, podendo, contudo, ser exercida em conjunto com a acção penal (artº 226º).

3. Coadjuvando os meios próprios da tutela penal *directa* do direito de autor e dos direitos conexos - e em sintonia com o disposto no artº 228º do CDADC [27] -, a Lei das Comunicações Electrónicas [28], que não tem como destinatários os autores ou os titulares dos direitos conexos ou de direitos *sui generis* (artº 2º, nº 1, a) e b) da referida Lei), garantindo a inviolabilidade das emissões codificadas, as quais estão sujeitas a um regime de acesso condicionado pela obtenção da respectiva autorização, protege também, *indirectamente*, os interesses da defesa da propriedade intelectual, em particular dos organismos de radiodifusão.

Criminalizando, através do seu artº 104º, a) o fabrico, importação, distribuição, venda, locação ou detenção, para fins comerciais de *dispositivos ilícitos*.

Sendo considerados como tal, nos termos da alínea a) do nº 2 do artº 104º da Lei das Comunicações Electrónicas, todo o equipamento ou programa informático concebido ou adaptado com vista a permitir o acesso a um serviço protegido, sob forma inteligível, sem autorização do prestador desse serviço.

A este crime semipúblico (o procedimento criminal depende de queixa) corresponde uma moldura penal de até 3 anos de prisão ou pena de multa, se ao caso não for aplicável pena mais grave. A tentativa é punível.

Por outro lado,

> b) A instalação, manutenção ou substituição, para fins comerciais, de dispositivos da mesma natureza; e
>
> c) A utilização de comunicações comerciais de promoção desses dispositivos são consideradas contra-ordenações muito graves, nos termos da alínea zz) do nº 3 do artº 113º.

Enquanto,

> d) A aquisição, utilização, propriedade ou mera detenção, a qualquer título, de dispositivos ilícitos *para fins privados* do adquirente, do utilizador, do proprietário ou do detentor constitui uma contra-ordenação grave, nos termos da alínea oo) do nº 2 do mesmo artº 113º da Lei das Comunicações Electrónicas.

4. Por último, é importante destacar que, quando as infracções contempladas no CDADC forem cometidas por meio de um sistema informático ou quando for necessário proceder à recolha de prova em suporte electrónico, aplicam-se as disposições processuais, bastante mais

[27] *"Tutela por outras disposições legais. A tutela instituída neste Código não prejudica a conferida por regras de diversa natureza relativas, nomeadamente, (...) [ao] acesso condicionado (...)".*
[28] Lei nº 5/2004, de 10 de Fevereiro, com alterações sucessivas.

eficazes, previstas na Lei do Cibercrime[29], com excepção dos artºs 18º e 19º (intercepção de comunicações e acções encobertas, respectivamente) dessa mesma Lei (cfr. artº 11º da Lei do Cibercrime).

V. Vantagens e desvantagens do recurso à tutela penal do direito de autor e direitos conexos

Em jeito de balanço conclusivo da nossa exposição, podemos dizer que o recurso à tutela penal nesta matéria de natureza essencialmente civil, tem as vantagens naturais do efeito dissuasor da prevenção geral própria das sanções criminais. Para além disso, nalguns casos, sobretudo relacionados com as infracções praticadas por meios informáticos, *maxime* na Internet, a recolha e a produção de prova só são viáveis com a ajuda dos órgãos especializados de polícia criminal e do MP.

Em tudo o mais, predominam as desvantagens: em primeiro lugar, o grau de exigência em relação à qualidade da prova que tem de ser produzida para se lograr uma condenação penal ("para além de qualquer dúvida razoável"); em segundo lugar, a incompetência do Tribunal especializado da Propriedade Intelectual em matéria criminal; em terceiro lugar, a censura ética ainda pouco exigente no que toca a certos tipos de conduta criminosa nesta área, o que está longe de ser um fenómeno exclusivamente nacional (exemplo: a partilha de ficheiros em rede); em quarto e último lugar, os obstáculos colocados à solução negociada dos litígios, em resultado da natureza pública da maioria dos crimes em questão, que não admitem desistência.

Vídeo da apresentação

https://educast.fccn.pt/vod/clips/6dd0g4l02/flash.html?locale=pt

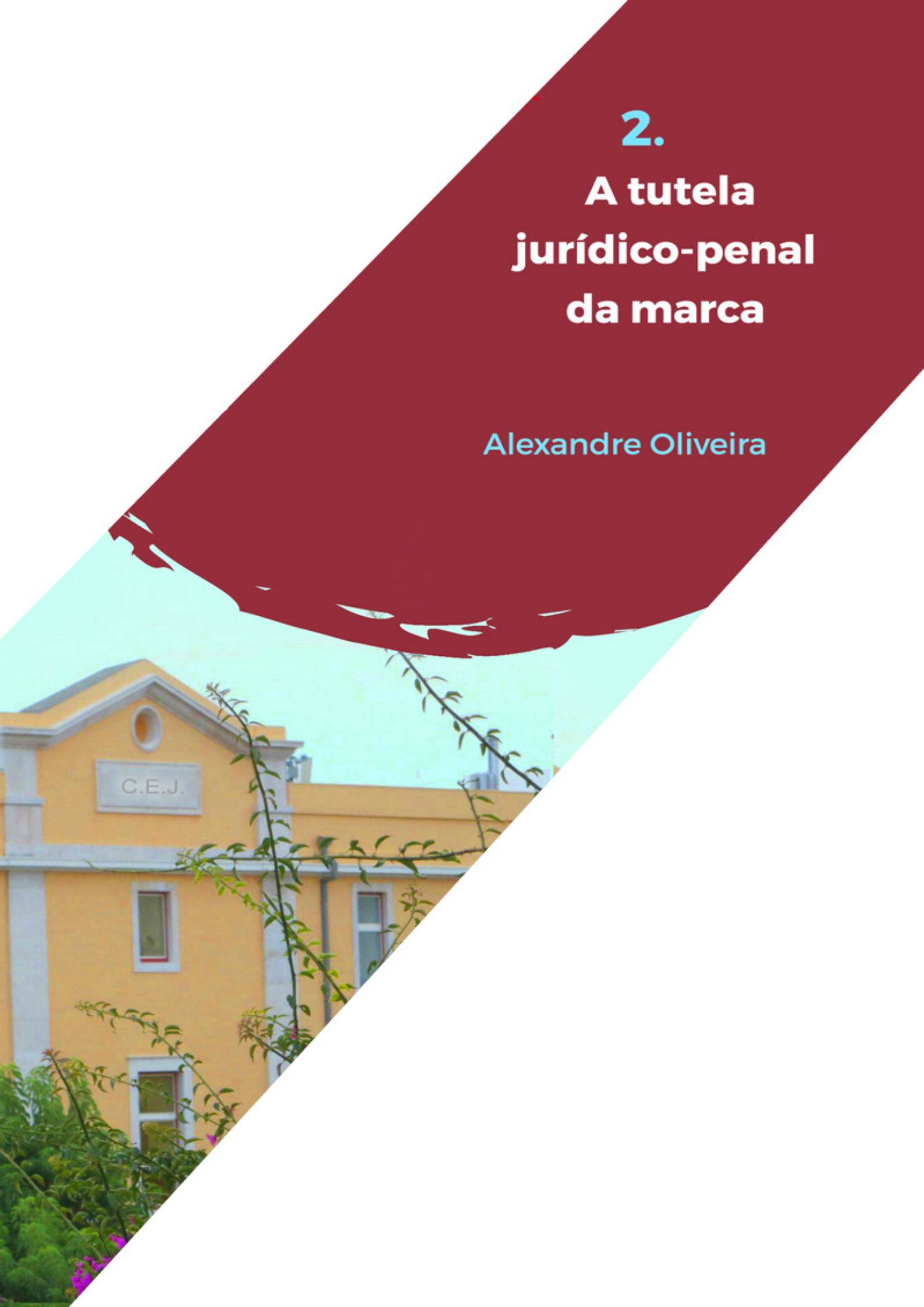
[29] Lei nº 109/2009, de 15 de Setembro.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

2.

A tutela jurídico-penal da marca

Alexandre Oliveira



CENTRO
DE ESTUDOS
JUDICIÁRIOS

A TUTELA JURÍDICO-PENAL DA MARCA**

Alexandre Oliveira*

** Apresentação que serviu de base à conferência proferida pelo autor no CEJ / Porto, em 3 de Fevereiro de 2017.
* Juiz de Direito e Docente do CEJ.

I. INTRODUÇÃO ÀS MARCAS
II. TUTELA PENAL DA MARCA
III. CAUSAS DE EXCLUSÃO DA ILICITUDE

2

I. INTRODUÇÃO ÀS MARCAS

3

VISÃO GERAL

- ✓ **Definição**: Sinal (i) susceptível de representação gráfica e (ii) que permita distinguir no mercado os produtos/serviços de uma empresa dos das outras empresas
- ✓ **Função essencial**: garantir aos consumidores a proveniência do produto/serviço
- ✓ **Outras funções**: garantia de qualidade, comunicação, investimento, publicidade

VISÃO GERAL

- ✓ **Direito subjectivo absoluto, oponível *erga omnes***: confere aos titulares um monopólio de exploração, impondo a todos os demais sujeitos a obrigação de não exploração (cf. arts. 224.º, n.º 1 e 258.º do CPI)
- ✓ Direito sujeito a registo constitutivo

Requisitos Essenciais

SUSCEPTIBILIDADE DE REPRESENTAÇÃO GRÁFICA

6

PALAVRAS, LETRAS, NÚMEROS, CORES, DESIGN

YAHOO®

(MARCA NOMINATIVA OU VERBAL)

(MARCA NOMINATIVA ESTILIZADA)

DESENHOS OU IMAGENS

(MARCA FIGURATIVA)

CONJUGAÇÕES DE ELEMENTOS VERBAIS E FIGURATIVOS

(MARCA MISTA)

FORMAS, SONS, CHEIROS, GESTOS, CORES ÚNICAS

(MARCAS NÃO TRADICIONAIS)

CONFIGURAÇÃO DE UM ESPAÇO

(MARCAS NÃO TRADICIONAIS)

Requisitos Essenciais

CARÁCTER DISTINTIVO

12

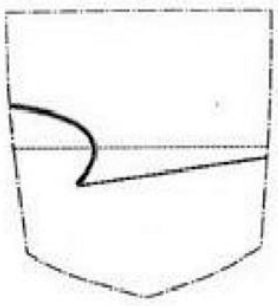
CARÁCTER DISTINTIVO

- ✓ O carácter distintivo é uma questão de grau
- ✓ Não são distintivos os **sinais descritivos** da espécie, qualidade, origem, finalidade ou outras características, nem os **sinais genéricos**
- ✓ É distintivo em grau reduzido o **sinal alusivo**, que alude a características dos produtos, mas não é exclusivamente descritivo relativamente às mesmas, e.g. "bom", "super"
- ✓ Considera-se que um sinal que não é descritivo nem alusivo possui um grau «normal» de carácter distintivo intrínseco
- ✓ Um maior grau de carácter distintivo pode ser adquirido através da utilização e da reputação daí derivada ("**significado secundário**")

MERAMENTE DESCRITIVO?

(CONSERVAS DE PEIXE)

FALTA DE CAPACIDADE DISTINTIVA



(CALÇAS DE GANÇA, CALÇÕES, SAIAS)

MERAMENTE DESCRITIVO

"ÉVORA HOTEL"

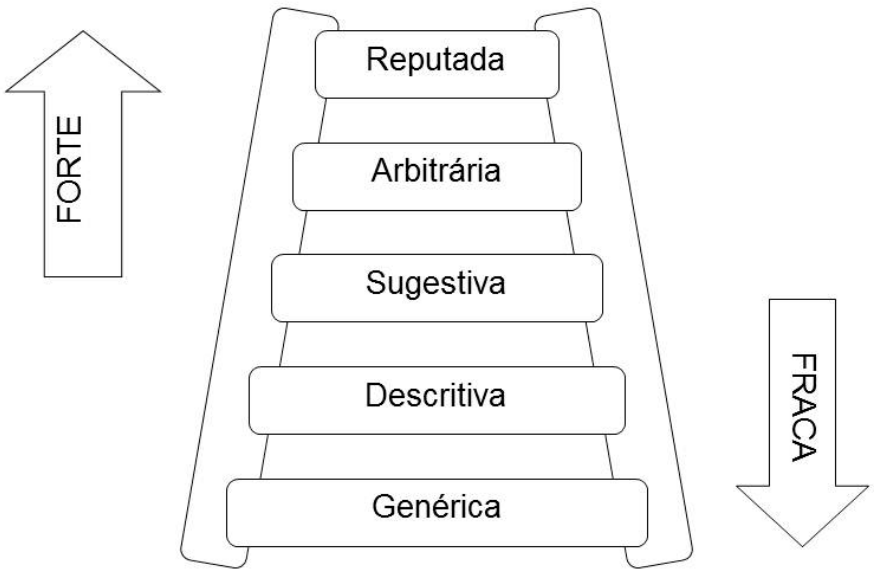
(HOTEL EM ÉVORA)

AQUISIÇÃO DE SIGNIFICADO SECUNDÁRIO

(INSTITUIÇÃO BANCÁRIA CAIXA GERAL DE DEPÓSITOS)

GENÉRICO (DESIGNAÇÃO USUAL)

- "ASPIRINA" (Ácido acetilsalicílico)
- "KETCHUP" (Molho à base de tomate)
- "THERMOS" (Recipiente térmico)
- "XEROX" (Máquina fotocopiadora)



Definição de Marca

DISTINÇÃO ENTRE MARCA E OUTROS DIREITOS INDUSTRIAIS

20

MARCA VS LOGÓTIPO

- Sinal distintivo do comércio que visa distinguir produtos/serviços de uma empresa dos de outras empresas
- Função essencial: garantir a proveniência do produto/serviço ("indicação de origem")
- Deve ser aposto nos produtos e/ou serviços
- Tutela penal

- Sinal distintivo do comércio que visa distinguir entidades que operam no mercado (sociedades comerciais, estabelecimentos)
- Pode ser utilizado em locais diversos (anúncios, impressos ou correspondência)
- Tutela apenas por via contra-ordenacional

Existência Jurídica

REGISTO CONSTITUTIVO

22

REGISTO

- ✓ **Regra**: registo constitutivo do direito
- ✓ **Excepções**: marca livre (6 meses), marcas notórias (reconhecido pelos consumidores daquele tipo de produto/serviço) e marcas de prestígio (reconhecido pela generalidade dos consumidores, que a associam a uma elevada qualidade dos produtos/serviços)
- ✓ **Territorialidade**: a marca apenas é protegida no território onde o registo foi concedido
- ✓ **Especialidade**: a marca é limitada ao universo de produtos/serviços que visa assinalar e para os quais foi registada
- ✓ **Prazo**: 10 anos, perpetuamente renovável (art. 255.º)

REGISTO

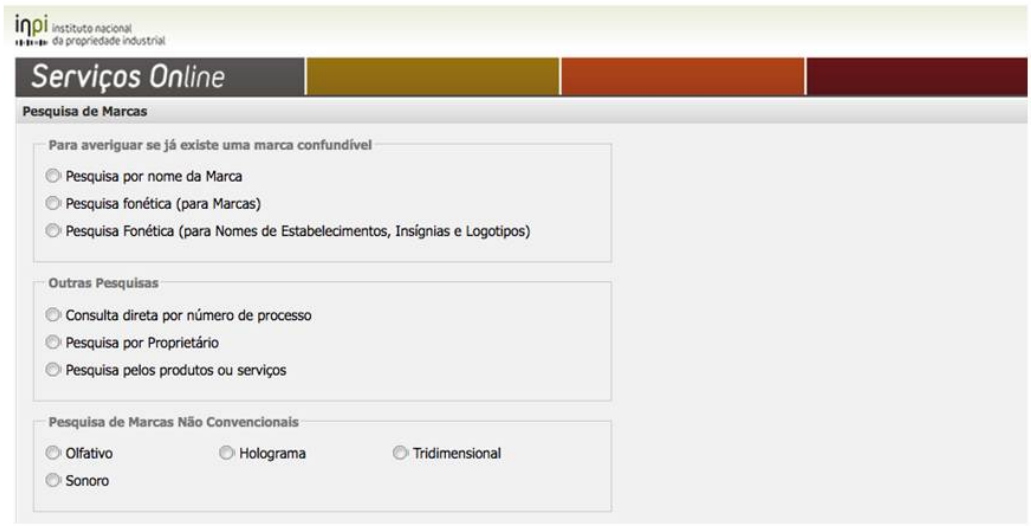
- ✓ **Vias de registo**: nacional, regional (e.g. UE) e internacional
- ✓ **Marca nacional:** vigora num país apenas
- ✓ **Marca da UE**: vigora em todos os países da UE
- ✓ "**Marca Internacional**": não existe uma marca que vigore em todos os países, mas apenas um sistema centralizado de registos, que permite a partir de um (pedido de) registo solicitar registos de marcas (nacionais) noutros países

- **Legislação**: Código de Propriedade Industrial (CPI)
- **Autoridade**: Instituto Nacional de Propriedade Industrial (INPI)
- **Exame** *ex officio* de motivos de recusa absolutos (razões de ordem pública) e relativos (direitos anteriores)

MARCA NACIONAL
VS
MARCA DA UE

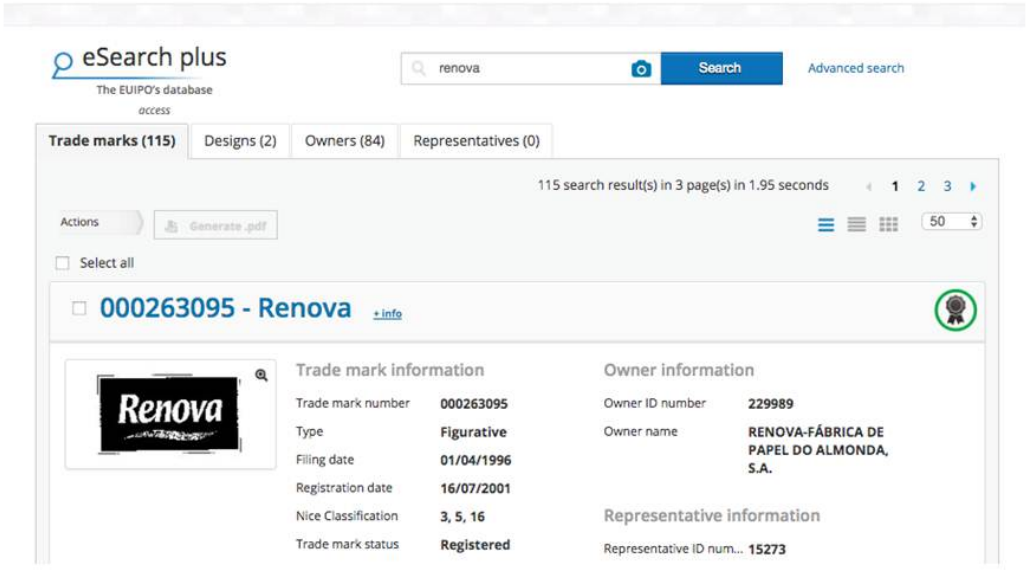
- **Legislação**: Regulamento 207/2009 de 26.02.2009 alterado pelo Regulamento 2015/2424 de 16.02.2015
- **Autoridade**: Instituto da Propriedade Intelectual da União Europeia (IPIUE, antigo IHMI ou, em inglês, OHIM)
- **Exame** não envolve *ex officio* motivos relativos de recusa

PESQUISAR



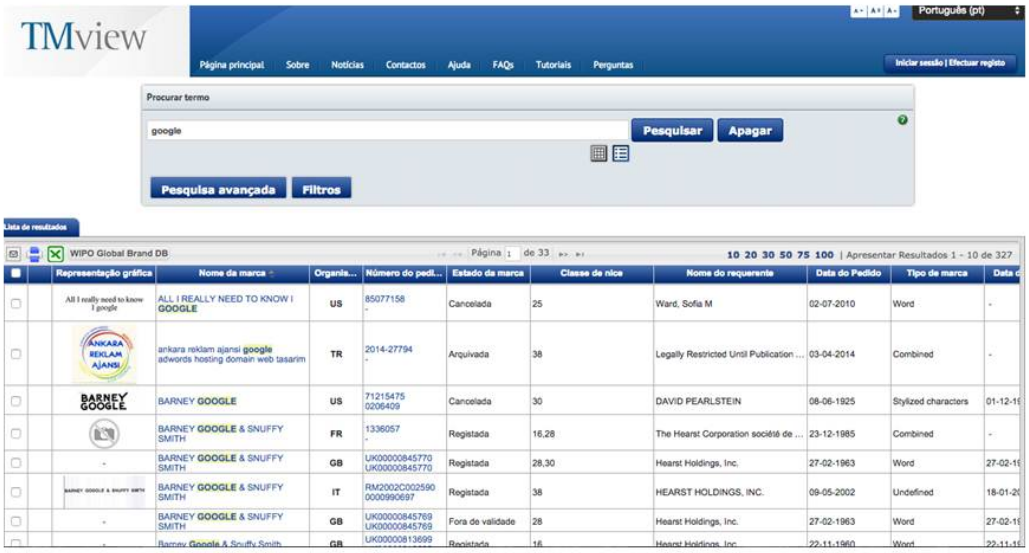
http://servicosonline.inpi.pt/pesquisas/main/marcas.jsp?lang=PT

PESQUISAR



https://euipo.europa.eu/eSearch/

PESQUISAR



https://tmdn.org/tmview

II. TUTELA PENAL DA MARCA

29

DIREITO SUBSIDIÁRIO

- ✓ **Art. 320.º CPI**: Remissão para o DL 28/84 de 20.01
- ✓ **Tentativa punível**: art. 4.º DL 28/84 (vs regra geral do art. 23.º/1 do CP: tentativa não seria punível, uma vez que os crimes que protegem as marcas não são puníveis com penas de prisão superiores a 3 anos)

CONTRAFACÇÃO, IMITAÇÃO E USO ILEGAL DE MARCA (art 323.º CPI)

É punido com pena de prisão até 3 anos ou com pena de multa até 360 dias quem, sem consentimento do titular do direito:
a) **Contrafizer**, total ou parcialmente, ou, por qualquer meio, reproduzir uma marca registada;
b) **Imitar**, no todo ou em alguma das suas partes características, uma marca registada;
c) **Usar** as marcas contrafeitas ou imitadas;
d) **Usar**, contrafizer ou imitar marcas notórias cujos registos já tenham sido requeridos em Portugal;

CONTRAFACÇÃO, IMITAÇÃO E USO ILEGAL DE MARCA (art 323.º CPI)

e) **Usar**, ainda que em produtos ou serviços sem identidade ou afinidade, marcas que constituam tradução ou sejam iguais ou semelhantes a marcas anteriores cujo registo tenha sido requerido e que gozem de prestígio em Portugal, ou na Comunidade Europeia se forem comunitárias, sempre que o uso da marca posterior procure, sem justo motivo, tirar partido indevido do carácter distintivo ou do prestígio das anteriores ou possa prejudicá-las;
f) **Usar**, nos seus produtos, serviços, estabelecimento ou empresa, uma marca registada pertencente a outrem.

CONTRAFACÇÃO, IMITAÇÃO E USO ILEGAL DE MARCA (art 323.º CPI)

- ✓ **Bem jurídico protegido**: monopólio de exploração gerado pelo registo da marca (e não e.g. a confiança do consumidor)
- ✓ **Ofendido**: titular da marca e eventuais licenciados (cf. art. 32.º CPI: licenciados gozam, para todos os efeitos legais, das faculdades conferidas ao titular do direito)
- ✓ **Contrafacção**: reprodução do sinal tal qual consta do registo
- ✓ **Imitação**: conceito complexo que envolve analise de 3 requisitos – prioridade, especialidade e confusão (cf. art. 245.º CPI)
- ✓ **Uso (alíneas c) a f) do art. 323.º)**: uso do sinal que assuma a função de indicação de origem, mas com interpretação restritiva…

Conceito de Imitação (art. 245.º CPI)

PRIORIDADE

34

PRIORIDADE

- ✓ Se a marca alegadamente de imitação estiver registada, será necessário verificar qual das marcas (a imitada e a alegadamente infractora) foi registada primeiro.
- ✓ Como tivemos oportunidade de ver supra, é fácil confirmar este facto nas bases de dados oficiais de marcas.

Conceito de Imitação (art. 245.º CPI)

ESPECIALIDADE

36

PRINCÍPIO DA ESPECIALIDADE

- ✓ A classificação de Nice não é determinante para aferir se existe efectiva "afinidade" entre produtos/serviços
- ✓ **Afinidade** (TJUE, C-39/97 "Canon", de 29.09.1998), para. n.º 23): análise de todos os factores pertinentes que caracterizam a relação entre os produtos, em especial a sua natureza, destino, utilização, bem como o seu carácter concorrente ou complementar
- ✓ **Complementaridade** (TJUE, primeira instância, T-74/04, de 11.05.2011): produtos são complementares se existir uma relação estreita entre si, no sentido de que um é indispensável (essencial) ou importante (significativo) para a utilização do outro, de molde a que os consumidores possam entender que é a mesma empresa que é responsável pela sua produção. Por definição, os produtos destinados a diferentes públicos não podem ser complementares.

Conceito de Imitação (art. 245.º CPI)

CONFUNDIBILIDADE

38

CONFUNDIBILIDADE

- ✓ Existe risco de confusão entre marcas se existir a possibilidade de o público relevante considerar que os produtos/serviços provêm da mesma empresa (**confusão *stricto sensu***), ou de empresas economicamente ligadas (**confusão por associação**)
- ✓ **Juízo de confundibilidade** depende de uma apreciação global de vários factores interdependentes, e.g.: semelhança dos produtos/serviços, semelhança dos sinais, elementos distintivos e dominantes dos sinais em situação de conflito, carácter distintivo da marca anterior, público relevante
- ✓ **Público relevante**: consumidor médio atual ou potencial dos produtos/serviços em questão

CONFUNDIBILIDADE

- ✓ **Impressão global** (TJUE, C-251/95 "Sabèl", de 11/11/1997): "apreciação global deve, no que respeita à semelhança visual, fonética ou conceptual das marcas em causa, basear-se na impressão de conjunto produzida pelas marcas, atendendo, designadamente, aos elementos distintivos e dominantes destas" (para. n.º 23)
- ✓ **Exame sucessivo** (Ac. do STJ de 25.03.2004, processo n.º 03B3971): a comparação entre duas marcas deve ser feita tendo em conta que o comprador, quando compra um produto marcado com um sinal semelhante a outro que já conhecia, não tem simultaneamente as marcas sob os olhos para as comparar. Juiz não deve colocar marcas lado a lado, para exame simultâneo.

CONFUNDIBILIDADE

- ✓ Primeiro deve analisar-se cada uma das marcas para verificar o respectivo grau de distintividade e se contem elementos descritivos ou alusivos; não devem ser tomados em conta elementos destituídos de capacidade distintiva
- ✓ O **elemento fonético** deve ser considerado preponderante, uma vez que o consumidor médio normalmente refere-se a determinada marca pronunciando o seu elemento verbal (TJUE, T-312/03 "Selenium-Ace", de 14.07.2005)
- ✓ Os **inícios das palavras** assumem, em regra, maior preponderância
- ✓ Semelhança entre sinais é questão de facto, mas juízo de existência ou não de risco de confusão é **questão de direito**

Conceito de Uso

USO ABRANGIDO PELA TUTELA PENAL

42

USO ILEGAL DE MARCA

- **Função de indicação de origem:** conceito de "uso de marca" deve ser interpretado de acordo com a função essencial da marca, a função de *"garantir aos consumidores a proveniência do produto ou serviço".*
- **Uso no comércio**: "Há assim uso da marca sempre que um operador económico, na vida económica, distingue os produtos ou serviços que comercializa de outros produtos ou serviços, por meio de uma marca" (Oliveira Ascensão).
- Princípio da **especialidade**: o uso aludido deve ocorrer no âmbito do princípio da especialidade, porquanto é este que determina o âmbito da tutela da marca.
- No que toca a **marcas de prestígio**, não se aplica o princípio da especialidade. Tal ocorre com vista a tutelar o especial valor simbólico destas marcas, a sua especial força atractiva. Nestes termos, o uso criminalmente punível nesta sede é mais lata.
- Usar uma marca verbal ou o elemento verbal de uma marca mista, como **nome de domínio**, constitui "uso de marca contrafeita ou imitada [al. c)]? Sim, se tal nome de domínio server para indicar a origem dos produtos enunciados no respectivo *site*.

VENDA, CIRCULAÇÃO OU OCULTAÇÃO (art 324.º CPI)

É punido com pena de prisão até 1 ano ou com pena de multa até 120 dias quem vender, puser em circulação ou ocultar produtos contrafeitos, por qualquer dos modos e nas condições referidas nos artigos 321.º a 323.º, com conhecimento dessa situação.

VENDA, CIRCULAÇÃO OU OCULTAÇÃO (art 324.º CPI)

- ✓ **Bem jurídico protegido**: monopólio de exploração gerado pelo registo da marca (e não e.g. a confiança do consumidor)
- ✓ **Ofendido**: titular da marca e eventuais licenciados (cf. art. 32.º CPI: licenciados gozam, para todos os efeitos legais, das faculdades conferidas ao titular do direito)
- ✓ **Actos de comercialização** de produtos contendo marcas que reproduzam, imitem ou usem marca alheia, em concreto, vender, pôr em circulação ou ocultar os respectivos produtos
- ✓ **Relação com art. 323.º : tutela antecipada**, uma espécie de crime de perigo abstracto, pois consome-se independentemente de se verificar a efectiva comercialização dos produtos?

VENDA, CIRCULAÇÃO OU OCULTAÇÃO (art 324.º CPI)

- ✓ Cremos que existe uma relação de **concurso aparente** entre os crimes do art. 323.º e 324.º atenta a identidade do bem jurídico
- ✓ Ac. do TRL de 13-11-2014, processo n.º 7912/12.7TDLSB, Rel. Calheiros da Gama: importação, após aquisição no site EBAY, de, pelo menos 10 comandos para PS3 da Sony, ostentando marca contrafeita. Este acórdão (sobre despacho de não pronúncia), concluiu, contrariamente à primeira instância, atenta a inverosimilhança da versão declarada pelo arguido, que existiam indícios suficientes da prática, pelo mesmo arguido, quer de um crime do art. 323.º, quer de um crime do 324.º, na forma tentada, não analisando uma eventual relação de consunção entre tais crimes.

VENDA, CIRCULAÇÃO OU OCULTAÇÃO (art 324.º CPI)

- ✓ Não está tipificada a conduta de **importação** de produtos que ostentem marcas contrafeitas, pelo que resta ao titular os mecanismos de defesa do art. 319.º CPI (retenção ou suspensão do desalfandegamento) e os instrumentos previstos em sede alfandegária, em concreto o Regulamento (CE) n.º 608/2013 (que revoga o Regulamento (CE) 1383/2003, executado pelo DL 360/2007. de 02.11) (retenção ou suspensão da autorização e saída)
- ✓ As autoridades alfandegárias impedem os produtos que ostentam marcas contrafeitas ou imitadas de entrar no mercado, pelo que a aplicabilidade do art. 324.º se vê reduzida, restando a punição deste tipo de condutas pela tentativa [punível apesar do crime não ser punível com penas de prisão superior a 3 anos atenta a remissão feita pelo art. 320.º do CPI para o DL. n.º 28/84, de 20 de Janeiro]

REGISTO OBTIDO OU MANTIDO COM ABUSO DE DIREITO (art 327.º CPI)

É punido com pena de prisão até 3 anos ou com pena de multa até 360 dias quem requerer, obtiver ou mantiver em vigor, em seu nome ou no de terceiro, **registo de marca**, de nome, de insígnia ou de logótipo que constitua reprodução ou imitação de marca ou nome comercial pertencentes a nacional de qualquer país da União, independentemente de, no nosso país, gozar da prioridade estabelecida no artigo 12.º, com a finalidade comprovada de constranger essa pessoa a uma disposição patrimonial que acarrete para ela um prejuízo ou para dela obter uma ilegítima vantagem económica.

III. CAUSAS DE EXCLUSÃO DA ILICITUDE

49

CAUSAS DE EXCLUSÃO DA ILICITUDE ESPECÍFICAS DAS MARCAS

- **Limitações aos direitos de exclusivo sobre marcas (art. 260.º CPI)**:

  Os direitos conferidos pelo registo da marca não permitem ao seu titular impedir terceiros de usar, na sua actividade económica, desde que tal seja feito em conformidade com as **normas e os usos honestos** em matéria industrial e comercial:

  a) O seu próprio nome e endereço;

  b) Indicações relativas à espécie, à qualidade, à quantidade, ao destino, ao valor, à proveniência geográfica, à época e meio de produção do produto ou da prestação do serviço ou a outras características dos produtos ou serviços;

  c) A marca, sempre que tal seja necessário para indicar o destino de um produto ou serviço, nomeadamente sob a forma de acessórios ou peças sobressalentes.

CAUSAS DE EXCLUSÃO DA ILICITUDE ESPECÍFICAS DAS MARCAS

- ✓ **Limitações (excepções) aos direitos de exclusivo sobre marcas (art. 260.º CPI)**: possibilidade de alegação em sede de contestação crime

E ainda…

- ✓ **Falta de distintividade ou outra causa de nulidade do registo (art. 223.º CPI)**: poderá ser alegada em sede de contestação crime ou carecerá de declaração prévia de nulidade pelo TPI? (propendemos para esta segunda alternativa, atenta a natureza absoluta do direito)
- ✓ **Uso privado**: uso da marca de prestígio "Boeing" num iate privado não integra o crime p.p. art. 323.º/1 c) e d), pois não é um uso que assuma a função de indicação de origem no mercado

Obrigado

Alexandre Au-Yong Oliveira
Juiz de Direito, Formador do CEJ
CEJ - Porto, 3 de Fevereiro de 2017

Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/ytly46cui/flash.html?locale=pt

CENTRO
DE ESTUDOS
JUDICIÁRIOS

3.

A recolha de prova digital através de pesquisas informáticas transfronteiriças

David Silva Ramalho

CENTRO
DE ESTUDOS
JUDICIÁRIOS

A RECOLHA DE PROVA DIGITAL ATRAVÉS DE PESQUISAS INFORMÁTICAS TRANSFRONTEIRIÇAS*

David Silva Ramalho**

1. O problema

Pense-se numa busca. Uma busca regularmente realizada ao local de trabalho de um suspeito da prática de um qualquer crime grave. No despacho do Ministério Público pode ler-se «[t]endo em conta que alguns dos elementos a apreender no decurso das buscas autorizadas podem estar contidos e armazenados em sistemas informáticos (computadores), designadamente em ficheiros de texto, bases de dados, registos de acesso e em gravações em formato vídeo e áudio, ordena-se, nos termos do disposto no n.º 1 do artigo 15º da Lei n.º 109/2009, de 15 de Setembro (Lei do Cibercrime), a pesquisa nos sistemas informáticos que venham a ser encontrados nos locais a buscar».

Assim sucede. Uma vez iniciada a pesquisa informática no computador do suspeito, percebe-se que existe muito pouca informação com relevo probatório, excepto alguns elementos que indiciam que a informação relevante há-de estar algures na *cloud*. Consultados os *Favoritos* do navegador de Internet do computador pesquisado, constata-se que aí se encontra, de facto, o *link* para um serviço de armazenamento de informação baseado na *cloud*. Ao seleccionar o *link*, percebe-se que as credenciais de acesso estão memorizadas e que, por isso, basta clicar na opção *sign in* para se poder ter acesso à informação pretendida.

O Ministério Público prepara-se para autorizar a extensão da pesquisa à conta do utilizador nessa *cloud*, ao abrigo do disposto no artigo 15.º, n.º 5, da Lei do Cibercrime, quando se apercebe que o fornecedor de serviços de armazenamento tem a sua sede na Alemanha e todos os seus servidores na Holanda, Bélgica e Irlanda. Pergunta-se: poderá clicar legitimamente na opção *sign in* para aceder e apreender[1] a informação armazenada noutro

* O presente texto corresponde, no essencial, à minha intervenção oral na acção de formação contínua sobre "Temas de Direito Penal e Processual Penal", organizada pelo Centro de Estudos Judiciários, que teve lugar no dia 9 de Março de 2018, no Tribunal da Relação do Porto. O texto conserva, por isso, o registo de oralidade que esteve na sua génese, bem como o seu propósito essencialmente expositivo.

** Assistente Convidado da Faculdade de Direito da Universidade de Lisboa, investigador do Centro de Investigação de Direito Penal e Ciências Criminais e Advogado na Morais Leitão, Galvão Teles, Soares da Silva & Associados – Sociedade de Advogados, SP, RL..

[1] De acordo com o disposto no artigo 16.º, n.º 7, da Lei do Cibercrime, a apreensão de dados informáticos poderá, consoante seja mais adequado e proporcional, revestir uma das seguintes formas: «a) Apreensão do suporte onde

Estado? Ou será que essa pesquisa e apreensão se lhe encontra vedada, sob pena de violação da soberania do Estado pesquisado, devendo por isso recorrer-se obrigatoriamente aos mecanismos de cooperação judiciária disponíveis? E se a informação pesquisada estiver, porventura, na *Dark Web*, sem que seja possível identificar o concreto Estado onde está armazenada? E se estiver armazenada em diferentes Estados em simultâneo, seja replicada, seja fragmentada? A questão não é de resolução fácil.

Com efeito, o problema do acesso transfronteiriço a prova digital vem sendo objecto de controvérsia há já pelo menos 3 décadas ([2]), quando a sua relevância era ainda diminuta, e não se antecipa que se venha a alcançar num futuro próximo uma solução satisfatória e consensual no plano internacional. Contudo, com a disseminação dos serviços de computação em nuvem e a deslocalização da informação, os obstáculos jurídicos à investigação criminal que daqui decorrem ganham um relevo muito prático e que, em certos casos, podem levar ao bloqueio da investigação criminal.

O problema jurídico-internacional tem sido, porém, desconsiderado em vários Estados pela prática judiciária, em prol de um conjunto de argumentos de natureza fundamentalmente pragmática que se prendem essencialmente com:

(i) A percepção da reduzida relevância da violação de soberania decorrente deste tipo de pesquisas e apreensões no contexto de processos-crime;

(ii) A volatilidade da prova, especialmente tendo em consideração a possibilidade de o arguido, ou alguém a seu pedido, poder eliminá-la a partir de qualquer sistema informático seu enquanto os mecanismos de cooperação judiciária são desencadeados;

(iii) A lentidão dos mecanismos de cooperação judiciária;

(iv) A ideia de que a Internet é um espaço sem fronteiras;

(v) A impossibilidade, em certos casos, de se descobrir o local onde a prova se encontra armazenada (o problema da *loss of location*) ou

(vi) A ideia de que, estando em causa a violação de normas que regulam relações entre Estados e que não visam conferir específicos direitos aos cidadãos na sua relação com o

está instalado o sistema ou apreensão do suporte onde estão armazenados os dados informáticos, bem como dos dispositivos necessários à respectiva leitura; b) Realização de uma cópia dos dados, em suporte autónomo, que será junto ao processo; c) Preservação, por meios tecnológicos, da integridade dos dados, sem realização de cópia nem remoção dos mesmos; ou d) Eliminação não reversível ou bloqueio do acesso aos dados».

[2] O tema foi suscitado, ainda que em termos genéricos, na Recomendação n.º R(89)9 do Comité de Ministros do Conselho da Europa, de 13 de Setembro de 1989, e complementada, com maior detalhe, pelo relatório sobre criminalidade informática do Comité Europeu para os Problemas Criminais, de 1990. Apesar de neste relatório se abordar já expressamente o problema da "penetração directa" em sistemas informáticos localizados no estrangeiro e de se incluírem algumas condições para a sua eventual admissibilidade a título excepcional, o Comité concluiu que a questão não se encontrava suficientemente amadurecida pelo que não seria altura de avançar uma proposta sobre a matéria - Conselho da Europa, *Computer-related crime* (prefácio de August Bequai), Estrasburgo: Council of Europe Publishing and Documentation Service, 1990, pp. 86-89.

Estado, as únicas consequências negativas que daí possam advir serão no plano supranacional e não no da invalidade da prova[3].

Por vezes a prática judiciária de aceder irrestritamente a prova armazenada no estrangeiro encontra inclusivamente esteio em disposições legais de origem nacional que, sem especial preocupação com os limites da sua jurisdição, admitem, de forma mais ou menos expressa, a extensão das pesquisas informáticas a outros territórios.

A solução assim adoptada por alguns legisladores nacionais parte do pressuposto que a mera existência de norma legal habilitante torna inconsequente, pelo menos no imediatismo do plano probatório e da respectiva validade, a violação de direito internacional. Esta solução é, todavia, um mero *remendo* para um problema mais grave, cuja solução deverá assentar num debate aberto e descomplexado quanto à eventual inaptidão do quadro jurídico vigente para fazer face a uma realidade que já não é nova mas que permanece presa às amarras da analogia com o que já não é analógico, por ser digital.

2. A Convenção sobre o Cibercrime

O Conselho da Europa procurou integrar na Convenção sobre o Cibercrime os termos em que o acesso transfronteiriço seria consensualmente admitido pelos seus membros.

Começou, porém, por assinalar que a Convenção não tornaria possível, por si só, qualquer intromissão na soberania nacional dos Estados-signatários no decurso de investigações criminais de cariz nacional, assim delimitando geograficamente, salvo disposição legal (tendencialmente) supranacional que dispusesse em sentido contrário[4], a aplicação das medidas processuais previstas na sua Secção 2, aos dados trocados, enviados ou armazenados no mesmo território em que decorre a investigação.

Deste modo, a limitação territorial do acesso a dados informáticos foi expressamente referida a propósito, não só da busca e apreensão de dados informáticos armazenados (artigo 19.º), mas também da injunção de comunicar (artigo 18.º), da recolha, em tempo real de dados de tráfego (artigo 20.º) e da intercepção de dados de conteúdo (artigo 21.º).

Apenas o acesso transfronteiriço a dados armazenados veio a merecer consagração expressa na Convenção, e não o acesso a — leia-se, a recolha ou intercepção de — dados de tráfego ou

[3] Nesse sentido, referiu recentemente o *Transborder Group*, junto do Conselho da Europa, o seguinte: «*As noted by the T-CY previously, given these limitations and in the absence of a clear, efficient and feasible international legal framework, governments increasingly pursue unilateral solutions in practice. It seems to be widespread practice that law enforcement in a specific criminal investigation access data not only on the device of the suspect but also on connected devices such as email or other cloud service accounts if the device is open or the access credentials have been obtained lawfully even if they know that they are connecting to a different, known country*» - COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), *Criminal Justice Access to electronic evidence in the cloud: Recommendations for consideration by the T-CY*, Estrasburgo: Conselho da Europa, Setembro de 2016, disponível em https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

[4] Dado que o objectivo da Convenção é também completar e não substituir quaisquer tratados e acordos bilaterais e multilaterais celebrados entre as Partes, é permitida a estipulação de norma em sentido contrário, a qual, naturalmente, terá um âmbito de aplicação limitado aos seus signatários — cf. artigo 39.º da Convenção e parágrafos 293, 308 e 309 do Relatório Explicativo da Convenção sobre o Cibercrime.

de conteúdo em tempo real, em relação aos quais a regra expressamente consagrada foi, sem excepções, a do recurso à cooperação internacional (cf. artigos 33.º e 34.º da Convenção). Facto que é, aliás, facilmente compreensível, tendo em conta que, se o consenso para a apreensão de dados armazenados apenas foi conseguido em situações absolutamente excepcionais, então qualquer consenso sobre a realização de intercepções transfronteiriças seria, naturalmente, inalcançável[5].

Assim, refere-se no parágrafo 195 do Relatório Justificativo da Convenção sobre o Cibercrime que o artigo 19.º, dedicado à *busca e apreensão de dados informáticos armazenados*, «não aborda a "busca e apreensão transfronteiriça" que confere aos Estados a possibilidade de busca e apreensão de dados no seio do território de outras Partes, sem que seja necessário recorrer às modalidades tradicionais de assistência jurídica mútua», uma vez que este meio de obtenção de prova se encontra regulado no capítulo da cooperação internacional. Duas excepções a esta regra são, porém, contempladas no artigo 32.º da Convenção, a saber:

> (i) Quando os dados forem publicamente acessíveis, ou,
>
> (ii) Se os dados se encontrarem armazenados no território de uma outra Parte da Convenção, quando for obtido o consentimento legal e voluntário da pessoa com legitimidade para divulgar os dados através desse sistema informático.

Nesta matéria, como se refere no parágrafo 293 do Relatório Justificativo da Convenção, «[f]oram examinadas em pormenor todas as situações nas quais se considera admissível que os Estados actuem de forma unilateral, bem como as situações nas quais tal não será aceitável» até que "[o]s redactores chegaram […] à conclusão de que, nesta fase, não seria ainda possível elaborar um regime global, legalmente vinculativo, que regulamentasse esta matéria», devido «em parte, à inexistência, até à data, de uma experiência objectiva relativamente a este tipo de situações, ao que se acrescenta o facto de se considerar que a resolução adequada está, frequentemente, ligada à conjuntura do caso em concreto, pelo que se torna difícil estipular regras gerais», pelo que, em conclusão, «os redactores decidiram que apenas seriam definidas, ao abrigo do artigo 32.º da Convenção, as situações nas quais, por unanimidade, a acção unilateral se mostrasse aceitável».

A regra geral configurada na Convenção é, então, a do recurso à cooperação internacional, sempre que os dados estejam armazenados em território estrangeiro, salvo acordo supranacional em sentido diferente, entre os Estados envolvidos, e exceptuando os dois casos que se analisarão de seguida.

Todavia, por força da tendencial lentidão dos mecanismos de cooperação internacional tradicionais, especialmente agravada em virtude do carácter altamente volátil da prova digital, o Conselho da Europa, inspirado na rede de pontos de contacto estabelecida em 1998, por

[5] Assim, PAUL DE HERT, «Cybercrime and jurisdiction in Belgium and the Netherlands. Lotus in cyberspace — whose sovereignty is at stake?», em *Cybercrime and Jurisdiction* (ed. Susan Brenner/Bert-Jaap Koops), Haia: T.M.C. Asser Press, 2006 , p. 83.

iniciativa do G8, criou a Rede 24/7[6], composta por pontos de contacto, em cada Parte, disponíveis vinte e quatro horas por dia, sete dias por semana, a fim de assegurar de imediato a prestação de auxílio nas investigações e nos procedimentos relativos a infracções penais relacionadas com sistemas informáticos, ou na recolha de provas sob a forma electrónica, da prática de infracções penais[7].

2.1. O acesso transfronteiriço a dados publicamente acessíveis

Dispõe o artigo 32.º, alínea *a)*, da Convenção sobre o Cibercrime, que uma Parte pode, sem autorização de uma outra Parte, «aceder a dados informáticos acessíveis ao público (fonte aberta), independentemente da sua localização geográfica». Assim, sempre que seja necessário recolher dados[8] num *website* ao qual o público pode ter acesso, ainda que mediante subscrição ou registo prévio[9] — pense-se numa rede social[10], num *blog*, ou mesmo numa pasta *Dropbox* acessível através de um *link* público[11] —, podem as autoridades fazê-lo sem necessidade de recurso aos mecanismos de cooperação internacional, procedendo ao *download* dos documentos relevantes ou mesmo realizando *screenshots* da página em questão[12].

---

[6] A Rede viria a ser alargada ao contexto da União Europeia por via da Decisão-Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro de 2005, relativa a ataques contra sistemas de informação — cf. PEDRO VERDELHO, *The effectiveness of international co-operation against cybercrime: examples of good practice,* 2008, Conselho da Europa, pp. 15, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf.

[7] Referindo-se essencialmente a actos de espionagem mas com relevo para esta matéria, refere JOHANN-CHRISTOPH WOLTAG o seguinte: «[i]*f these operations are undertaken by merely accessing publicly available data, the performing State does not substitute the target State's sovereignty on its own. Consequently only those operations that access data not readily available to a foreign State can be considered in their effects to be infringe on the target State's sovereignty and political independence*» — CHRISTOPH WOLTAG, *Cyber Warfare — Military Cross-Border Computer Network Operations under International Law*, Cambridge: Intersentia, 2014, p. 127.

[8] A circunstância de o artigo 32.º, n.º 1, alínea a), da Convenção sobre o Cibercrime falar em "acesso" e não em "aceder a, ou receber", como faz a alínea b), poderia indicar que aquele acesso não permitiria uma apreensão de prova. A distinção parece, porém, ser inconsequente, permitindo também a apreensão da prova. Assim, cf. o excelente e incontornável artigo de ULRICH SIEBER / CARL-WENDELIN NEUBERT, «Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty», em *Max Planck Yearbook of United Nations Law* (ed. Frauke Lachenmann et al.), Vol. 20, Leiden | Boston: Brill, Nijhoff, 2016, pp. 267-268.

[9] Assim, cf. a recente obra incontornável de ULRICH SIEBER / CARL-WENDELIN NEUBERT, «Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty», em *Max Planck Yearbook of United Nations Law* (ed. Frauke Lachenmann et al.), Vol. 20, Leiden | Boston: Brill, Nijhoff, 2016, pp. 267-268 e COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), *T-CY Guidance Note #3 — Transborder access to Data (Article 32)*, Estrasburgo: Conselho da Europa, p. 4., disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY(2013)7REV_GN3_transborder_V11.pdf.

[10] Nesse sentido, veja-se o recente acórdão do Tribunal da Relação do Porto, de 5 de Abril de 2017, Proc. 671/14: «A recolha ou cópia de informação que alguém disponibiliza ou publicita no seu mural de Facebook sem restrição de acesso, não impede a sua utilização como prova para efeitos de procedimento criminal. Deste modo, a utilização da cópia da publicação pela qual o arguido divulgou factos pouco abonatórios e falsos no mural do Facebook sobre a conduta dos assistentes no âmbito da parceria de trabalho que tinham em Angola, sem restrição de acesso, constitui prova perfeitamente válida».

[11] Cf. BERT-JAAP KOOPS / MORAG GOODWIN, *Cyberspace, the cloud and cross-border criminal investigation – The limits and possibilities of international law*, Tilburg: Universiteit van Tilburg, 2014, p.53.

[12] Cf. PEDRO VERDELHO, *The effectiveness of international co-operation against cybercrime: examples of good practice*, cit., pp. 12-15, e CRISTOS VELASCO SAN MARTÍN, *La jurisdicción y competencia sobre delitos cometidos a través de sistemas de cómputo e internet*, Valencia: Tirant lo blanch, 2012, pp. 155-160.

Trata-se, porém, de uma permissão cuja ausência tende a ser considerada como relativamente inócua tendo em conta que já se encontraria a coberto de um costume internacional[13], em virtude de se tratar de uma prática geral (*consuetudo*), considerada juridicamente vinculativa (*opinio iuris sive necessitatis*)[14].

2.2. O acesso transfronteiriço a dados informáticos com o consentimento da pessoa legalmente autorizada

Por outro lado, consta do artigo 32.º, alínea b), da Convenção sobre o Cibercrime que «[u]ma Parte pode, sem autorização de uma outra Parte […] [a]través de um sistema informático situado no seu território, aceder a dados informáticos no território de uma outra Parte, ou recebê-los, se obtiver o consentimento legal e voluntário da pessoa com legitimidade para lhe divulgar os dados através desse sistema informático».

A primeira questão que cumpre clarificar prende-se com o significado de *pessoa com legitimidade para divulgar os dados*, cujo significado poderá variar em função da legislação de cada Estado-signatário. Nesta matéria, esclarece o Relatório Justificativo da Convenção sobre o Cibercrime, no parágrafo 294, que «a pessoa "legalmente autorizada" a divulgar os dados poderá variar em função das circunstâncias, da natureza jurídica da pessoa e da respectiva legislação aplicável», avançando o seguinte exemplo, «uma mensagem de correio electrónico de uma dada pessoa poderá ser armazenada num outro país por um fornecedor de serviços, ou a pessoa poderá intencionalmente armazenar os dados num outro país. Estas pessoas poderão, assim, recuperar os dados e, visto que dispõem de uma autoridade legal, proceder voluntariamente à divulgação dos dados junto dos serviços competentes para a aplicação da lei, ou permitir a estes últimos o acesso aos dados em conformidade com as disposições contidas neste artigo»[15].

A segunda questão a dirimir prende-se com o conceito de *consentimento legal e voluntário*. Nesta matéria, cabe não esquecer que, não só a pessoa legalmente autorizada a divulgar os dados tem de querer, livremente, facultar o acesso aos mesmos, como, no momento em que

[13] Sendo certo que existem algumas vozes que tendem a atribuir relevo apenas ao critério do local de armazenamento, sem distinção quanto à eventual publicidade dos dados. Assim, de acordo com a opinião do Conselho de Estado da Bélgica, «*most of the member States tend to consider a cross-border search on the web carried out by the competent authorities entrusted with the inquiry without the authorization of the competent authorities to be a violation of their sovereignty and of international law*» — cf. PAUL DE HERT / GERTJAN BOULET, «Report for Belgiu»", *Révue Internationale de Droit Pénale*, Ano 84 (1.º e 2.º trimestres de 2013), p. 36 e BERT-JAAP KOOPS, "Police investigations in Internet open sources: Procedural-law issues, *Computer Law & Security Review*, n.º 29 (2013), p. 658.

[14] Assim, NICOLAI SEITZ, «Transborder Search: a new perspective in law enforcement?», *Yale Journal of Law and Technology*, Vol. 7 (2005), p. 38, e, SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), *Transborder access and Jurisdiction: What are the options?*, Conselho da Europa, 2012, disponível em http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TCY_2012_3_transborder_rep_V30public_7Dec12.pdf, p. 20. Nesta matéria, na doutrina portuguesa, cf. BENJAMIM SILVA RODRIGUES, *Da Prova Penal — Tomo IV — Da Prova -Electrónico- Digital e da Criminalidade Informático-Digital* (com prefácio de Catarina dos Santos Gomes), Lisboa: Rei dos Livros, 2011, p. 376 e PEDRO VERDELHO et al., *Leis do Cibercrime — Volume 1*, Lisboa: Centro Atlântico, 2003, p. 20.

[15] Cf. SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), *Transborder access and Jurisdiction: What are the options?*, cit., pp. 23-24. Para maior desenvolvimento sobre este tema, veja-se o nosso *Métodos Ocultos de Investigação Criminal em Ambiente Digital*, Coimbra: Almedina, 2017, pp. 73-75.

decide fazê-lo, tem de estar cabalmente esclarecida e informada do teor e consequências do seu consentimento[16]. A estes requisitos tem de juntar-se o da admissibilidade legal de concessão válida do consentimento, nos termos da legislação interna do Estado no qual o mesmo é prestado, designadamente em casos de menoridade ou de anomalia psíquica do visado.

A alínea *b)* do artigo 32.º, embora tenha entretanto sido praticamente replicada noutras disposições supranacionais[17], foi, e continua a ser, uma das disposições mais controversas da Convenção sobre o Cibercrime[18], por poder implicar uma cedência de soberania nacional[19], ao permitir — sem, contudo, definir procedimentos para o efeito — que um Estado execute actos processuais materialmente incidentes sobre o território de outro Estado sem recorrer aos mecanismos de auxílio mútuo[20], para que esta faculte o acesso aos dados[21].

Assim, tendo em conta que a norma em apreço é aplicável apenas às Partes da Convenção, se, por hipótese, os dados visados estiverem armazenados num sistema informático localizado num Estado que não seja Parte, ou, se for impossível descobrir a localização dos dados, o artigo 32.º, alínea b), da Convenção não será aplicável[22].

---

[16] Acerca da eventual revogabilidade deste consentimento cf. o relatório elaborado por JOSEPH J. SCHWERHA IV, *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"*, Estrasburgo: Conselho da Europa, 2010, p. 12, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/2079_reps_IF10_reps_joeschwerha1a.pdf

[17] Assim sucede com o artigo 40.º, n.º 2, da Convenção Árabe sobre o Combate a Infracções Informáticas, de 2010, ou com o artigo 49.º da Lei Modelo sobre Cibersegurança da *Common Market for Eastern and Southern Africa* (COMESA).

[18] Aliás, como se pode ver nos Relatórios da 2.ª Consulta Multilateral das Partes da Convenção sobre o Cibercrime [CM/Inf(2007)38], de 2007, na qual consta que a Federação Russa teve uma aproximação positiva à Convenção mas entendeu que teria de ser feita uma análise adicional ao artigo 32b, «*em particular à luz da experiência recolhida do uso deste artigo*» — disponível em https://wcd.coe.int/ViewDoc.jsp?id=1167033&Site=COE, acedido e consultado em 5 de Agosto de 2012 —, bem como ao Relatório da 4.ª Consulta Multilateral no qual consta que uma «*delegação de observadores fez uma declaração a expressar preocupação acerca das incertezas relativas à aplicação do artigo 32 (b) da Convenção e sugerindo que o T-CY deveria iniciar um processo que resultaria na emenda desta previsão. O T-CY não aceitou esta sugestão*» — disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/TC-Y_2009_06.pdf, acedido e consultado em 5 de Agosto de 2012. Sobre este assunto cf. MICHEÁL O'FLOINN, «It wasn't all white light before Prism: Law enforcement practices in gathering data abroad, and proposals for further transnational access at the Council of Europe», *Computer Law & Security Review*, n.º 29 (2013), p. 611.

[19] Cf. MARCO GERCKE, «10 years Convention on Cybercrime», *Computer Law Review International*, Vol. 5/2011 (Outubro de 2011), p. 149, e *Understanding Cybercrime: A Guide for Developing Countries*, Genebra: ITU, 2011, pp. 277-278.

[20] Foi, aliás, em grande medida, devido a esta norma que a Rússia, apesar de ser membro do Conselho da Europa, se recusa, até à data, a assinar a Convenção sobre o Cibercrime, porquanto, no seu entendimento, o artigo 32.º, alínea b), «poderia danificar a soberania e a segurança dos Estados membros e os direitos dos seus cidadãos» — cf. CNEWS (2008), «Putin defies Convention on Cybercrime», 27 de Março, disponível em http://eng.cnews.ru/news/top/indexEn.shtml?2008/03/27/293913.

[21] Há, inclusivamente, quem questione a admissibilidade jurídica da criação desta excepção, alegando para tal que a soberania nacional de um Estado não está à disposição de um indivíduo — sobre esta matéria, cf. NICOLAI SEITZ, «Transborder Search: a new perspective in law enforcement?», cit., p. 40.

[22] A menos que, como refere NICOLAI SEITZ, também aqui possamos reconhecer, quanto à procura do consentimento da pessoa legalmente autorizada, a existência de um costume internacional que permita estender esta excepção a Estados não-signatários da Convenção — *Idem,* p. 45. Cabe, porém, sublinhar, que, o facto de não se aplicar esta disposição da Convenção, não impede que a medida tenha lugar relativamente a outros Estados, mas antes significa que não será este o supedâneo jurídico habilitante dessa medida.

3. Possíveis vias de solução

A admissibilidade da realização de pesquisas informáticas transfronteiriças sem suporte em instrumentos jurídicos de cariz supranacional tem sido amplamente discutida na doutrina, sem que se tenha, até à data, encontrado uma solução que satisfaça simultaneamente, por um lado, os interesses dos Estados em perseguir eficazmente os agentes da prática de crimes cujo suporte probatório se encontre em ambiente digital e, por outro, os interesses dos Estados *pesquisados* em não sofrerem ingerências directas em sistemas informáticos localizados nos seus territórios, sem suporte jurídico internacional.

As soluções têm sido procuradas, naturalmente, em três frentes:

– A primeira, o direito vigente dos tratados, a jurisprudência internacional e as excepções comummente admitidas às ingerências na soberania de outros Estados;

– A segunda, na eventual formação de um costume internacional que permita legitimar este meio de obtenção de prova;

– A terceira, na eventual criação de um protocolo adicional à Convenção sobre o Cibercrime que permita alargar aos seus signatários uma nova permissão de acesso.

No plano do direito internacional vigente, entendem SIEBER e NEUBERT que a única solução juridicamente sustentável, no contexto da investigação criminal, que permitiria excepcionar a necessidade de cumprimento da obrigação de não ingerência na soberania de outros Estados seria o caso em que a pesquisa transfronteiriça respeitasse a um Estado desconhecido pelo Estado actuante e fosse necessária a salvaguardar um interesse essencial contra um perigo grave e iminente. Entre esses interesses, entendem os Autores, pode encontrar-se o de garantir o exercício efectivo da jurisdição executiva contra criminosos que afectem o seu território. Não se trata aqui, naturalmente, de garantir o exercício da jurisdição executiva em casos isolados ou perante qualquer tipo de crimes, mas sim de permitir um funcionamento continuado do sistema de aplicação coerciva do direito, enquanto serviço essencial do Estado, em relação a certo tipo de crimes cuja gravidade o justifique e em circunstâncias particularmente exigentes. Uma vez identificado um interesse essencial, será necessário verificar se o mesmo enfrenta um perigo grave e iminente, o que, de acordo com os Autores, depende da circunstância de a impossibilidade de identificação do local onde se encontra a prova impedir as autoridades de executar qualquer investigação em ambiente digital em relação a áreas importantes da criminalidade. Subjacente a esta ideia está a criação de *paraísos digitais do crime*, para onde os agentes do crime se deslocariam impunemente, perante o olhar impotente do Estado, que se veria colocado perante uma «impossibilidade sistemática de investigar o crime relacionado com a Internet»[23].

[23] Cf. ULRICH SIEBER / CARL-WENDELIN NEUBERT, «Transnational Criminal Investigations in Cyberspace: Challenges to National Sovereignty», cit., pp. 296-302.

Mesmo nestes casos, porém, seria necessário que o meio utilizado fosse o *único* apto a proteger o interesse essencial contra o perigo grave e iminente. Daqui retiram os autores uma consequência relevante nos casos de impossibilidade (ou extrema dificuldade, quando aplicadas todas as medidas razoavelmente exigíveis, dentro dos constrangimentos de recursos e tempo existentes) de identificação do local onde se encontra a prova: é que se for possível, através do acesso transfronteiriço, identificar a localização dos dados informáticos pesquisados, então deverá o Estado actuante notificar o Estados pesquisado do acesso, requerendo a obtenção da prova através dos canais existentes em matéria de cooperação internacional. Em caso de recusa por parte do Estado pesquisado, os dados deveriam ser imediatamente eliminados pelo Estado actuante. Será apenas no caso de não ser possível, de todo, mesmo após aceder à informação visada, identificar o Estado onde a mesma se encontra armazenada, que o Estado actuante poderá copiá-la e utilizá-la em processo penal[24].

As dificuldades que esta interpretação do regime vigente gera para a investigação criminal em ambiente digital tem levado certa doutrina a procurar identificar lugares paralelos no direito internacional que outrora tenham justificado a criação de excepções à impossibilidade de ingerência em território estrangeiro. O objectivo é o de, por essa via, procurar descortinar se os fundamentos que levaram à gradual permissividade dos Estados perante ingerências pouco relevantes na sua soberania poderão alargar-se a casos como os da pesquisa transfronteiriça de dados informáticos[25].

Assim, KOOPS e GOODWIN começam por explorar a possibilidade de o ciberespaço poder configurar património comum da Humanidade, à semelhança do que prescreve a Convenção das Nações Unidas sobre Direito do Mar e o Acordo Relativo à Aplicação da Parte XI da mesma Convenção a propósito do leito do mar, dos fundos marinhos e oceânicos e do seu subsolo que se situam para além dos limites da jurisdição nacional. A comparação é ainda alargada ao regime constante do Tratado sobre os Princípios Que Regem as Actividades dos Estados na Exploração e Utilização do Espaço Exterior, Incluindo a Lua e Outros Corpos Celestes, assinado em Washington, Londres e Moscovo em 27 de Janeiro de 1967, comparando o ciberespaço ao espaço exterior. A comparação, que serve como mero exercício introdutório, é rapidamente abandonada pelos Autores, na medida em que a generalidade dos Estados pretende, evidentemente, reclamar soberania sobre os sistemas informáticos que se localizem no seu território[26].

Os Autores prosseguem a sua análise, convocando, já não o regime do património da Humanidade, mas sim o da *navegação* em alto mar. Referem que, apesar de o alto mar não se

[24] *Idem*, pp. 303-307.
[25] «*A critical approach to international law, as espoused by David Kennedy and Martti Koskenniemi among others, is that international law is permanently caught in the need to compromise between the positivist (i.e., that law is the outcome of an authoritative process, regardless of its content) and naturalist (i.e., that law is only law if it is both made in the right (authoritative) process and speaks to some broader goal of the international order, such as justice or fairness) traditions of law. What this means is that international law has to make a claim to being something more than simply state interests – otherwise it is just brute power; yet at the same time it needs to reflect the actual practice of states – otherwise it is just wishful thinking*» - BERT-JAAP KOOPS / MORAG GOODWIN, *Cyberspace, the cloud and cross-border criminal investigation – The limits and possibilities of international law*, cit., p. 65.
[26] *Idem*, pp. 67-68.

encontrar sujeito a qualquer reivindicação territorial, o mesmo não sucede com os navios que dele fazem uso, os quais se encontrarão sujeitos à jurisdição do país da sua bandeira.

Entre as limitações à liberdade de navegação encontram-se um conjunto de cenários contemplados pelo direito consuetudinário internacional, que incluem:

(i) O envolvimento dos barcos em actos de pirataria;

(ii) O tráfico de pessoas;

(iii) Ameaças ao Estado (que incluem actos de terrorismo e tráfico de droga) e

(iv) Casos de perseguição em curso (*hot pursuit*), ou seja, casos em que um navio persegue outro desde águas territoriais até ao alto mar. A ideia explorada pelos autores seria a de comparar a *cloud* ao alto mar e os fornecedores de serviços a navios, abrangidos pela jurisdição do seu país, mas sujeitos a *abordagens* decorrentes de excepções análogas às que acima se identificaram[27].

Por fim, os Autores referem-se ao caso da aquisição remota de imagens por teledetecção, através de satélite. A ideia é a de que também na década de 60 a utilização de satélites para recolha remota de imagens era vista por alguns como uma ingerência na soberania dos Estados, para o que seria necessária a sua autorização. O que torna esta comparação especialmente interessante é o facto de, à semelhança do que se refere quanto às pesquisas transfronteiriças, também a recolha de imagens implicava um grau de ingerência mensurável nos Estados. Ao passo que as pesquisas transfronteiriças despoletam reacções físicas, ainda que insignificantes, em sistemas informáticos localizados noutros Estados, a recolha de imagens por satélite implicava a emissão de radiação para identificar o relevo do terreno. Esta concepção viria a ser afastada pela criação do princípio céu aberto, que previa, em termos sumários, a liberdade de recolher e distribuir imagens através de satélite e de disseminá-las de forma não discriminatória[28].

Com este excurso, pretendem os Autores assinalar que também noutras alturas houve necessidade de consensualmente adaptar os quadros jurídicos vigentes em prol de um interesse comum entendido como benéfico. Poderia, questionam, ponderar-se se solução semelhante poderia ocorrer com este tema.

Também o Conselho da Europa tem procurado explorar uma solução para o problema do acesso transfronteiriço a dados informáticos. Assim, o Comité da Convenção sobre o Cibercrime junto do Conselho da Europa estabeleceu, na sua reunião plenária de 23 e 24 de Novembro de 2011, o sub-grupo *ad-hoc* sobre jurisdição e acesso transfronteiriço a dados e fluxos de dados (*Transborder Group)*, com o objectivo de «desenvolver um instrumento jurídico — como uma adenda à Convenção, um Protocolo ou Recomendação — que regule o acesso transfronteiriço a dados e fluxo de dados, bem como o uso de medidas de investigação

[27] *Idem*, pp. 68-71.
[28] *Idem*, pp. 71-72.

transfronteiriças na Internet e assuntos conexos, e para apresentar um relatório com as conclusões do Comité»[29].

Em 9 de Abril de 2013, o *Transborder Group* apresentou uma proposta com os elementos preliminares para um Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime[30], no qual fez constar cinco propostas para enfrentar o problema da *loss of location*, a saber:

a) A aplicabilidade da excepção prevista no artigo 32.º, alínea *b)*, da Convenção a qualquer Estado, ainda que não signatário da Convenção sobre o Cibercrime, quando não seja claro o local de armazenamento dos dados ou quando os mesmos se encontrem em *movimento*[31], ainda que seguida de notificação do Estado no qual os dados se encontrem armazenados, uma vez descoberta a sua localização;

b) O acesso transfronteiriço mediante credenciais legitimamente obtidas, seguido da notificação do Estado no qual se encontrem armazenados os dados;

c) O acesso transfronteiriço em certos casos, com o objectivo de evitar a concretização de um perigo iminente, ofensa à integridade física, a fuga de um suspeito ou o perigo de destruição de elementos probatórios relevantes, novamente seguido de notificação ao Estado no qual se encontrassem armazenados os dados. Adicionalmente poderia ser criada uma disposição destinada a cobrir as situações de *boa fé*, em que, durante uma pesquisa, a autoridade competente não saiba se o sistema informático pesquisado se encontra em território estrangeiro, ou, mesmo que o saiba, não saiba em que território estrangeiro se encontra, ou tenha inadvertidamente obtido prova digital armazenada em território estrangeiro (em todos estes casos não seria necessário que o Estado em causa fosse parte da Convenção);

d) A simples remoção da limitação territorial da pesquisa informática, embora, neste caso, a medida apenas possa ocorrer em relação a Estados que sejam Partes na Convenção;

e) A utilização do critério do poder de disposição[32] (*power of disposal*), e que, em síntese, se traduz na ligação existente entre os dados visados e a pessoa ou pessoas que a eles têm, exclusiva ou colectivamente, acesso e que preservam o direito de os alterar,

[29] Cf. SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME (T-CY), *Transborder access and Jurisdiction: What are the options?*, cit., p. 4.

[30] Cf. SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME, *(Draft) elements of an Additional Protocol to the Budapest Convention on Cybercrime regarding transborder access to data*, T-CY(2013)14, 2013, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)14transb_elements_protocol_V2.pdf.

[31] Sendo certo que, como consta da proposta, esta opção poderia conflituar com o artigo 34.º da Convenção de Viena sobre o Direito dos Tratados, nos termos do qual «um tratado não cria obrigações nem direitos para um terceiro Estado sem o consentimento deste».

[32] Cf. JAN SPOENLE, «Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal», pp. 10-12, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/internationalcooperation/2079_Cloud_Computing_power_disposal_31Aug10a.pdf.

eliminar, suprimir ou tornar inutilizáveis, bem como o direito de excluir o seu acesso e a sua utilização de qualquer modo a terceiros[33].

Com base no referido documento, o T-CY, na sua 9.ª reunião plenária, ocorrida em 4 e 5 de Junho de 2013, deliberou começar a preparação de um protocolo adicional à Convenção sobre o Cibercrime, com vista à regulação do acesso transfronteiriço[34], a começar após reflexão e diálogo com as partes interessadas, incluindo intervenientes do sector privado e autoridades de protecção de dados[35].

Por vicissitudes várias, até à data, não existe uma solução oficial adoptada e o grupo permanece a trabalhar nesse sentido.

4. A resposta nacional

Perante as dificuldades colocadas pela impossibilidade de aceder remotamente a informação armazenada no estrangeiro, e dada a tendencial ausência de consequências no foro diplomático e probatório deste tipo de práticas, certos Estados têm optado por prever o acesso transfronteiriço nas suas legislações nacionais.

É o caso, desde logo, da Bélgica, onde o legislador previu, no artigo 39*bis* do Código de Processo Penal, a possibilidade de ser alargada a pesquisa informática a outros Estados, independentemente da sua localização, desde que, quando se suspeite que a informação não esteja armazenada na Bélgica, a informação não seja eliminada mas apenas copiada e sob condição de o Ministro da Justiça informar o Estado pesquisado, quando este possa ser identificado (embora, segundo conste, esta notificação nunca tenha ocorrido)[36].

Em Portugal o legislador adoptou uma solução mais discreta na formulação mas, ao que tudo indica, mais ousada do que a belga. Ao suprimir, por comparação com a norma homóloga da Convenção sobre o Cibercrime, a limitação territorial à extensão da pesquisa informática a sistemas informáticos acessíveis através do primeiro sistema pesquisado (por exemplo, no caso dado no início desta apresentação), o investigador poderia, nos termos do artigo 15.º, n.º

[33] O legislador português incluiu um conceito semelhante no artigo 15.º, n.º 3, alínea a), da Lei do Cibercrime, ao prever a desnecessidade de recurso a autorização da autoridade judiciária para a realização de uma pesquisa informática quando «[a] mesma for voluntariamente consentida por quem tiver **a** disponibilidade ou controlo desses dados […]».

[34] Cf. SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME, *Draft Decision Preparation by the T-CY of a draft Additional Protocol to the Convention on Cybercrime (ETS 185) regarding transborder access to data*, T-CY(2013)18, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)18_TB_prot_mandate_v5.pdf.

[35] Cf. SUB-GRUPO AD-HOC SOBRE JURISDIÇÃO E ACESSO TRANSFRONTEIRIÇO A DADOS E FLUXOS DE DADOS JUNTO DO COMITÉ DA CONVENÇÃO SOBRE O CIBERCRIME, *Report of the Transborder Group for 2013*, T-CY (2013)30, p. 6, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY%282013%2930_Final_transb_rep_V5.pdf e T-CY, Abridged meeting report, T-CY (2013)28E rev, disponível em: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY%202013/T-CY(2013)28_Plen10AbrRep_V3.pdf.

[36] Na ilustrativa expressão de Jan Kerkhofs, na Bélgica prevaleceria a *teoria do aquário*, o que significa que o investigador se comportaria como se estivesse a olhar para o interior de um aquário através do vidro, sem possibilidade de tocar no seu conteúdo, mas com o poder de fotografar a imagem que perante si se apresenta.

5, da Lei do Cibercrime, recolher a informação independentemente da sua localização. Como refere Pedro Verdelho «[e]sta norma é bastante aberta, deixando por regular muitos dos seus detalhes de aplicação ao caso concreto. Desde logo, por exemplo, não limita o acesso a computadores em território nacional. Isto é, legitima o acesso *virtual* a todo e qualquer computador, independentemente da sua localização física que, assim, pode ser em qualquer parte do mundo»[37]. A solução portuguesa aparenta admitir essa pesquisa num cenário de busca, e, portanto, a título excepcional – embora não seja evidente que essa pesquisa não possa ocorrer directamente por via do artigo 15.º, n.º 1, da Lei do Cibercrime, quando as credenciais de acesso estejam na posse do investigador –, sem prever especiais normas de apreensão para o efeito. Parece, contudo, que uma solução de compatibilização possível entre os interesses em causa pressuporia que a única modalidade de apreensão a realizar nestes casos seria a *cópia* e não qualquer das outras previstas no artigo 16.º, n.º 7, da Lei do Cibercrime.

Solução semelhante foi adoptada recentemente pelo legislador espanhol, que previu expressamente no artigo 588 *sexies* a possibilidade de serem realizadas pesquisas informáticas a sistemas de armazenamento massivo de informação, designadamente por via de extensão da pesquisa, sem que da norma conste qualquer limitação territorial em relação ao local onde se encontre armazenada a informação.

Embora pareça difícil que venha a formar-se um costume internacional sobre o tema do acesso transfronteiriço, em grande medida por questões de princípio dos Estados que não querem abdicar de qualquer parcela da sua soberania, tudo indica que o debate continuará a decorrer numa plataforma essencialmente académica ou no plano da discussão legislativa supranacional[38], enquanto uma parte cada vez maior dos operadores judiciários tenderá a ignorar o problema, por ignorância ou por despreocupação – eventualmente fundada – em relação a eventuais consequências no foro diplomático ou probatório daí decorrentes.

Afigura-se, contudo, da maior importância que o debate seja alargado e que se procure explorar uma solução adequada à realidade digital, se necessário repensando conceitos tradicionais que neste foro são de difícil aplicabilidade e procurando uma compatibilização de interesses adaptada às especificidades deste ambiente.

[37] PEDRO VERDELHO, *A obtenção de prova online*, em AA.VV. *Cibercrimen – Aspectos de Derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet* (org. Daniela Dupuy / Mariana Kiefer), Montevideo Buenos Aires: BdeF, 2016, p. 445.
[38] Sem prejuízo, naturalmente, de se continuarem a procurar soluções que tornem mais expeditos os mecanismos de auxílio mútuo, como é o caso da proposta de Regulamento do Parlamento Europeu e do Conselho sobre a Ordem de Produção e Preservação Europeia de prova digital em matéria criminal, publicada no dia 17 de Abril de 2018.

CENTRO
DE ESTUDOS
JUDICIÁRIOS

4.

Métodos ocultos de investigação criminal em ambiente digital

David Silva Ramalho

CENTRO
DE ESTUDOS
JUDICIÁRIOS

MÉTODOS OCULTOS DE INVESTIGAÇÃO CRIMINAL EM AMBIENTE DIGITAL*

David Silva Ramalho**

1. Dificuldades da investigação criminal em ambiente digital
2. O recurso a métodos ocultos de investigação criminal
3. O acesso oculto a dados informáticos armazenados
4. As acções encobertas em ambiente digital
5. *Hacking* e o uso de *malware*

*Apresentação que serviu de base à conferência proferida pelo autor no CEJ / Porto, em 9 de Março de 2018.

** Assistente Convidado da Faculdade de Direito da Universidade de Lisboa, investigador do Centro de Investigação de Direito Penal e Ciências Criminais e Advogado.

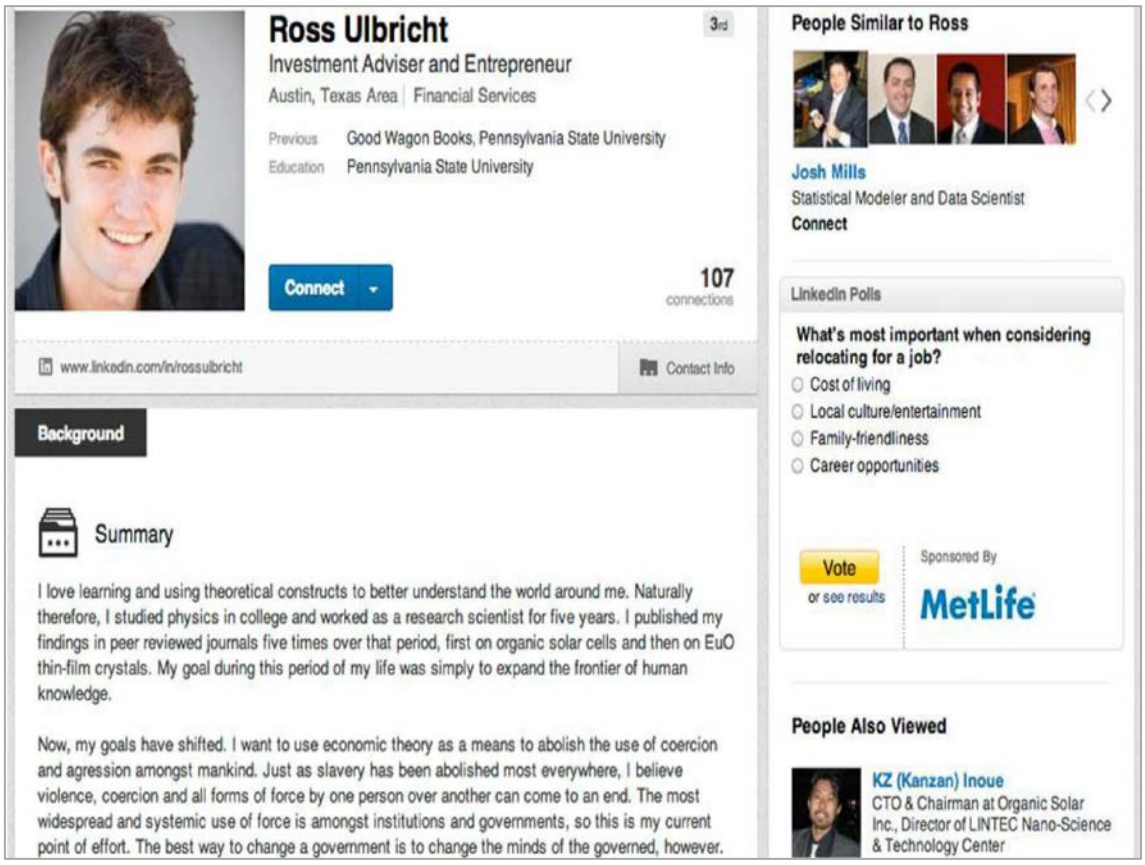
Métodos ocultos de investigação criminal em ambiente digital

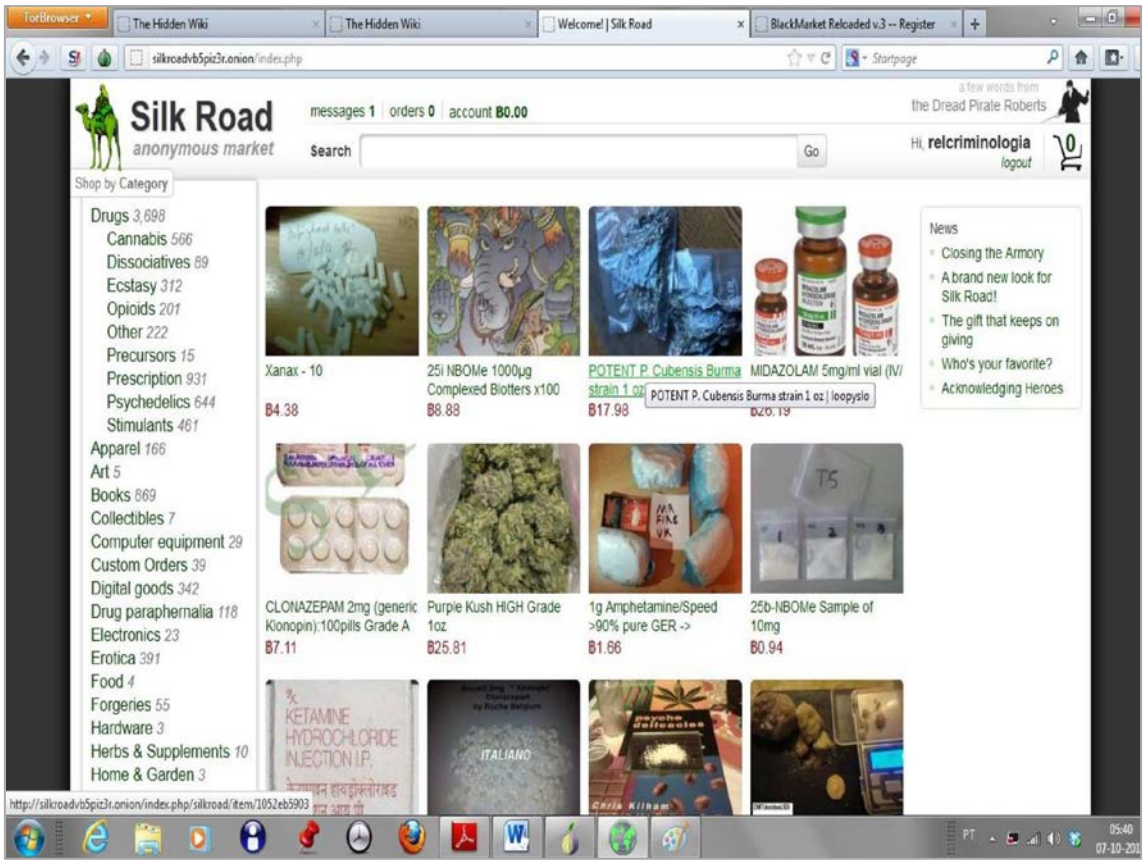
1. Dificuldades da investigação criminal em ambiente digital.
2. O recurso a métodos ocultos de investigação criminal.
3. O acesso oculto a dados informáticos armazenados.
4. As acções encobertas em ambiente digital.
5. *Hacking* e o uso de *malware*

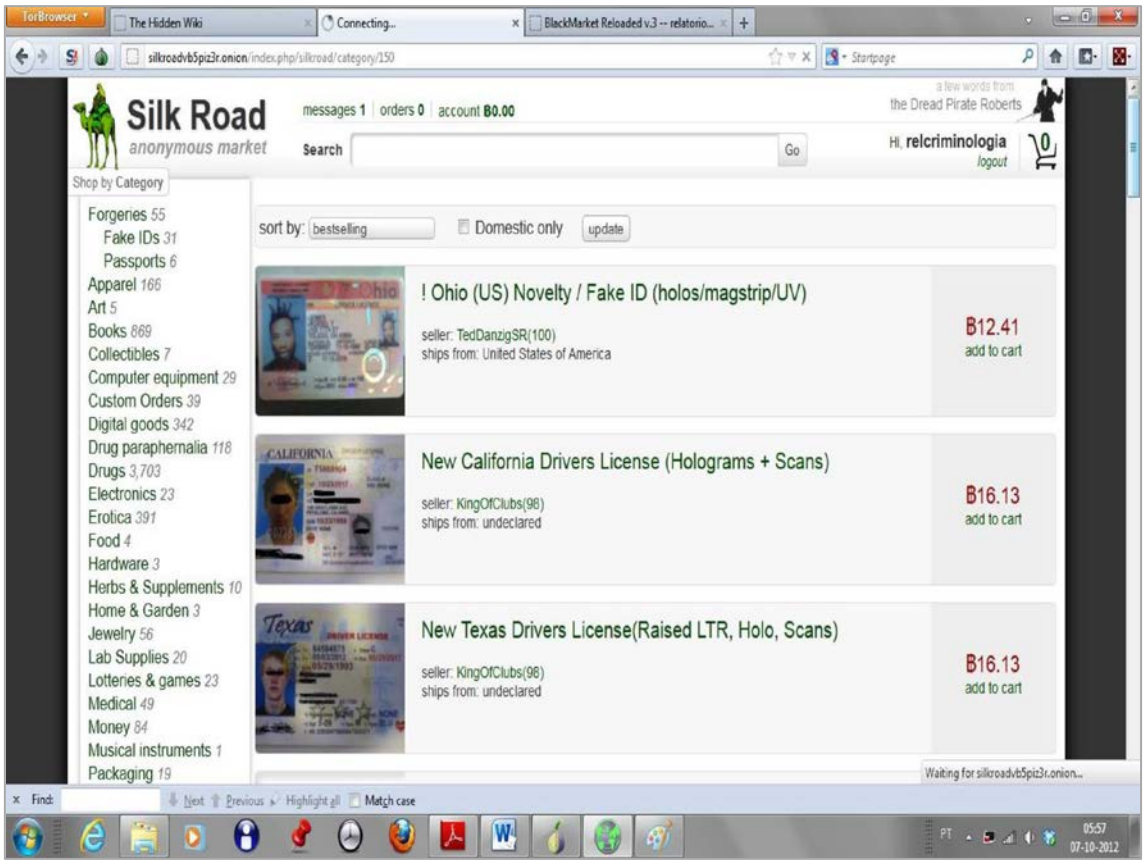
CENTRO DE ESTUDOS JUDICIÁRIOS

1. Dificuldades da investigação criminal em ambiente digital

CENTRO DE ESTUDOS JUDICIÁRIOS


Ross Ulbricht
3rd
Investment Adviser and Entrepreneur
Austin, Texas Area | Financial Services
Previous Good Wagon Books, Pennsylvania State University
Education Pennsylvania State University
Connect
107
connections
www.linkedin.com/in/rossulbricht
Contact Info
Background
Summary
I love learning and using theoretical constructs to better understand the world around me. Naturally therefore, I studied physics in college and worked as a research scientist for five years. I published my findings in peer reviewed journals five times over that period, first on organic solar cells and then on EuO thin-film crystals. My goal during this period of my life was simply to expand the frontier of human knowledge.
Now, my goals have shifted. I want to use economic theory as a means to abolish the use of coercion and agression amongst mankind. Just as slavery has been abolished most everywhere, I believe violence, coercion and all forms of force by one person over another can come to an end. The most widespread and systemic use of force is amongst institutions and governments, so this is my current point of effort. The best way to change a government is to change the minds of the governed, however.
People Similar to Ross
Josh Mills
Statistical Modeler and Data Scientist
Connect
LinkedIn Polls
What's most important when considering relocating for a job?
Cost of living
Local culture/entertainment
Family-friendliness
Career opportunities
Vote
or see results
Sponsored By
MetLife
People Also Viewed
KZ (Kanzan) Inoue
CTO & Chairman at Organic Solar Inc., Director of LINTEC Nano-Science & Technology Center


TorBrowser
The Hidden Wiki
The Hidden Wiki
Welcome! | Silk Road
BlackMarket Reloaded v.3 -- Register
silkroadvb5piz3r.onion/index.php
Silk Road
anonymous market
messages 1 | orders 0 | account B0.00
Search
Go
a few words from the Dread Pirate Roberts
Hi, relcriminologia
logout
Shop by Category
Drugs 3,698
Cannabis 566
Dissociatives 89
Ecstasy 312
Opioids 201
Other 222
Precursors 15
Prescription 931
Psychedelics 644
Stimulants 461
Apparel 166
Art 5
Books 869
Collectibles 7
Computer equipment 29
Custom Orders 39
Digital goods 342
Drug paraphernalia 118
Electronics 23
Erotica 391
Food 4
Forgeries 55
Hardware 3
Herbs & Supplements 10
Home & Garden 3
Xanax - 10
B4.38
25i NBOMe 1000µg Complexed Blotters x100
B8.88
POTENT P. Cubensis Burma strain 1 oz
B17.98
MIDAZOLAM 5mg/ml vial (IV/
News
Closing the Armory
A brand new look for Silk Road!
The gift that keeps on giving
Who's your favorite?
Acknowledging Heroes
CLONAZEPAM 2mg (generic Klonopin):100pills Grade A
B7.11
Purple Kush HIGH Grade 1oz
B25.81
1g Amphetamine/Speed >90% pure GER ->
B1.66
25b-NBOMe Sample of 10mg
B0.94
KETAMINE HYDROCHLORIDE INJECTION I.P.
ITALIANO
http://silkroadvb5piz3r.onion/index.php/silkroad/item/1052eb5903



1.1. Dificuldades na identificação do agente do crime

- Anonimizadores (*proxies*, TOR, *Freedom Hosting*);
- Moedas virtuais (*bitcoins* e *altcoins*);
- Conservação de dados de tráfego *(data retention);*
- Aspectos jurisdicionais

CENTRO DE ESTUDOS JUDICIÁRIOS

1.2. Dificuldades na descoberta e valoração da prova

- Cifragem de dados;
- Cifragem do disco;
- Alteração de *metadata,* como data de criação (*Timestomp*);
- Ataques contra perícias forenses.

CENTRO DE ESTUDOS JUDICIÁRIOS

2. O recurso a métodos ocultos de investigação criminal

CENTRO DE ESTUDOS JUDICIÁRIOS

2.1. Características

- Métodos ocultados do visado;
- Um imperativo de eficácia;
- Neutralizam alguns dos seus direitos processuais (e.g. não auto-incriminação ou direito a recusar prestar testemunho);
- São abrangentes (incluem terceiros e não se limitam ao momento do facto);
- Ignoram a intimidade e fiabilidade da comunicação.
- O centro do processo desloca-se para o inquérito

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da reserva de lei:
  - Métodos ocultos atípicos?
    1 – Delimitação positiva: subsidiariedade da prova atípica à típica;
    2 – Existência de limites expressos na lei e CRP
    3 – Aptidão para restringir direitos fundamentais

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da reserva de lei:
  - Segurança jurídica;
  - Prevenção de abuso e arbítrio;
  - Conhecimento pela comunidade dos meios à disposição da investigação;
  - Possibilidade de sindicar a sua legalidade;

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da reserva de lei:
  - Proibição de analogia ou de argumentos por *maioria de razão* (e.g. acção encoberta e escutas).
    - Diferente de intervenção restritiva legitimada pela norma mas executada com um âmbito mais circunscrito

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da reserva de lei:
  - A lei como ponderação *específica*.
  - Não se aplica a novos modos de execução de métodos de obtenção típicos.
  - Necessidade de densidade normativa da habilitação legal, ainda que permitindo uma ponderação concreta.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da proporcionalidade:
  - Primeiro do legislador, depois do aplicador;
  - **Adequação**: susceptibilidade de o meio permitir a realização eficaz do fim da restrição.
    - Tendencialmente de verificação prática e não legislativa.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da proporcionalidade:
  - **Necessidade**: Entre os meios à disposição deve ser escolhido aquele que, em concreto, face aos pressupostos da lei e às circunstâncias do caso concreto, se revela necessário, exigível ou indispensável para atingir o fim.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da proporcionalidade:
  - **Proporcionalidade *stricto sensu***: verificação da *justeza* (ou da justa medida) da medida restritiva.
  - Critério da não desproporcionalidade?
  - Temperado por critérios objectivos: gravidade, força dos indícios, sanção previsível, etc.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da subsidiariedade:
  - No plano extrínseco: prioridade aos métodos *abertos*.
  - No plano intrínseco: o menos grave dos disponíveis;
  - Evitar a cumulação de métodos ocultos.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.2. Princípios gerais

- Princípio da reserva de juiz:
  - O direito fundamental ao juiz.
  - Um "tigre sem dentes"?
  - Várias excepções.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.3. Especificidades do ambiente digital

- A tutela jurídica do ambiente digital:
  - Autonomia ontológica da realidade digital;
  - Localização geográfica, conteúdo, ligação à Internet, extensão a outros sistemas.
  - O direito à integridade e confidencialidade dos sistemas informáticos (BVerfG) ou o direito à não intromissão no ambiente digital (Gonzalez-Cuellar Serrano).

CENTRO DE ESTUDOS JUDICIÁRIOS

2.3. Especificidades do ambiente digital

- Os conhecimentos fortuitos:
  - O problema da dimensão da informação e da existência de um *motor de busca*;
  - Crimes de catálogo vs meios livres;
  - O princípio do limiar da intervenção equivalente ou da intervenção substitutive hipotética e a mudança de fim que justifica o meio.

CENTRO DE ESTUDOS JUDICIÁRIOS

2.3. Especificidades do ambiente digital

- O direito a um contraditório qualificado:
  - O carácter técnico e hermético da informação sobre diligências informáticas;
  - A fragilidade da prova digital;
  - A necessidade de relatórios claros e densos.

CENTRO DE ESTUDOS JUDICIÁRIOS

3. O acesso oculto a dados informáticos

CENTRO DE ESTUDOS JUDICIÁRIOS

3.1. A pesquisa à distância de dados informáticos na disponibilidade de terceiros

- As normas da pesquisa estão pensadas para um contexto de busca;
- A pesquisa do artigo 15.º, n.º 5, da Lei do Cibercrime não pode, por natureza, ser oculta;
- Mas e a do 15.º, n.º 1?

CENTRO DE ESTUDOS JUDICIÁRIOS

3.1. A pesquisa à distância de dados informáticos na disponibilidade de terceiros

- A quem se dirige a cópia do despacho imposta pelo artigo 176/1 CPP ex vi 15/6 CPP?
- Quem tem a *disponibilidade* dos dados?
- A aplicação do regime das buscas "com as necessárias adaptações".
- Como preside a AJ à diligência?

CENTRO DE ESTUDOS JUDICIÁRIOS

3.1. A pesquisa à distância de dados informáticos na disponibilidade de terceiros

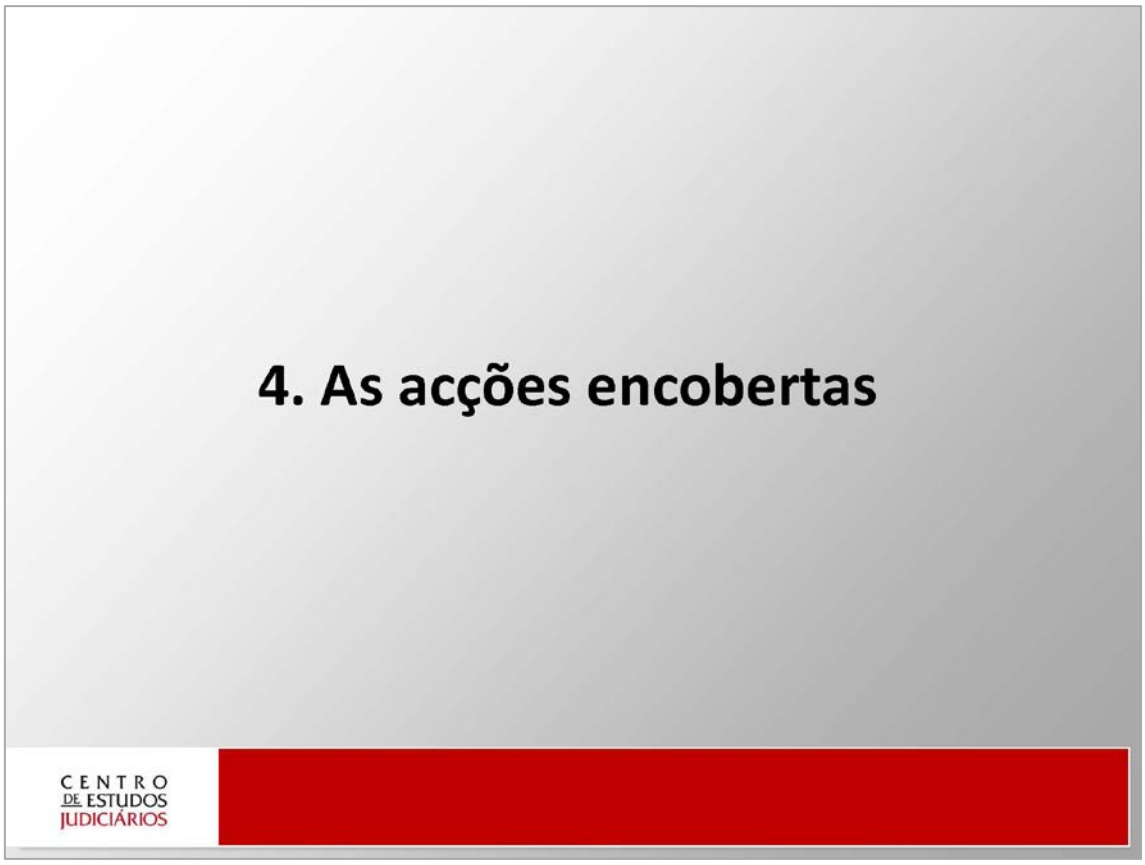
- Se não for admissível, será que apenas se pode aceder a outro Sistema a partir do 15/5 da LC?
- Obrigação de recorrer à injunção para apresentação ou concessão do acesso a dados?

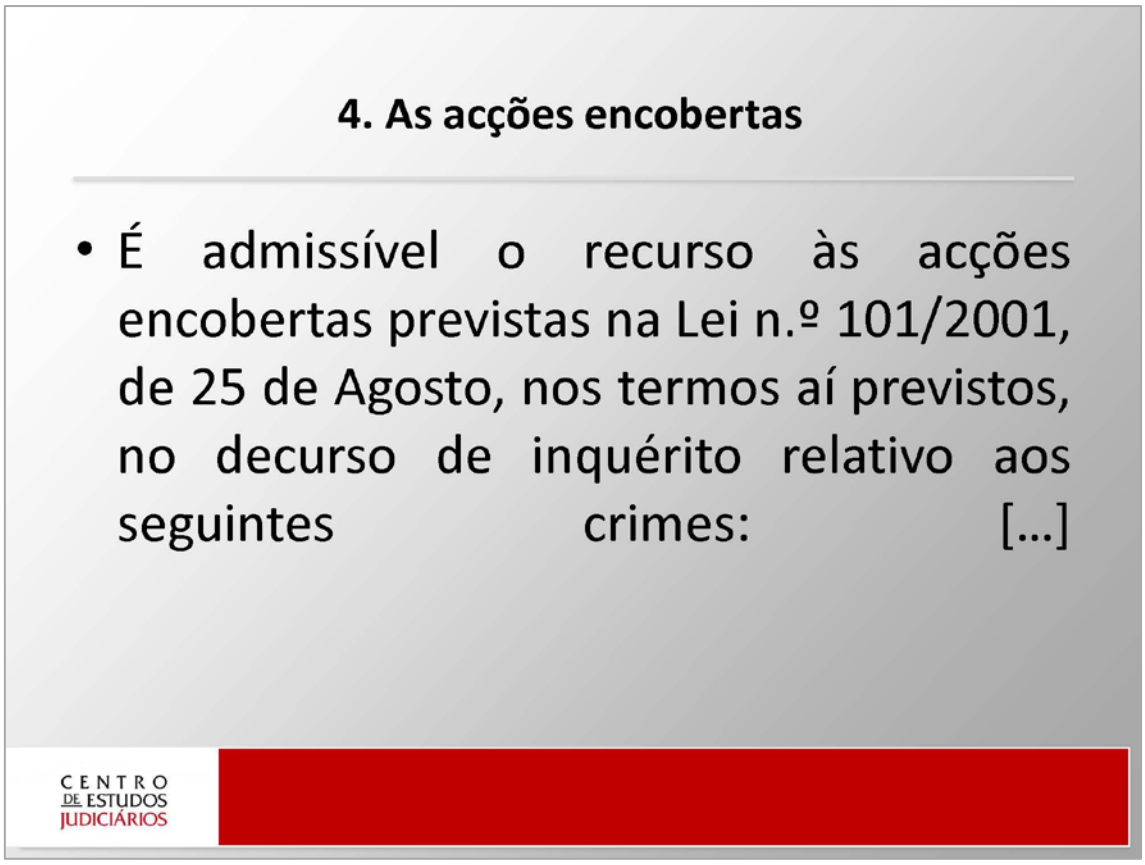
CENTRO DE ESTUDOS JUDICIÁRIOS

3.2. Outros meios

- A injunção para concessão ou apresentação do acesso a dados.
- A obtenção de dados de tráfego:
  - Problema da eventual impossibilidade de aplicação da Lei n.º 32/2008.

CENTRO DE ESTUDOS JUDICIÁRIOS


4. As acções encobertas
CENTRO DE ESTUDOS JUDICIÁRIOS


4. As acções encobertas
• É admissível o recurso às acções encobertas previstas na Lei n.º 101/2001, de 25 de Agosto, nos termos aí previstos, no decurso de inquérito relativo aos seguintes crimes: [...]
CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. Problemas gerais

– Comparação permanente com as acções encobertas em ambiente físico:
  - O início das acções encobertas *online* (*chats* e *posts* com link de conhecimento reservado; integração pública v. privada, activa v. passiva).
  - As múltiplas personalidades sucedâneas ou simultâneas numa ou mais salas de chat (o agente pode ser o traficante, o comprador, o menor ou o pedófilo – tem de ser regulado).

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. Problemas gerais

- A apropriação da identidade de terceiros (v. caso Silk Road).
- O risco de abusos por parte do agente encoberto (v. Carl Force IV e Shaun Bridges – 250.000,00$ em bitcoins).
- As novas vias de fronteira entre encobrimento e provocação (nomes provocadores ou identidades de ex-participantes).
- O registo integral e passivo de salas públicas.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. Problemas gerais

- Os terceiros infiltrados, em particular, os terceiros integrados na rede criminosa;
- Pode assumir a figura de agente infiltrado, o indivíduo que cometeu crimes no meio investigado?
  - Pode mas em geral não terá especial interesse;
  - as suas declarações serão sempre prestadas ao abrigo do regime aplicável ao co-arguido (cf. artigo 345.º, n.º 4, do CPP) e nunca ao das testemunhas (cf. artigo 133.º, n.º 1, alínea *a)*), do CPP),
  - Por força do seu estatuto processual, o arguido poderá sempre recusar-se a prestar declarações em sede de julgamento.
  - Pode valer para recolha e registo autónomo de prova

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. Problemas na aplicação da Lei 101/2001

- Identidade fictícia *online* mediante proposta do Director nacional da PJ e atribuída pelo MJ (usernames próprios ou de terceiros)?
  - Mas o mesmo username pode ser utilizado por vários agentes.
  - Questão operacional?
  - O relato do agente encoberto.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. Problemas na aplicação da Lei 101/2001

– A isenção de responsabilidade apenas quanto a actos preparatórios ou em em qualquer forma de comparticipação diversa da instigação e da autoria mediata (a *lógica de comparticipação*).

- Problemas em *peer-to-peer;*
- Envio de ficheiros de conteúdo ilícito (analogia com as entregas controladas).
- É necessária a publicação de regras ou manuais de boas práticas ou afins.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. O regime espanhol (LO 13/2015)

Novo artigo 282.º bis

6. El juez de instrucción podrá autorizar a funcionarios de la Policía Judicial para actuar bajo identidad supuesta en **comunicaciones mantenidas en canales cerrados de comunicación** con el fin de esclarecer alguno de los delitos a los que se refiere el apartado 4 de este artículo o cualquier delito de los previstos en el artículo 588 ter a.

El agente encubierto informático, **con autorización específica para ello**, podrá intercambiar o enviar por sí mismo archivos ilícitos por razón de su contenido y analizar los resultados de los algoritmos aplicados para la identificación de dichos archivos.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.4. Os *siti civetta*

- Siti civetta: Artigo 14/2 da *Legge* 3 agosto 1998, n. 269, que aprovou a lei contra a exploração da prostituição, da pornografia, do turismo sexual contra crianças, como novas formas de redução à escravidão.
- Criação de websites e gestão de áreas de comunicação como *chats*.

CENTRO DE ESTUDOS JUDICIÁRIOS

5. *Hacking* e o uso de *malware*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. *Malware*

- *Malicious + software*

«um conjunto de instruções executadas no computador que levam o sistema a fazer algo que um atacante quer que ele faça»

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. *Malware*

- Logic bombs;
- Spyware
- Rootkits;
- Virus;
- Worms
- Blended threats
- Keyloggers, sniffers, etc

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. *Malware*

- Permitem:
  - Recolher informação (incluindo credenciais de acesso) para envio a terceiros;
  - Criar *backdoors* (acesso remoto, contornar os mecanismos de autenticação);
  - Instalar mais *malware*;
  - Monitorizar a actividade do utilizador;
  - Activar o *hardware*, como microfones e *webcams*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.1. *Malware*

- Processos de instalação:
  - Via suporte físico removível (útil para redes locais);
  - Via *Web browser* (*drive-by downloads*) –Ex. *Magneto* e Freedom Hosting (MAC address e nome de utilizador do administrador do Windows, e, por fim, o IP);
  - Via *download* (*e-mails,* programas, falsas actualizações).

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. *Malware* em Itália: o caso Hacking Team

Software vendido a vários Estados, incluindo aos governos do Sudão, da Rússia, das Honduras, do Equador, do Panama e da região do Curdistão.

Após divulgação do código fonte do RCS Galileo, ele começou a ser utilizado por cibercriminosos para infiltrar computadores de terceiros

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. *Malware* em Itália: o caso Hacking Team

Remote Control System Galileo:

- Fácil de utilizar, inclusivamente por quem não seja especialista em tecnologias de informação.
- Em cerca de duas semanas, o agente de investigação está pronto a utilizá-lo.
- *Se os hackers são piratas, a Hacking Team é um corsário - Vaciago*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. *Malware* em Itália: o caso Hacking Team

Funcionalidades do *Galileo:*

- *Intercepção de comunicações*
- *Activação remota de webcams e microfones*
- *Activação das funcionalidades GPS*
- *Instalação de keyloggers*
- *Gravação de comunicações em IM (incluindo Skype)*
- *Screenshots da actividade do utilizador, etc.*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.2. *Malware* em Itália: o caso Hacking Team

Processo de instalação do *Galileo:*

- Processo de instalação:
- *Via vulnerabilidades do Flash, Word, etc.*
- *Engenharia social*
- *Ocupa menos de 1 MB*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Itália: jurisprudência

Italian Supreme Court of Cassation, Division V, Decision No. 24695, of 14 October 2009

The Italian Supreme Court did not find in the tools any kind of surveillance, based on the assumption that the investigative activity consisted of seizing and copying documents stored on the hard disk of the device used by the accused, and **did not involve any 'flow of communications',** but only 'an operational relationship between the microprocessor and video of the electronic system'.

This definition enabled the Public Prosecutor to avoid seeking a search warrant from the judge in charge of Preliminary Investigations to activate such a kind of tool.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Itália: jurisprudência

Questão foi colocada no plenário do Supremo para resolução do conflito de orientações jurisprudenciais:

Pergunta-se: possível levar a cabo vigilância electrónica entre pessoas presentes através da instalação deste tipo de ferramentas em dispositivos electrónicos portáteis, mesmo em contexto privado, apesar de não identificadas separadamente e mesmo se nenhuma actividade criminosa esteja a decorrer entre eles?

Tribunal admitiu-o em criminalidade muito grave.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Itália: legislação

Nos últimos 4 anos houve 4 tentativas de regulamentar o malware.

As primeiras duas foram alvo de críticas por não serem suficientemente garantísticas.

Encontram-se em discussão duas propostas.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Espanha: legislação

Artículo 588 septies a. Presupuestos. 1. El juez competente podrá autorizar la utilización de datos de identificación y códigos, así como la instalación de un software, que permitan, de forma remota y telemática, el examen a distancia y sin conocimiento de su titular o usuario del contenido de un ordenador, dispositivo electrónico, sistema informático, instrumento de almacenamiento masivo de datos informáticos o base de datos, siempre que persiga la investigación de alguno de los siguientes delitos:

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Espanha: legislação

2. La resolución judicial que autorice el registro deberá especificar:

a) Los ordenadores, dispositivos electrónicos, sistemas informáticos o parte de los mismos, medios informáticos de almacenamiento de datos o bases de datos, datos u otros contenidos digitales objeto de la medida.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Espanha: legislação

b) El alcance de la misma, la forma en la que se procederá al acceso y aprehensión de los datos o archivos informáticos relevantes para la causa y el software mediante el que se ejecutará el control de la información.

c) Los agentes autorizados para la ejecución de la medida.

d) La autorización, en su caso, para la realización y conservación de copias de los datos informáticos.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Espanha: legislação

e) Las medidas precisas para la preservación de la integridad de los datos almacenados, así como para la inaccesibilidad o supresión de dichos datos del sistema informático al que se ha tenido acceso.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.3. *Malware* em Espanha: legislação

3. Cuando los agentes que lleven a cabo el registro remoto tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo, pondrán este hecho en conocimiento del juez, quien podrá autorizar una ampliación de los términos del registro.

CENTRO DE ESTUDOS JUDICIÁRIOS

4.4. Outras experiências

- **França**: *captation des donées informatiques* 8arts. 706-102-1 a 706-102-9
- **Finlândia**: "instalação de dispositivo, procedimento ou programa num Sistema informático para fins de vigilância técnica" (art. 26.º do capítulo 10 da Lei n.º 806/2011).
- **Holanda**: Nova proposta, alterada em Dezembro de 2015, que prevê o poder de aceder remotamente a sistemas informáticos

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português

- Aplicação do regime das escutas?
- Aplicação do regime das escutas + buscas?
- Aplicação do regime da intercepção de comunicações?
- Extensão prevista no artigo 15.º, n.º 5, da Lei do Cibercrime?

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português

"Sendo necessário **o recurso a meios e dispositivos informáticos** observam-se, naquilo que for aplicável, as regras previstas para a intercepção de comunicações" (art. 19.º, n.º 2, da Lei do Cibercrime).

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português: requisitos

a) Adequação aos fins de prevenção e repressão criminais identificados em concreto e proporcionais, quer a essas finalidades, quer à gravidade do crime sob investigação (artigo 3.º, n.º 1, da Lei n.º 101/2001, de 25 de agosto);

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português: requisitos

b) Fundadas suspeitas da prática de um dos crimes previstos na Lei do Cibercrime ou de crimes cometidos por meio de um sistema informático, quando lhes corresponda, em abstracto, pena de prisão de máximo superior a 5 anos ou, ainda que a pena seja inferior, e sendo dolosos, os crimes contra a liberdade e autodeterminação sexual nos casos em que os ofendidos sejam menores ou incapazes, a burla qualificada, a burla informática e nas comunicações, a discriminação racial, religiosa ou sexual, as infrações económico-financeiras,bem como os crimes consagrados no título IV do Código do Direito de Autor e dos Direitos Conexos (artigo 19.º, n.º 1, da Lei do Cibercrime);

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português: requisitos

c) A sua utilização apenas pode ocorrer quando houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter (artigo 18.º, n.º 2, da Lei do Cibercrime);

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português: requisitos

d) A precedência de despacho fundamentado do juiz de instrução, mediante requerimento do Ministério Público (artigo 18.º, n.º 2 da Lei do Cibercrime). Não uma espécie de *deferimento tácito*

CENTRO DE ESTUDOS JUDICIÁRIOS

4.5. O caso português: requisitos

e) A delimitação dos dados que se visa obter, de acordo com as necessidades concretas da investigação (artigo 18.º, n.º 3 da Lei do Cibercrime).

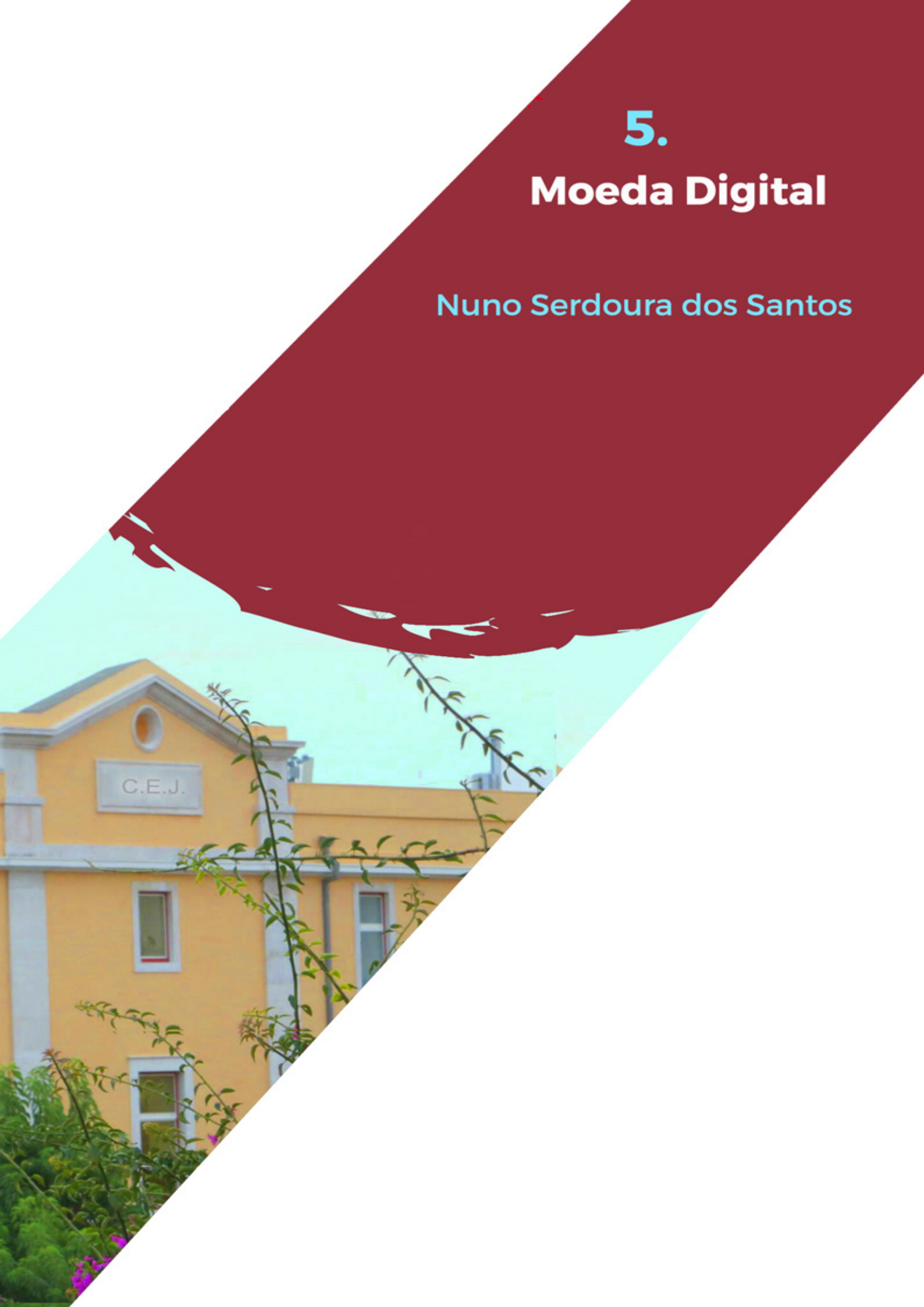
CENTRO DE ESTUDOS JUDICIÁRIOS


Obrigado pela V. atenção!
dsramalho@mlgts.pt
CENTRO DE ESTUDOS JUDICIÁRIOS

5.

Moeda Digital

Nuno Serdoura dos Santos



CENTRO
DE ESTUDOS
JUDICIÁRIOS

MOEDA DIGITAL**

Nuno Serdoura dos Santos*

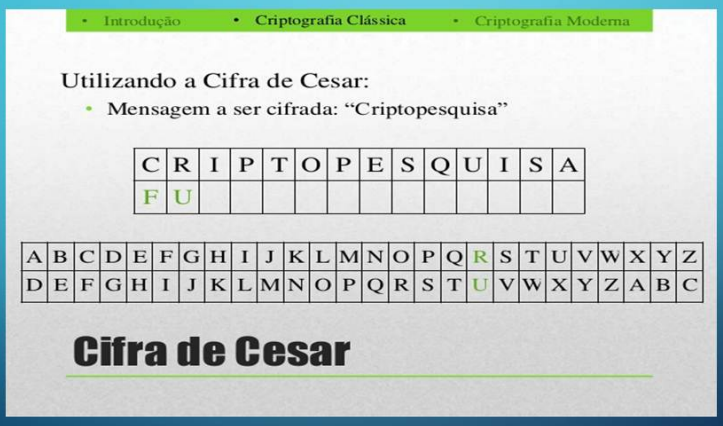
** Apresentação que serviu de base à conferência proferida pelo autor no CEJ / Porto, em 9 de Março de 2018.
* Procurador da República.

CRIPTO-MOEDA ?

- Uma moeda digital na qual se usam meios de encriptação (criptografia) para regular a criação de unidades de moeda e verificar a regularidade da transferência de fundos, operando independentemente (e apesar de) um Banco Central
- A primeira cripto moeda criada foi a Bitcoin, em 2009.
- Todavia, hoje há centenas de moedas, a que se dá o nome de Altcoins.

NS 2018

CRIPTOGRAFIA – A CIFRA DE CÉSAR



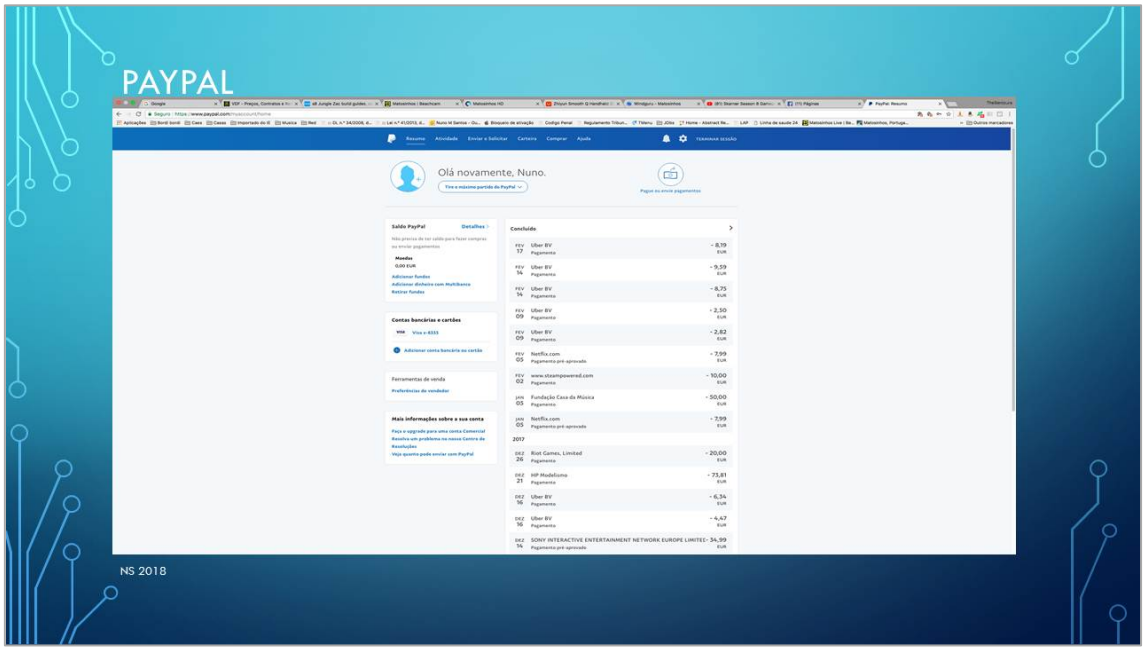
NS 2018

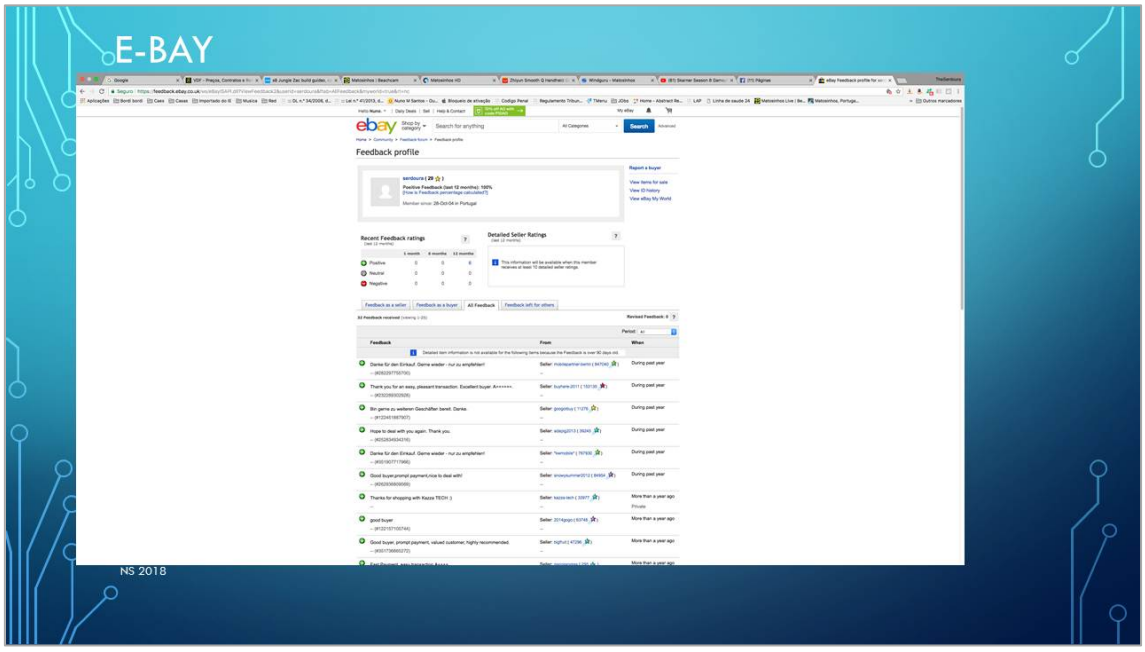
O QUE É A BITCOIN?

NS 2018

- Foi a primeira moeda digital descentralizada, criada por um tal Satoshi Nakamoto (alias);
- Ninguém controla a Bitcoin: não é moeda impressa, tratando-se de um sistema de pagamento baseado em prova matemática, produzido independentemente de uma autoridade central e não garantida por nenhum Estado;
- Usa a tecnologia peer-to-peer, com um código fonte de design publico, do qual ninguém é proprietário e toda a gente pode participar;
- Em termos simples, é um software open source que permite a transferência de dinheiro através da internet, sem custos, mais rapidamente, com maior confiança, e sem intermediários;

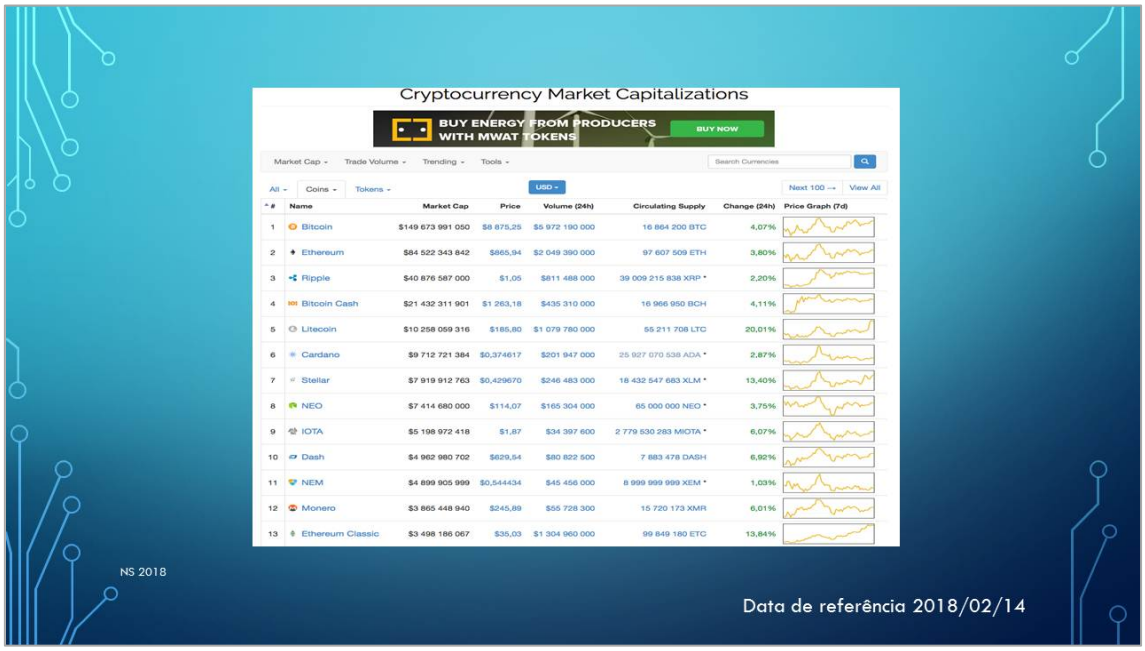
NS 2018

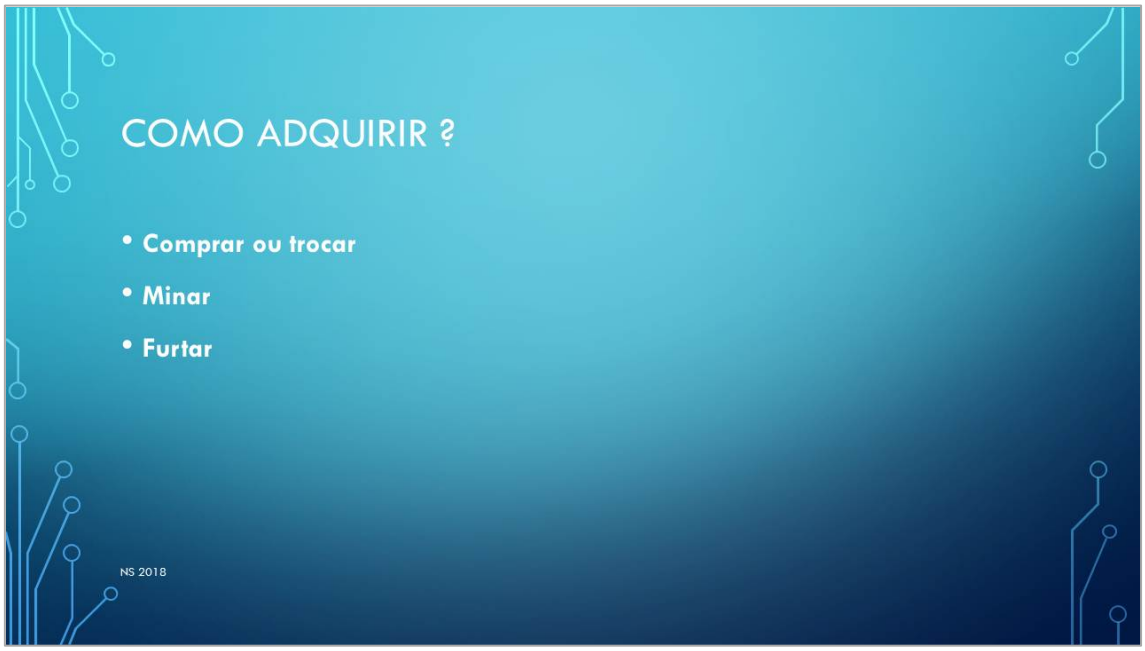

PAYPAL
Olá novamente, Nuno.
NS 2018


E-BAY
Feedback profile
NS 2018

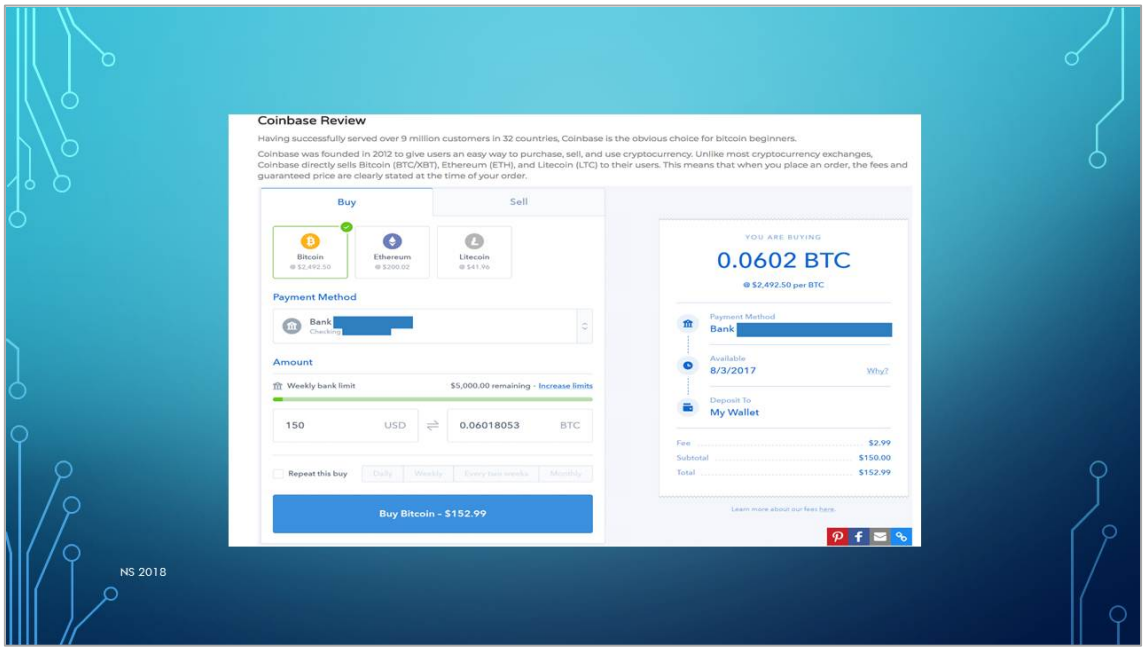

COMO SE COMPARA COM OUTROS MEIOS DE PAGAMENTO TRADICIONAIS ?
How Bitcoin Activity Stacks Up Against Other Payment Networks
Average daily transaction volume of selected payment networks (in million U.S. dollars)
Visa $17,559m
MasterCard $9,863m
China Union Pay $7,562m
American Express $2,434m
Discover (Pulse Network) $438m
PayPal $397m
Discover (Discover Network) $299m
Bitcoin $289m
Western Union $216m
Xoom $15m
0 1,000 2,000 8,000 9,000 10,000 17,000 18,000
Bitcoin transaction volume represents a 7-day average as of December 3. All other volumes based on latest company filings.
statista The Statistics Portal @StatistaCharts
Source: Coinometrics
NS 2018


COMO VARIA ?
Market Price (USD)
NS 2018
Data de referência 2018/02/14

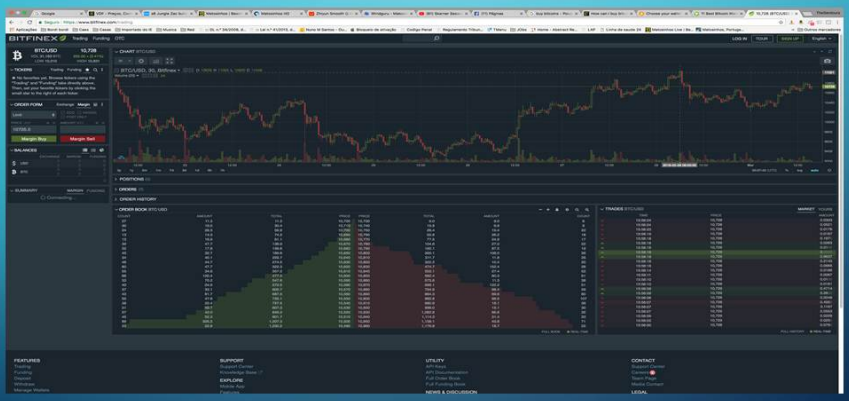

Cryptocurrency Market Capitalizations
BUY ENERGY FROM PRODUCERS WITH MWAT TOKENS
BUY NOW
Market Cap
Trade Volume
Trending
Tools
Search Currencies
All
Coins
Tokens
USD
Next 100 →
View All
Name Market Cap Price Volume (24h) Circulating Supply Change (24h) Price Graph (7d)
1 Bitcoin $149 673 991 050 $8 875,25 $5 972 190 000 16 864 200 BTC 4,07%
2 Ethereum $84 522 343 842 $865,94 $2 049 390 000 97 607 509 ETH 3,80%
3 Ripple $40 876 587 000 $1,05 $811 488 000 39 009 215 838 XRP * 2,20%
4 Bitcoin Cash $21 432 311 901 $1 263,18 $435 310 000 16 966 950 BCH 4,11%
5 Litecoin $10 258 059 316 $185,80 $1 079 780 000 55 211 708 LTC 20,01%
6 Cardano $9 712 721 384 $0,374617 $201 947 000 25 927 070 538 ADA * 2,87%
7 Stellar $7 919 912 763 $0,429670 $246 483 000 18 432 547 683 XLM * 13,40%
8 NEO $7 414 680 000 $114,07 $165 304 000 65 000 000 NEO * 3,75%
9 IOTA $5 198 972 418 $1,87 $34 397 600 2 779 530 283 MIOTA * 6,07%
10 Dash $4 962 980 702 $629,54 $80 822 500 7 883 478 DASH 6,92%
11 NEM $4 899 905 999 $0,544434 $45 456 000 8 999 999 999 XEM * 1,03%
12 Monero $3 865 448 940 $245,89 $55 728 300 15 720 173 XMR 6,01%
13 Ethereum Classic $3 498 186 067 $35,03 $1 304 960 000 99 849 180 ETC 13,84%
NS 2018
Data de referência 2018/02/14


COMO ADQUIRIR ?
• Comprar ou trocar
• Minar
• Furtar
NS 2018


COMO COMPRAR ?
WHERE TO BUY
BITCOIN EXCHANGERS
PEER 2 PEER
BTC e
kraken
BITSTAMP
LocalBitcoins.com
Bringing Bitcoin Everywhere
BITBOAT
NS 2018

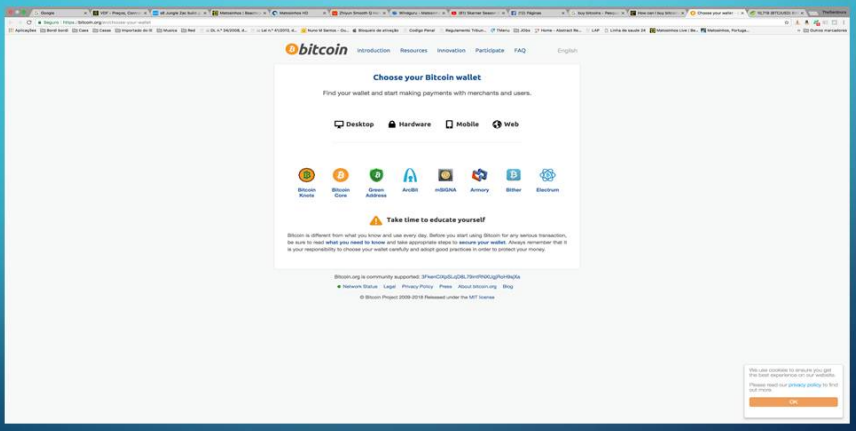

Coinbase Review
Having successfully served over 9 million customers in 32 countries, Coinbase is the obvious choice for bitcoin beginners.
Coinbase was founded in 2012 to give users an easy way to purchase, sell, and use cryptocurrency. Unlike most cryptocurrency exchanges, Coinbase directly sells Bitcoin (BTC/XBT), Ethereum (ETH), and Litecoin (LTC) to their users. This means that when you place an order, the fees and guaranteed price are clearly stated at the time of your order.
Buy
Sell
Bitcoin
Ethereum
Litecoin
Payment Method
Bank
Amount
Weekly bank limit
$5,000.00 remaining - Increase limits
150
USD
0.06018053
BTC
Repeat this buy
Buy Bitcoin - $152.99
YOU ARE BUYING
0.0602 BTC
@ $2,492.50 per BTC
Payment Method
Bank
Available
8/3/2017
Why?
Deposit To
My Wallet
Fee
$2.99
Subtotal
$150.00
Total
$152.99
NS 2018

ONDE E COMO COMPRAR ?



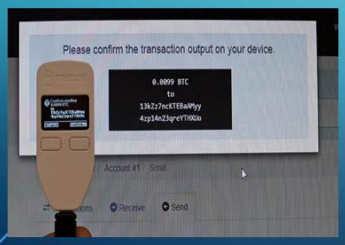
NS 2018

FURTAR...



NS 2018

EXEMPLOS DE "COLD STORAGE"



O QUE É "MINAR" ?

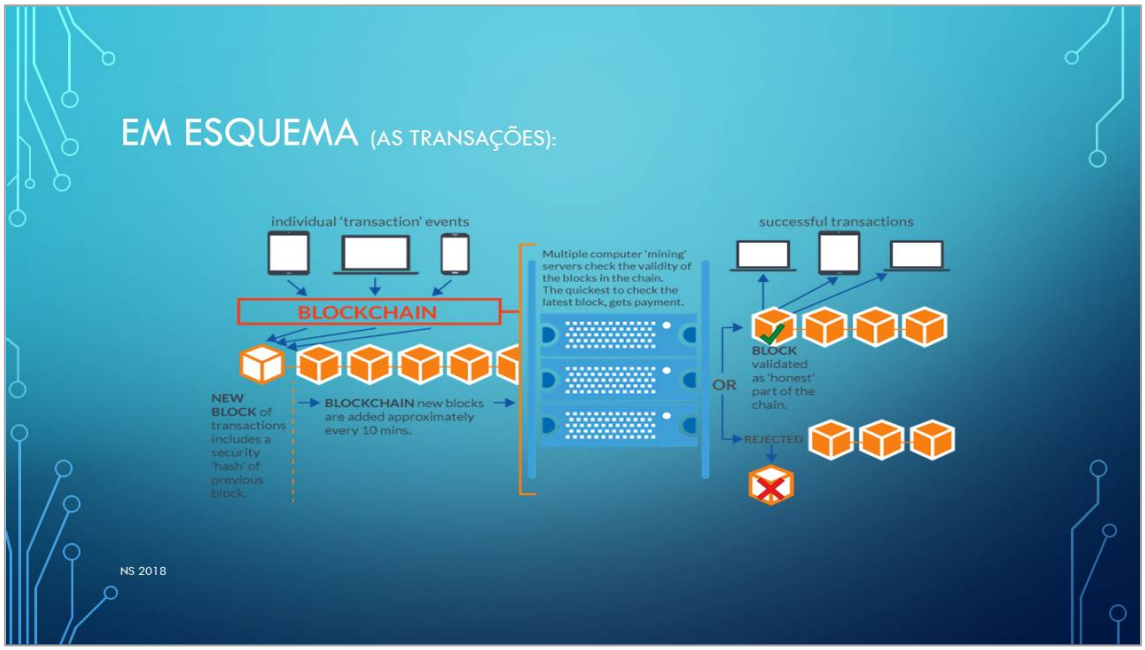
Desde o começo, o blockchain é tão seguro, por um mecanismo de consenso de prova de trabalho (PoW, na sigla em inglês), que usa poder de processamento para resolver cálculos matemáticos *muito* complicados para assegurar que o hash criptográfico do bloco é válido.

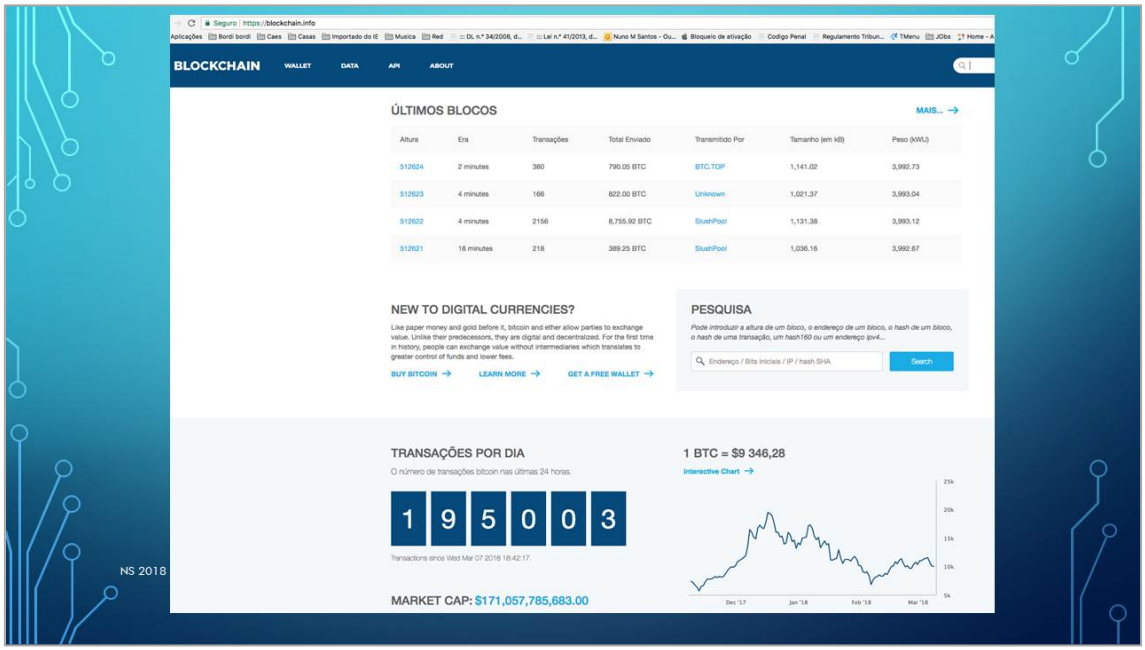
Quando alguém resolve a operação e consegue validar o bloco, recebe uma recompensa – as outras pessoas da rede também conseguem confirmar que o resultado é correto – porque as transações encriptadas aparecem num "diário de razão", e são publicas.

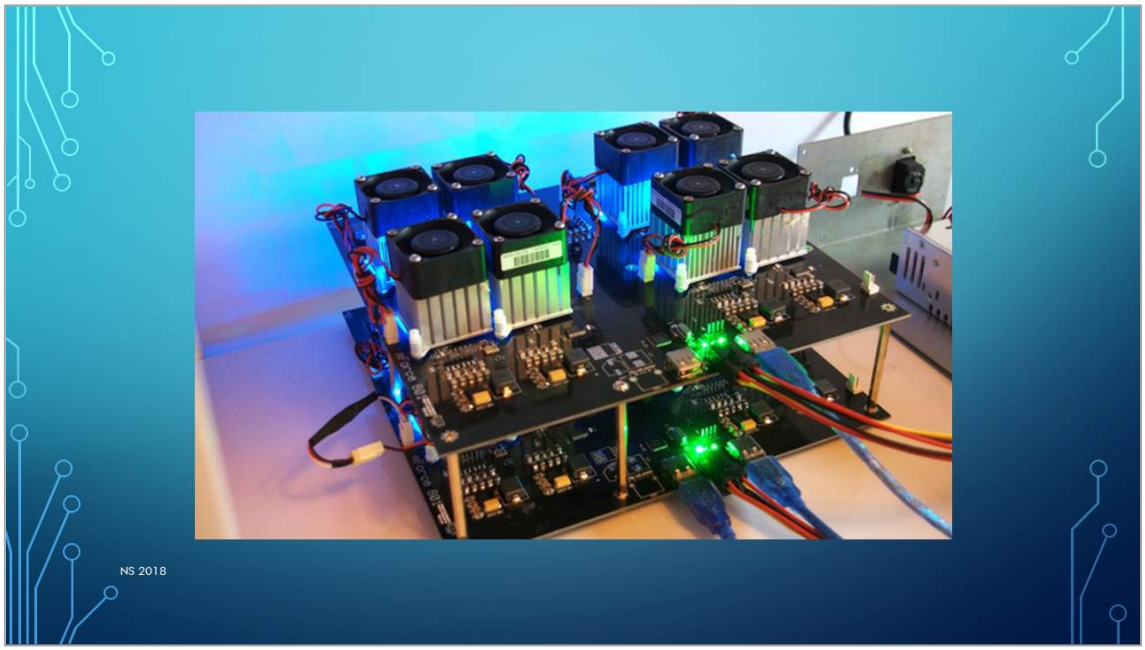
Portanto, na verdade, minar não é mais do que decifrar a criptografia de uma transação , a fim de a validar.

NS 2018

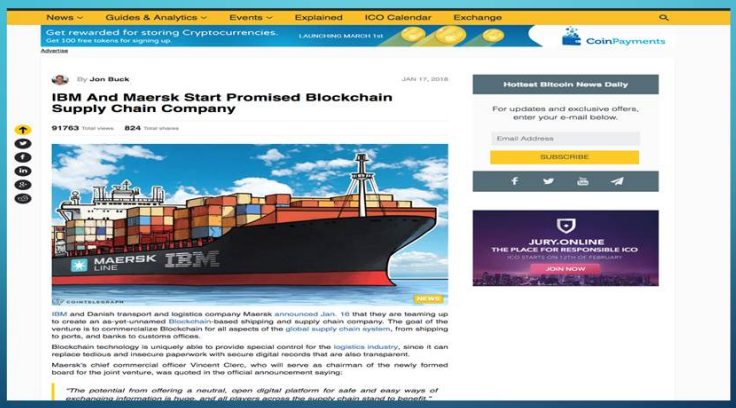

• No ambiente digital, os dados podem ser copiados, alterados e trocados. O **blockchain** foi a solução para eliminar as duas primeiras características: uma pessoa não pode gastar 1 BTC duas vezes ou dizer que enviou 10 BTC mas transferir apenas 0,01 BTC, por exemplo.
• Como funcionam os blocos ?
Bloco 1
Bloco 2
Bloco 3
CONTEÚDO
HASH 0
CONTEÚDO + HASH 0
HASH 1
CONTEÚDO + HASH 1
HASH 2
...
NS 2018
tecnoblog


EM ESQUEMA (AS TRANSAÇÕES):
individual 'transaction' events
BLOCKCHAIN
NEW BLOCK of transactions includes a security 'hash' of previous block.
BLOCKCHAIN new blocks are added approximately every 10 mins.
Multiple computer 'mining' servers check the validity of the blocks in the chain. The quickest to check the latest block, gets payment.
OR
successful transactions
BLOCK validated as 'honest' part of the chain.
REJECTED
NS 2018


BLOCKCHAIN
WALLET
DATA
API
ABOUT
ÚLTIMOS BLOCOS
MAIS...
NEW TO DIGITAL CURRENCIES?
PESQUISA
BUY BITCOIN
LEARN MORE
GET A FREE WALLET
Search
TRANSAÇÕES POR DIA
1 9 5 0 0 3
1 BTC = $9 346,28
Interactive Chart
MARKET CAP: $171,057,785,683.00
NS 2018


NS 2018

É LEGAL ?



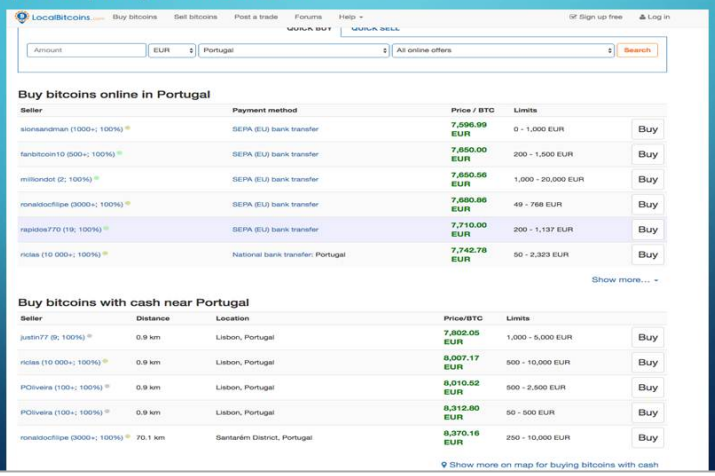
NS 2018

É LEGAL ?

NS 2018

É ILEGAL ? (NÃO !!!)

- Mas pode ser comprado, não só anonimamente, como com recurso a identidades falsas ou sequer sem qualquer comprovação de identidade.



NS 2018

É ILEGAL ? (NÃO !!!)

- Pode ser usado, e é-o frequentemente, para actividades criminosas, sejam pedidos de ransomware

É ILEGAL ? (NÃO !!!)

- Drogas, armas, documentos de identificação falsos, pornografia, serviços de hacking...

NS 2018

CRIME PERFEITO ?

NS 2018

CRIME PERFEITO ?

- Não existem crimes perfeitos, existem é crimes mal investigados... Sir Arthur Conan Doyle, Sherlock Holmes
- A luta contra a criminalidade organizada é muito difícil porque a criminalidade é organizada, e nós não – A. Amurri

NS 2018

FIM

NS 2018

Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/3n8x3702h/flash.html?locale=pt

6.

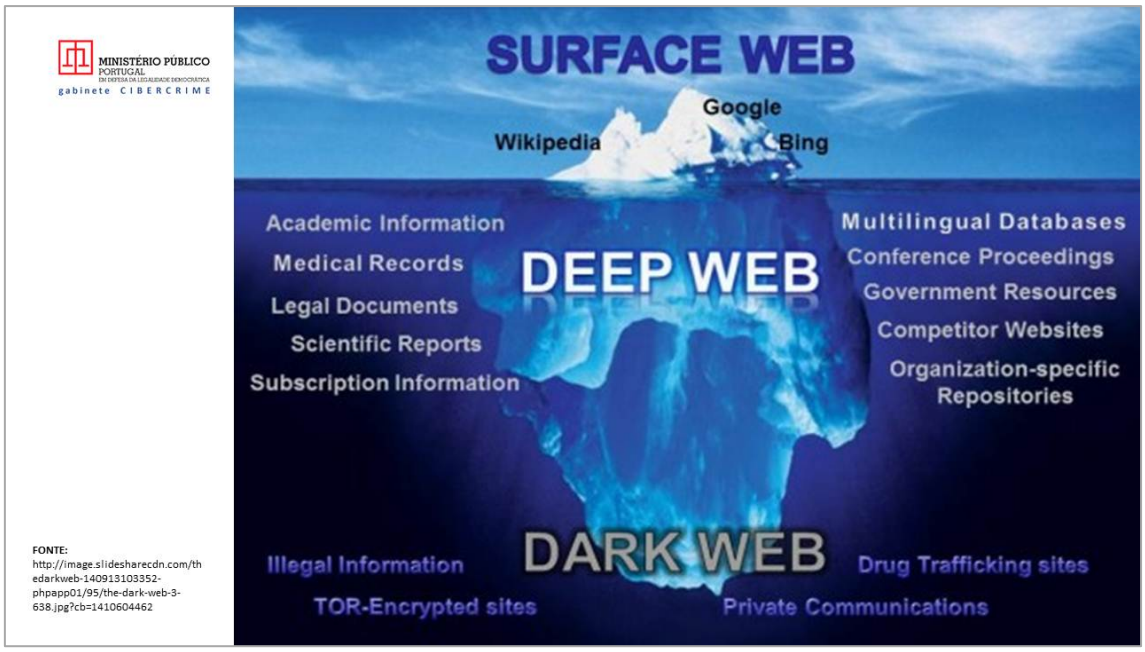
Dark web

Pedro Verdelho

CENTRO
DE ESTUDOS
JUDICIÁRIOS

DARK WEB[**]

Pedro Verdelho[*]



[**] Apresentação que serviu de base à conferência proferida pelo autor no CEJ / Porto, em 9 de Março de 2018.
[*] Procurador da República.

DARKWEB

- Pequenas redes *peer to peer*
- Que constituem grandes redes (TOR, Freenet, I2P)

TOR

- conjunto de servidores (geridos por voluntários)
- permitem comunicar em privacidade e segurança (como se fossem túneis, através da Internet)

DARKWEB

Permite

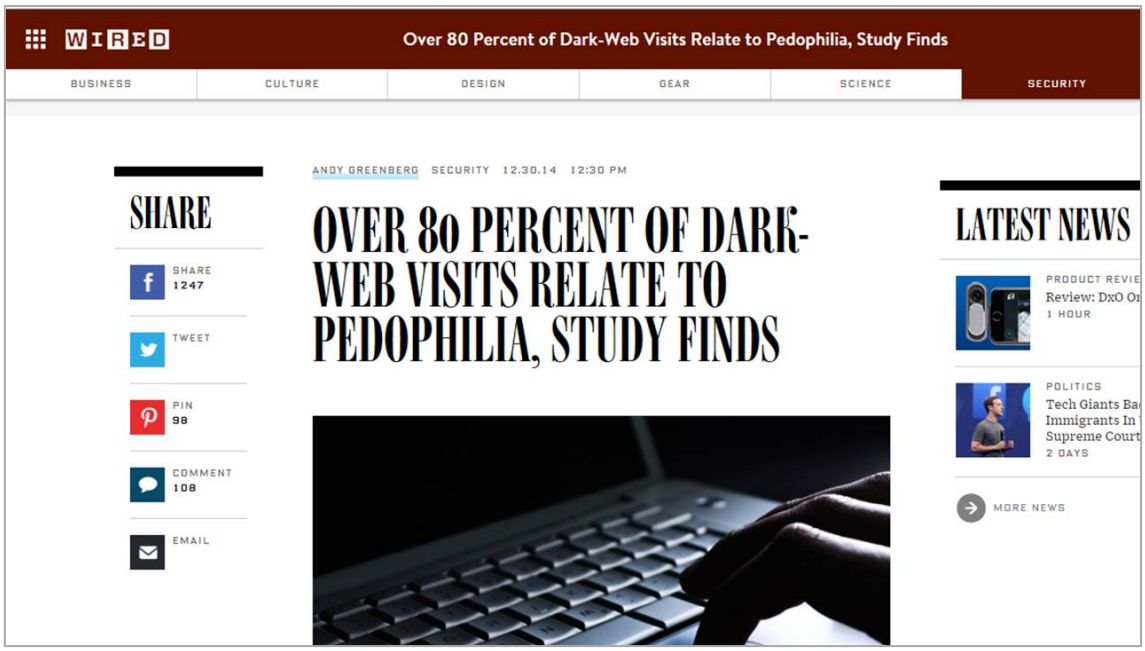
- manter websites em local escondido
- aceder a websites sem ser detetado
- comunicar com outrém anonimamente

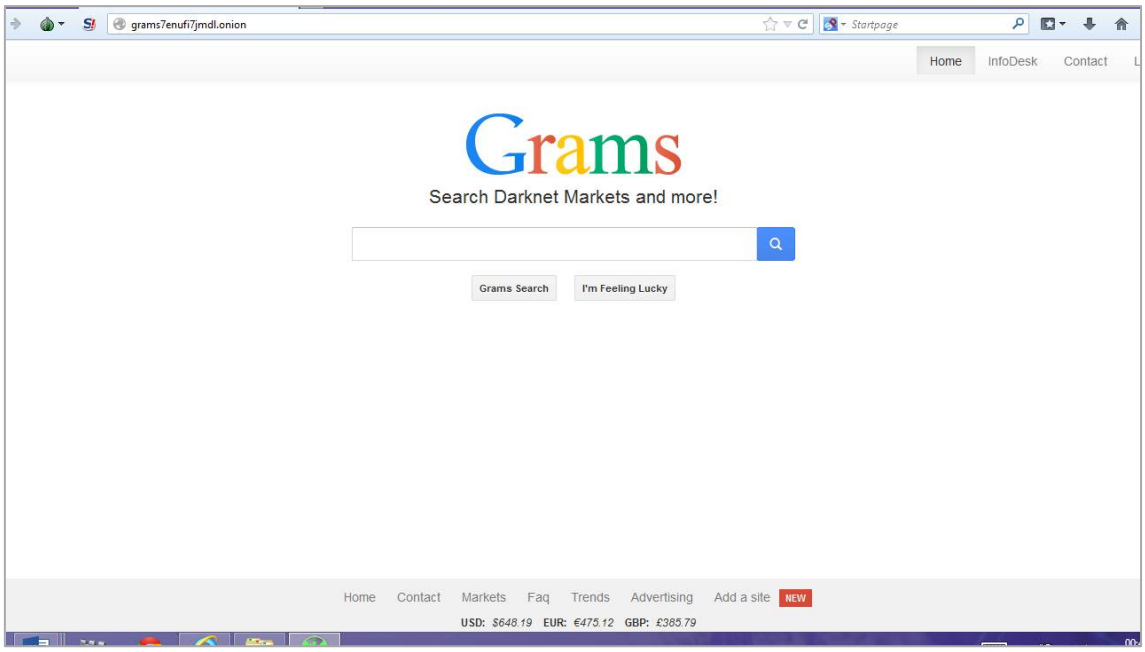
- **jornalistas** (para comunicar com informadores ou dissidentes politicos)
- Organizações de Direitos Humanos
- **empresas** (para preservar os seus segredos comerciais)
- **polícias** (em ações encobertas, para não sejam detetadas)

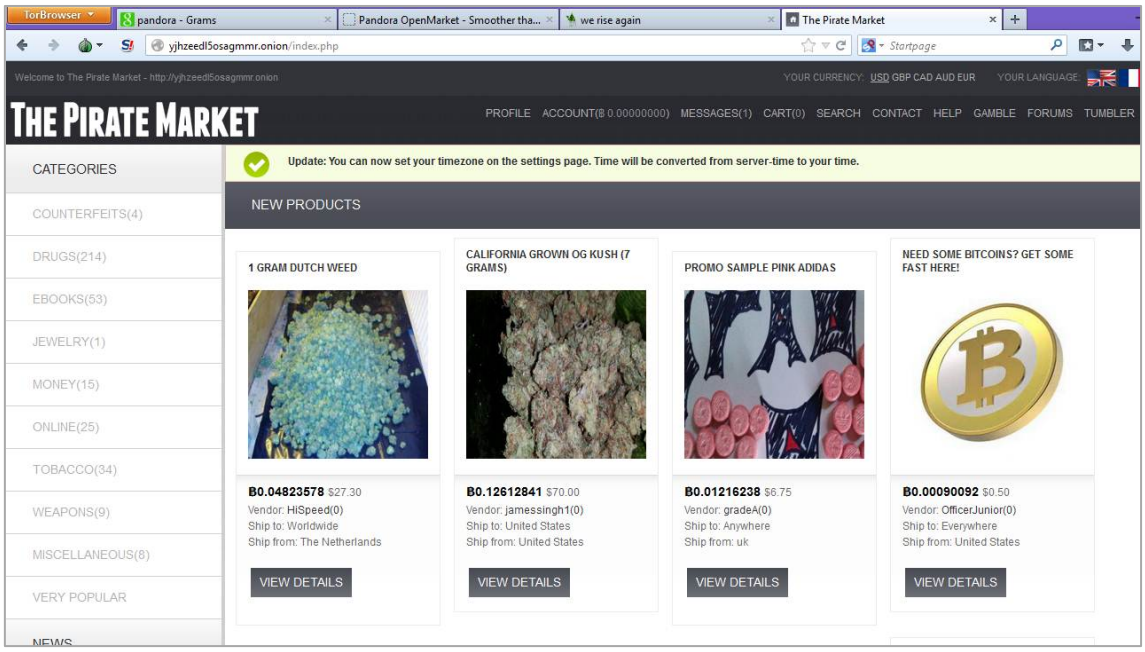
DARKWEB

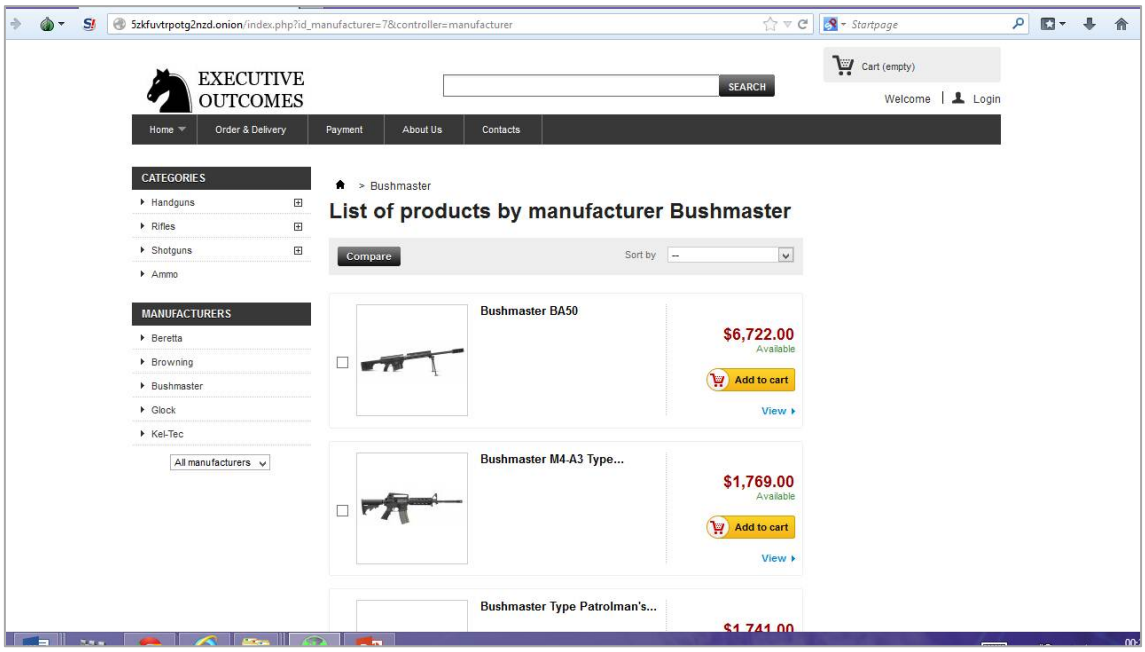
Para além disso….

Os mercados ilegais (droga, armas, pornografia infantil…)
O apoio ao terrorismo
Etc…




grams7enufi7jmdl.onion
Startpage
Home
InfoDesk
Contact
Grams
Search Darknet Markets and more!
Grams Search
I'm Feeling Lucky
Home
Contact
Markets
Faq
Trends
Advertising
Add a site
NEW
USD: $648.19 EUR: €475.12 GBP: £385.79


TorBrowser
pandora - Grams
Pandora OpenMarket - Smoother tha...
we rise again
The Pirate Market
yjhzeedl5osagmmr.onion/index.php
Startpage
Welcome to The Pirate Market - http://yjhzeedl5osagmmr.onion
YOUR CURRENCY: USD GBP CAD AUD EUR
YOUR LANGUAGE:
THE PIRATE MARKET
PROFILE ACCOUNT(฿ 0.00000000) MESSAGES(1) CART(0) SEARCH CONTACT HELP GAMBLE FORUMS TUMBLER
CATEGORIES
COUNTERFEITS(4)
DRUGS(214)
EBOOKS(53)
JEWELRY(1)
MONEY(15)
ONLINE(25)
TOBACCO(34)
WEAPONS(9)
MISCELLANEOUS(8)
VERY POPULAR
NEWS
Update: You can now set your timezone on the settings page. Time will be converted from server-time to your time.
NEW PRODUCTS
1 GRAM DUTCH WEED
B0.04823578 $27.30
Vendor: HiSpeed(0)
Ship to: Worldwide
Ship from: The Netherlands
VIEW DETAILS
CALIFORNIA GROWN OG KUSH (7 GRAMS)
B0.12612841 $70.00
Vendor: jamessingh1(0)
Ship to: United States
Ship from: United States
VIEW DETAILS
PROMO SAMPLE PINK ADIDAS
B0.01216238 $6.75
Vendor: gradeA(0)
Ship to: Anywhere
Ship from: uk
VIEW DETAILS
NEED SOME BITCOINS? GET SOME FAST HERE!
B0.00090092 $0.50
Vendor: OfficerJunior(0)
Ship to: Everywhere
Ship from: United States
VIEW DETAILS



localização desconhecida

anonimato

E isto importa?

- prova espalhada a nível global
  - localmente, em dispostivos
  - provavelmente também algures no mundo
  - necessidade de a obter fora das nossas fronteiras

- prova "em lado nenhum"

Questões difíceis:

local da prática do crime
qual a **lei penal** substantiva **aplicável**
Portugal é competente?
Código Penal aplica-se?

a **jurisdição nacional** é um **limite à investigação**
investigações transfronteiriças?
investigações na "cloud"?

MINISTÉRIO PÚBLICO PORTUGAL
gabinete CIBERCRIME

Lei nº 109/2009 - Lei do Cibercrime

Artigo 27.º

Aplicação no espaço da lei penal portuguesa e competência dos tribunais portugueses

1- (…) a lei penal portuguesa é aplicável a factos:

b) Cometidos **em benefício de pessoas colectivas** com sede em território português;

c) **Fisicamente praticados em território português**, ainda que visem sistemas informáticos localizados fora desse território; ou

d) Que **visem sistemas informáticos localizados em território português**, independentemente do local onde esses factos forem fisicamente praticados.

Questões difíceis:

local da prática do crime
qual a **lei penal** substantiva **aplicável**
Portugal é competente?
Código Penal aplica-se?

a **jurisdição nacional** é um **limite à investigação**
investigações transfronteiriças?
investigações na "cloud"?

convenção de Budapeste sobre cibercrime

Artigo 32º
Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público

Uma Parte pode, sem autorização de outra Parte:

(…)

b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, **se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados**, através deste sistema informático.

convenção de Budapeste sobre cibercrime

- aberta à assinatura a 21 de Novembro de 2001
- em vigor desde 2004 – para Portugal, desde 2009
- o primeiro (e único em vigor) tratado internacional sobre criminalidade contra sistemas de computadores, redes ou dados
- vocação universal
- cerca de 70 países

convenção de Budapeste sobre cibercrime

Artigo 32º
Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público

Uma Parte pode, sem autorização de outra Parte:

(…)

b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados situados no território de outra Parte, **se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados**, através deste sistema informático.

- localização dos dados?
- quem pode autorizar o acesso aos dados?

MINISTÉRIO PÚBLICO PORTUGAL
gabinete CIBERCRIME

Lei nº 109/2009 - Lei do Cibercrime

Artigo 15º
Pesquisa de dados informáticos

(...)

5 - Quando, no decurso de pesquisa, surgirem razões para crer que os **dados procurados se encontram noutro sistema informático**, ou numa parte diferente do sistema pesquisado, mas que tais dados são legitimamente acessíveis a partir do sistema inicial, **a pesquisa pode ser estendida** mediante autorização ou ordem da autoridade competente, nos termos dos nºs 1 e 2.

Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/qn2bsgg8p/flash.html?locale=pt

CENTRO
DE ESTUDOS
JUDICIÁRIOS

7.

A recolha de prova digital

Baltazar Rodrigues

CENTRO
DE ESTUDOS
JUDICIÁRIOS

A RECOLHA DE PROVA DIGITAL, AS FONTES ABERTAS (OSINT) E A "NOVA" INTERNET OF THINGS (IOT) OU INTERNET OF EVERYTHING (IOET)**

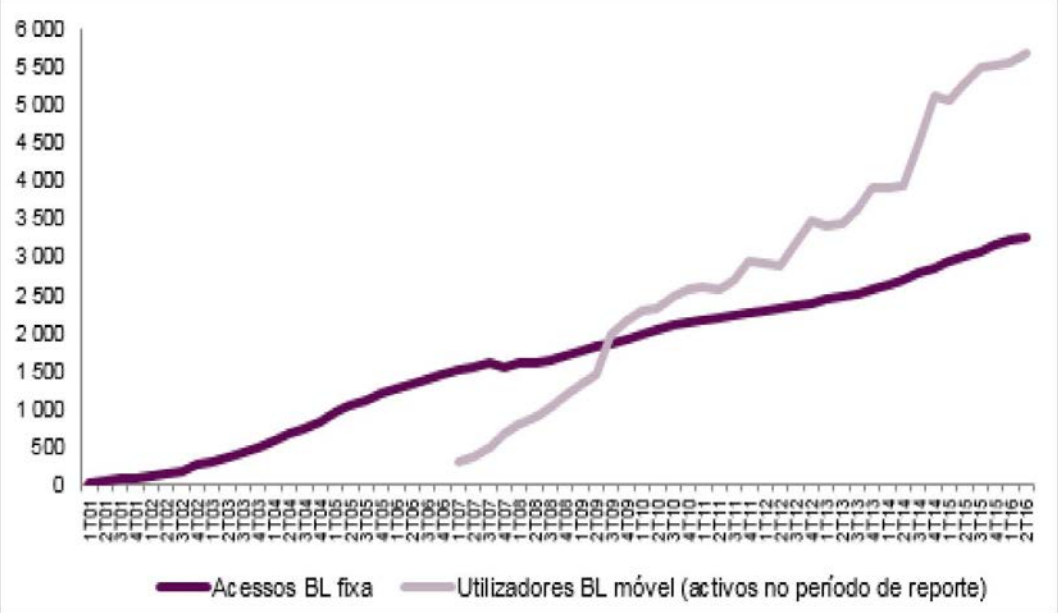
Baltazar Rodrigues*

** Apresentação que serviu de base à conferência proferida pelo autor no CEJ / Porto, em 10 de Fevereiro de 2017.
* Chefe do Gabinete de Tecnologia e Informática da Polícia Judiciária.

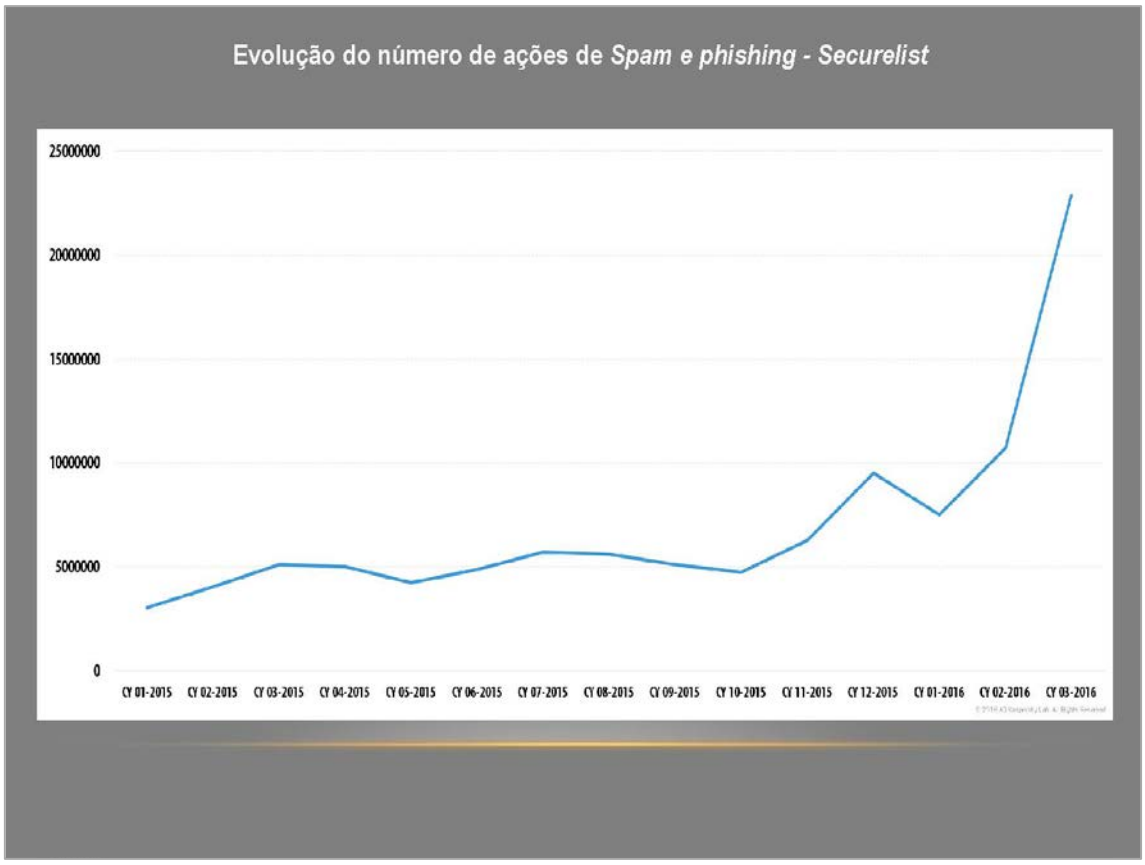
- Vantagens e perigos da informação disponibilizada na Internet (Redes Sociais), como fonte de recolha de prova digital.

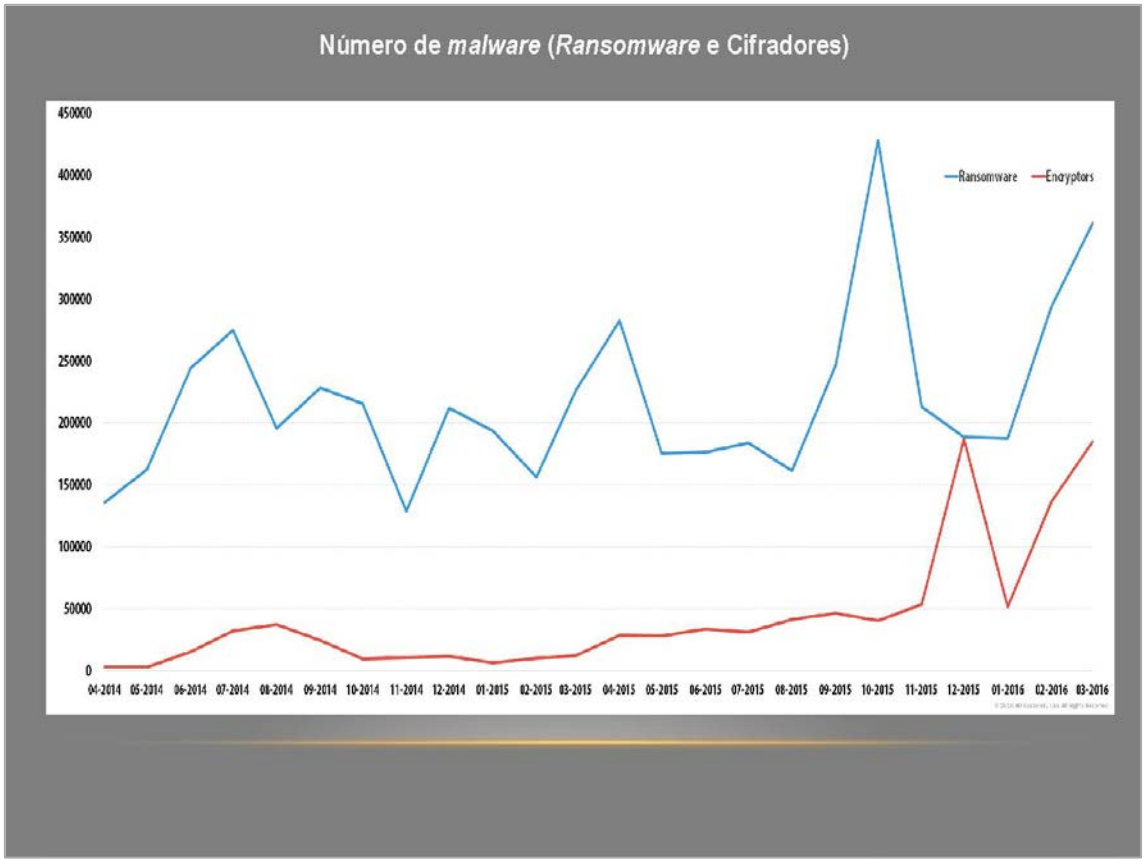
- Da Internet semântica para a Internet das coisas na recolha de informação para a investigação criminal e para o eficaz combate à crescente ameaça Ciberterrorista.

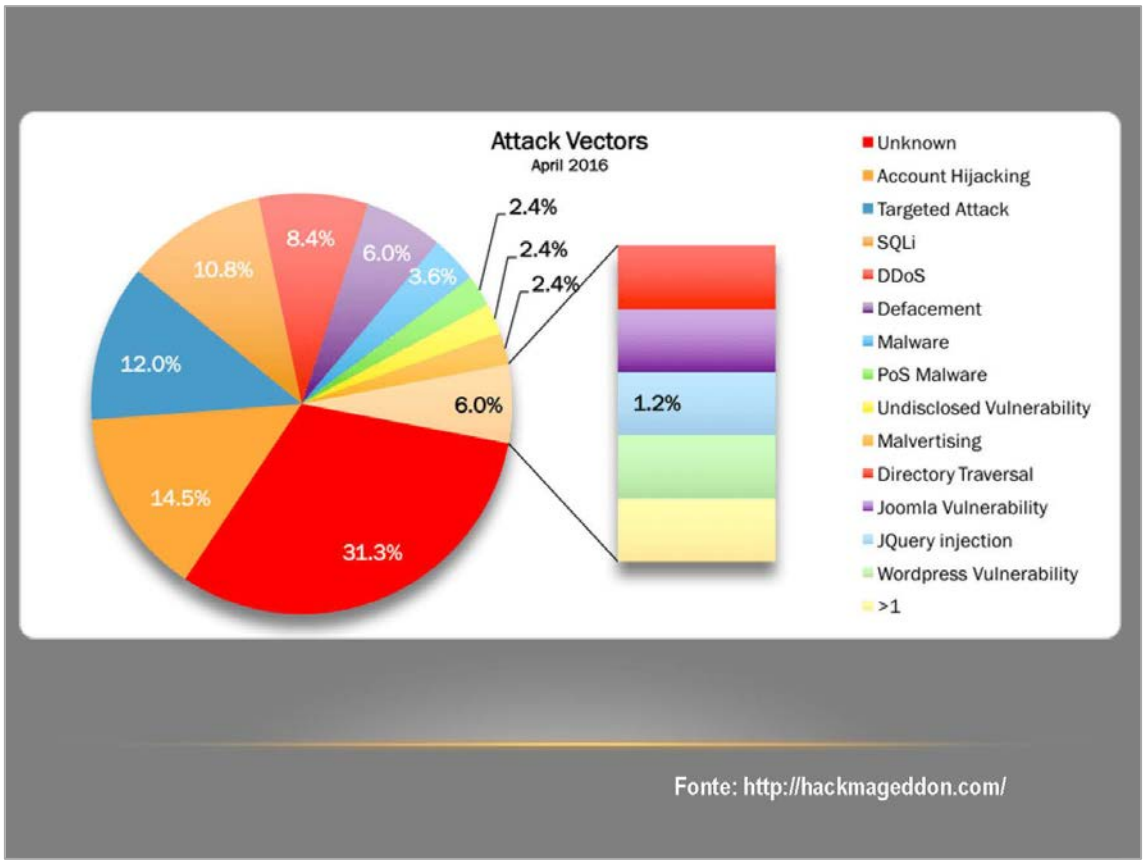
Evolução do número de clientes de banda larga



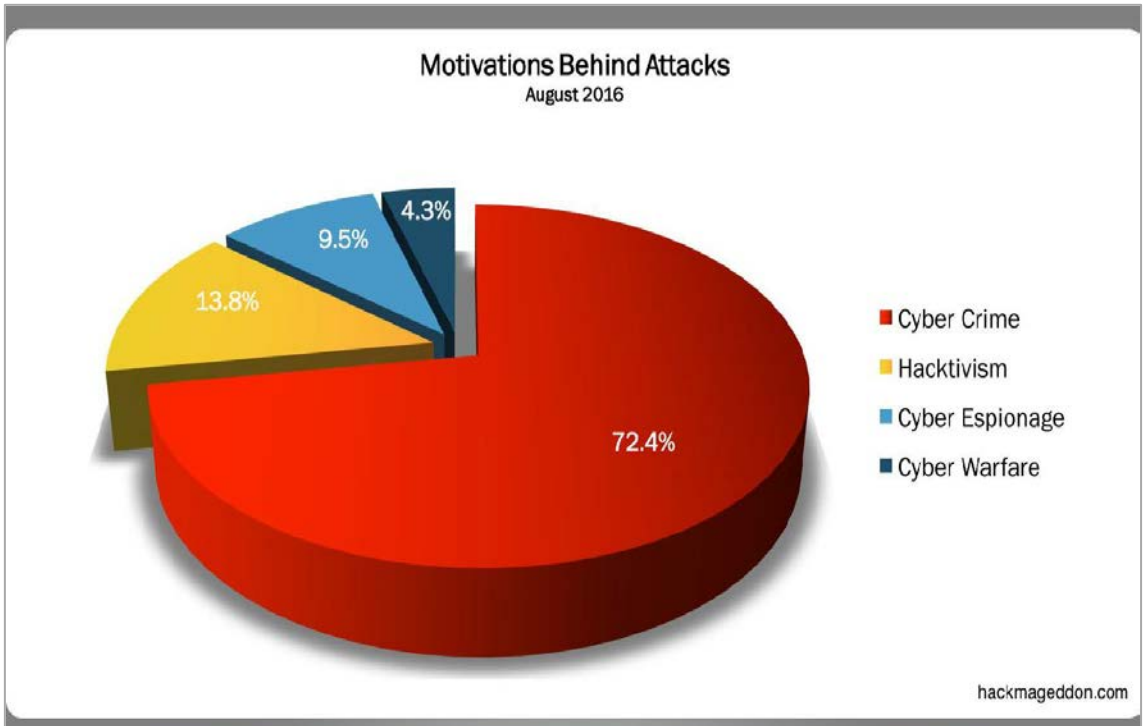
Fonte: ICP-ANACOM


Evolução do número de ações de Spam e phishing - Securelist
25000000
20000000
15000000
10000000
5000000
0
CY 01-2015
CY 02-2015
CY 03-2015
CY 04-2015
CY 05-2015
CY 06-2015
CY 07-2015
CY 08-2015
CY 09-2015
CY 10-2015
CY 11-2015
CY 12-2015
CY 01-2016
CY 02-2016
CY 03-2016

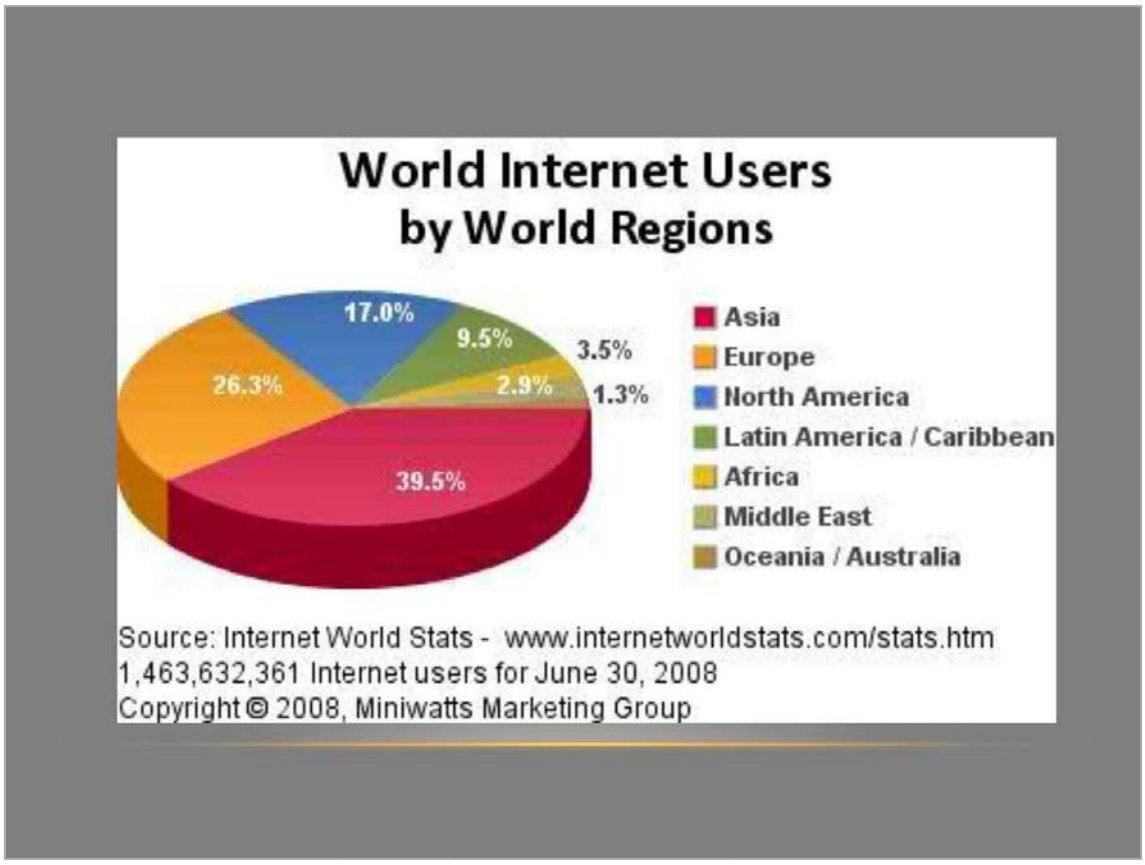

Número de malware (Ransomware e Cifradores)
450000
400000
350000
300000
250000
200000
150000
100000
50000
0
Ransomware
Encryptors
04-2014
05-2014
06-2014
07-2014
08-2014
09-2014
10-2014
11-2014
12-2014
01-2015
02-2015
03-2015
04-2015
05-2015
06-2015
07-2015
08-2015
09-2015
10-2015
11-2015
12-2015
01-2016
02-2016
03-2016

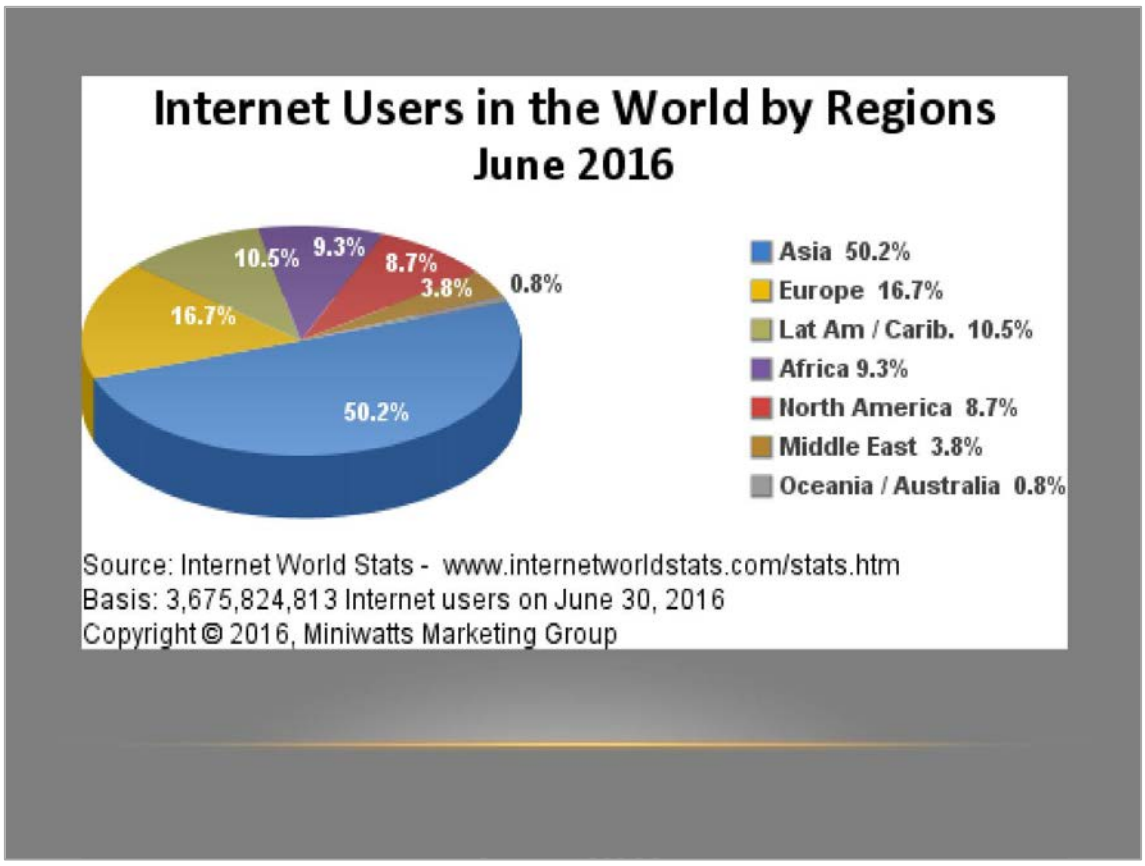


Fonte: http://hackmageddon.com/



Fonte: http://hackmageddon.com


World Internet Users
by World Regions
17.0%
9.5%
3.5%
26.3%
2.9%
1.3%
39.5%
Asia
Europe
North America
Latin America / Caribbean
Africa
Middle East
Oceania / Australia
Source: Internet World Stats - www.internetworldstats.com/stats.htm
1,463,632,361 Internet users for June 30, 2008
Copyright © 2008, Miniwatts Marketing Group


Internet Users in the World by Regions
June 2016
10.5%
9.3%
8.7%
3.8%
0.8%
16.7%
50.2%
Asia 50.2%
Europe 16.7%
Lat Am / Carib. 10.5%
Africa 9.3%
North America 8.7%
Middle East 3.8%
Oceania / Australia 0.8%
Source: Internet World Stats - www.internetworldstats.com/stats.htm
Basis: 3,675,824,813 Internet users on June 30, 2016
Copyright © 2016, Miniwatts Marketing Group

PHISHING – ESTATÍSTICAS 2015

	País	% de utilizadores
1	Brasil	26.73%
2	India	20.08%
3	Australia	19.37%
4	França	18.08%
5	EAU	17.13%
6	Canada	17.08%
7	Cazaquistão	16.09%
8	China	16.05%
9	Inglaterra	15.58%
10	Portugal	15.34%

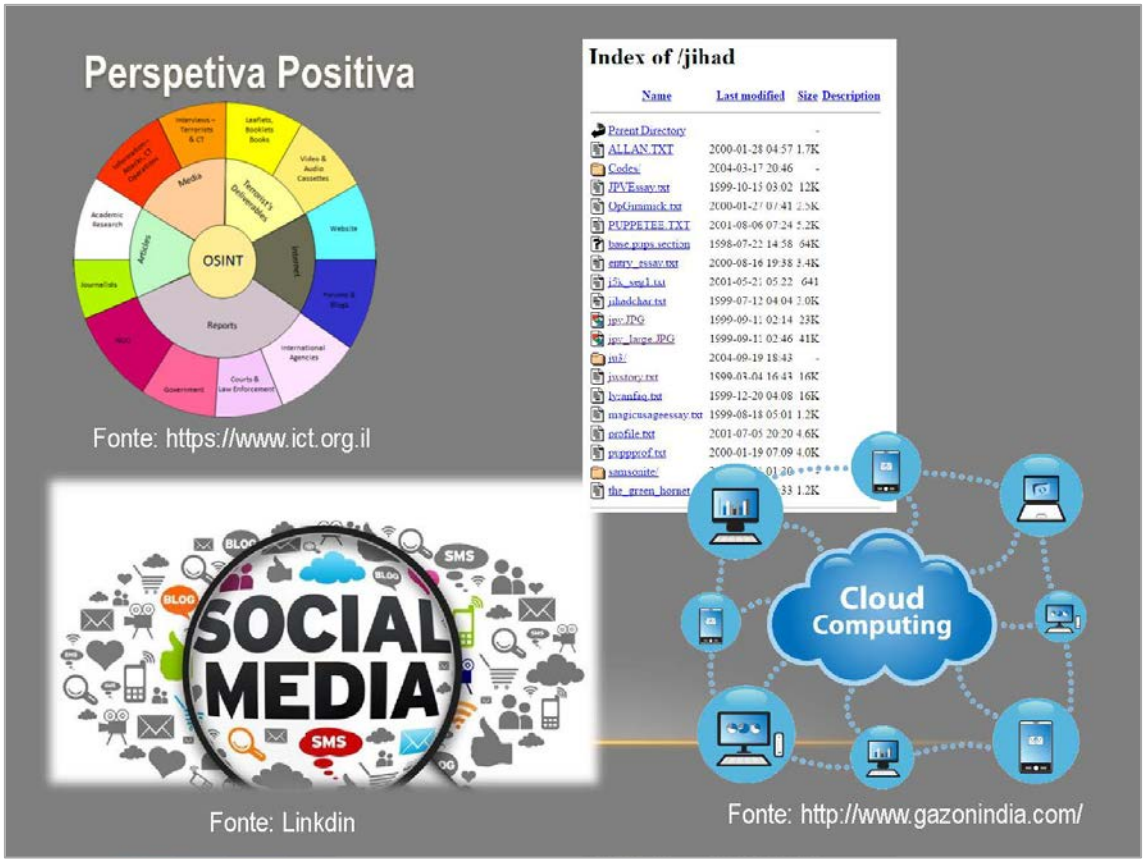
Fonte: https://securelist.com/

Maior Ameaça Somos Nós

Fonte: Dreamstime

Fonte: http://www.slideshare.net/marlos15


Perspetivas de visão:
Positiva
Negativa
Conformista
Indiferente


Perspetiva Positiva
OSINT
Media
Internet
Reports
Articles
Fonte: https://www.ict.org.il
Index of /jihad
Name
Last modified
Size
Description
SOCIAL MEDIA
SMS
BLOG
Fonte: Linkdin
Cloud Computing
Fonte: http://www.gazonindia.com/

A prova digital é como qualquer outra prova.

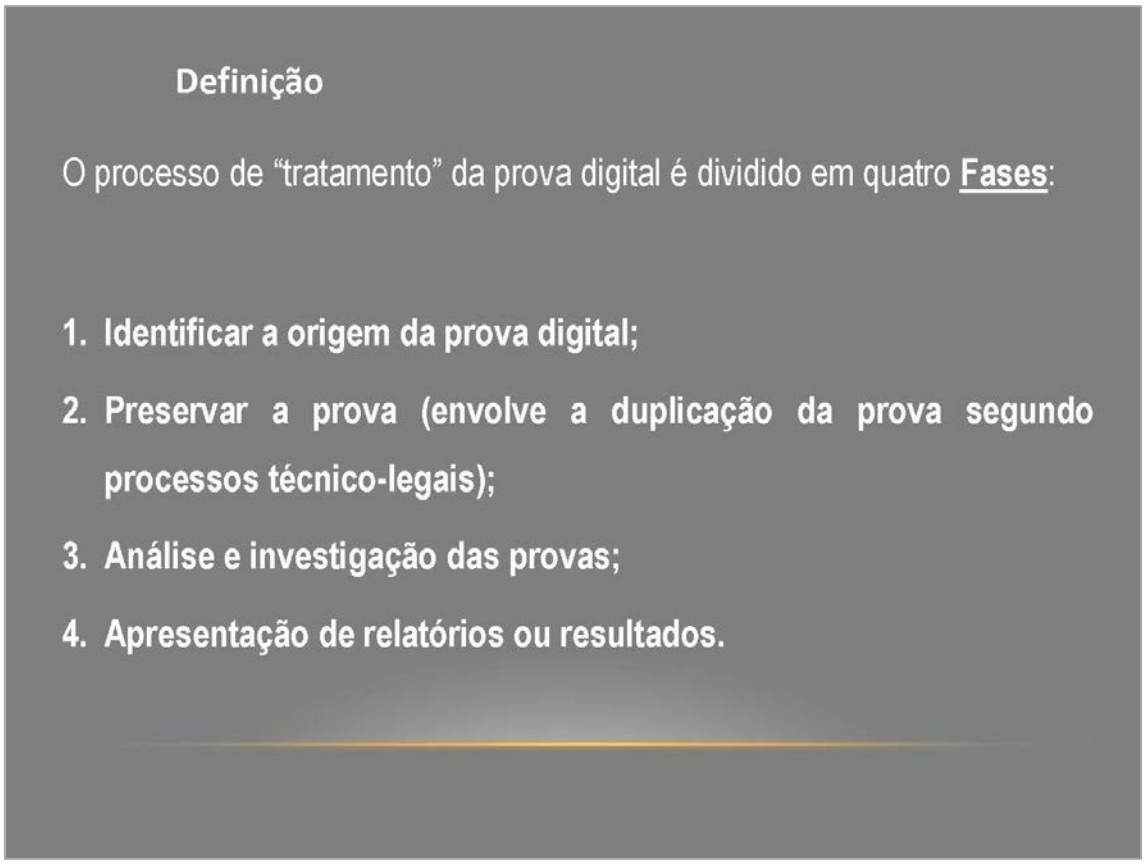
Deve ser:

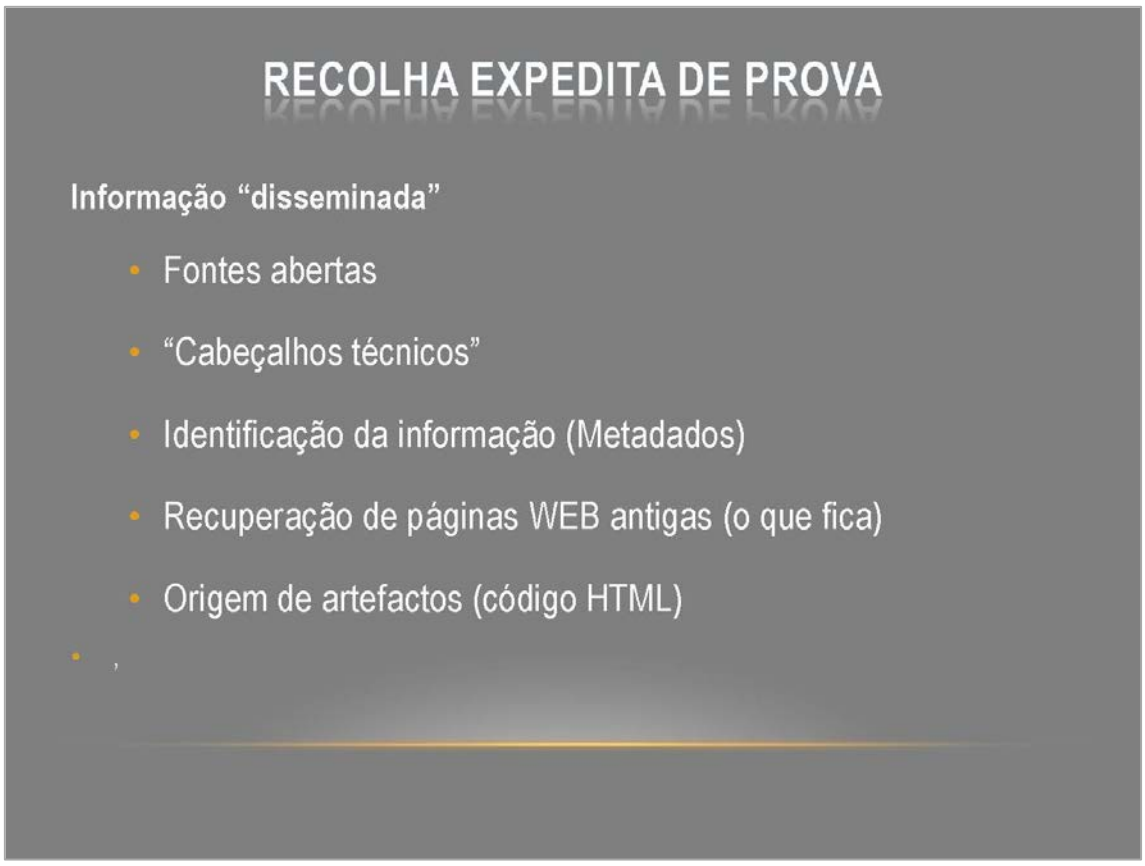
- **Admissível**
- **Autêntica**
- **Precisa**
- **Completa**

Prova Digital!

A prova digital é:

- Informação **armazenada, a ser transmitida, a ser recebida, ou a ser criada** em formatos ou meios digitais, cujo teor consubstancia prova.
- É **frágil e volátil**, de carácter fungível e temporário.


Definição
O processo de "tratamento" da prova digital é dividido em quatro Fases:
1. Identificar a origem da prova digital;
2. Preservar a prova (envolve a duplicação da prova segundo processos técnico-legais);
3. Análise e investigação das provas;
4. Apresentação de relatórios ou resultados.


RECOLHA EXPEDITA DE PROVA
Informação "disseminada"
Fontes abertas
"Cabeçalhos técnicos"
Identificação da informação (Metadados)
Recuperação de páginas WEB antigas (o que fica)
Origem de artefactos (código HTML)


CABEÇALHO TÉCNICO
http://www.ip2location.com/free/email-tracer
http://whatismyipaddress.com/trace-email

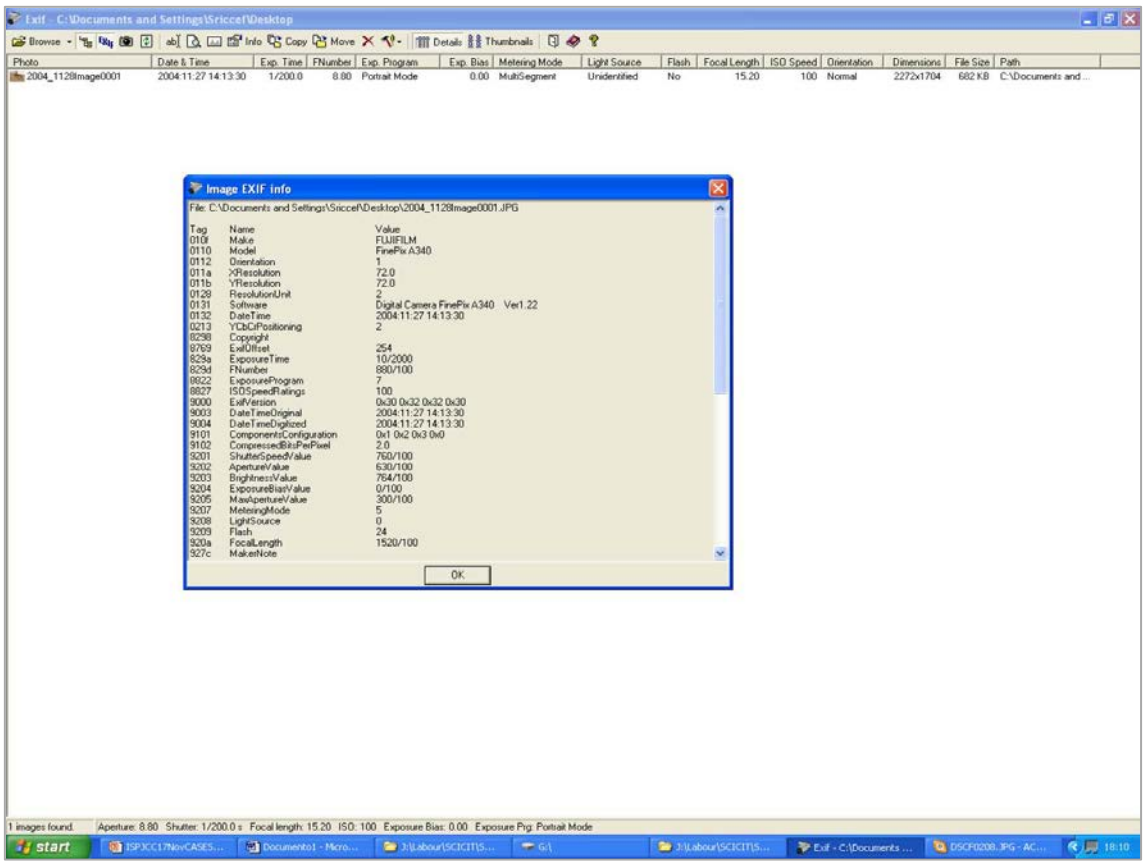


Image EXIF info

Recuperação de Páginas WEB

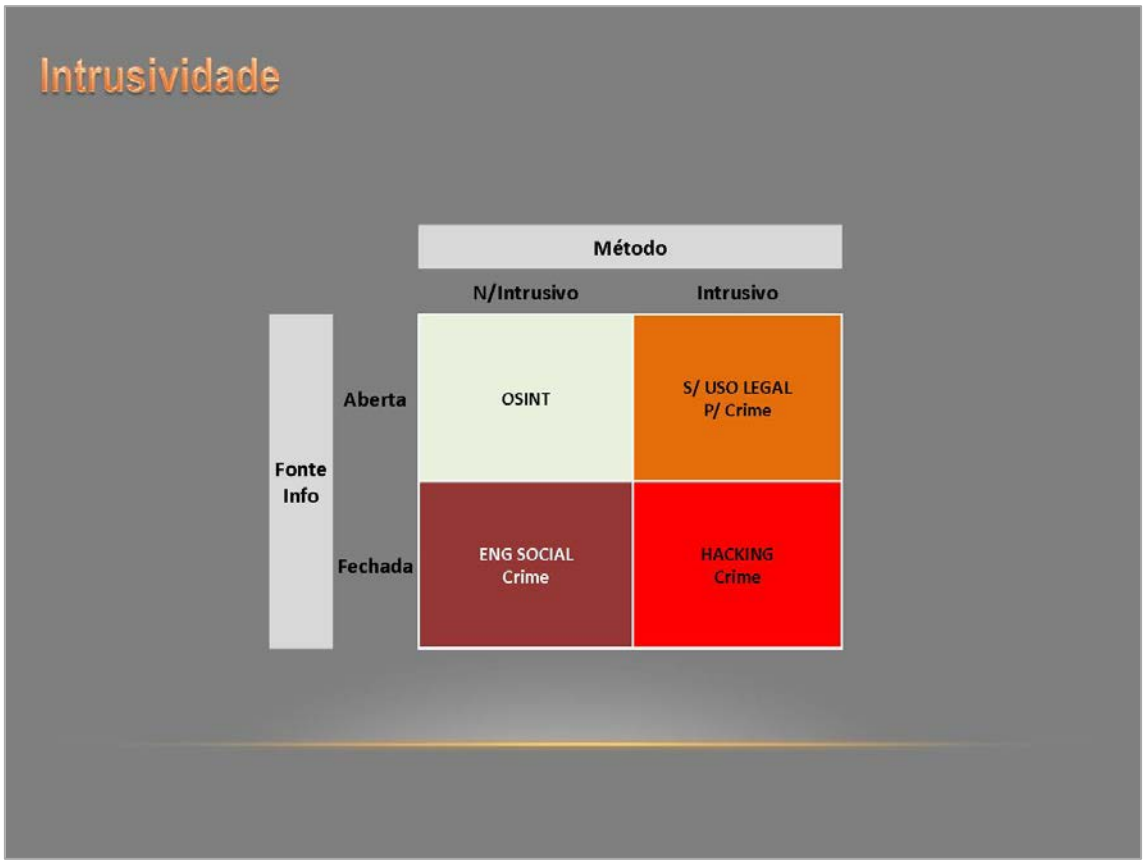
Google cache

(*wayback machine*)
http://archive.org/web/web.php

WAYBACK MACHINE – HISTORY OF INTERNET

Processamento automático de fontes na web

- Crawlers
- Analytics
- Pesquisa nas redes sociais (Facebook,Twitter,YouTube, Instagram, FourSquare, ...)
- Pegada digital, anonimização, IP como *internet id*
- API
- Darkweb


Intrusividade
Método
N/Intrusivo
Intrusivo
Fonte Info
Aberta
Fechada
OSINT
S/ USO LEGAL P/ Crime
ENG SOCIAL Crime
HACKING Crime


A caixa de pesquisa no gráfico social
Type to search for people, places and things
http://www.inteltechniques.com/index.html
OSINT Training by Michael Bazzell
Home
Blog
Forum
Online Training
Live Training
Experience
Online Resources
Books
Contact
Custom Facebook Tools
Buy the Book: Open Source Intelligence Techniques
Updated 05/29/2015 at IntelTechniques.com
Free Tutorial Video and OSINT Newsletter LINK
Email Address
Cell Number
Facebook Screen Name
(Account by Email)
(Account by Cell Phone)
(Displays User Number)
Facebook User Number
(Displays Places Visited)
(Displays Places Liked)
(Displays Pages Liked)
(Displays Photos By User)
(Displays Photos Liked)
(Displays Photos Of -Tagged)
(Displays Photo Comments)

Twitter API

Ferramentas disponíveis

1.http://localhost Custom Twitter Tools (Twitter Search Options)
2.http://twitter.com/search-advanced Advanced Twitter Search (Custom Options)
3.https://twitter.com/search?q=geocode%3A38.952451%2C-90.195011%2C1km&src=typd Twitter Location Search (Enter GPS)
4.https://twitter.com/search?q=Bomb%20since:2012-01-01%20until:2012-01-02 Twitter Time Search (Enter Dates and Keyword)
5.http://topsy.com Topsy (Occasional Deleted Posts)
6.http://www.allmytweets.net/index.php All My Tweets (Entire Archive)
7.http://mentionmapp.com/ MentionMapp (Closest Friends)
8.https://discover.twitter.com/first-tweet First Tweet (Display Date Joining Twitter)
9.http://ctrlq.org/first/ First Tweet (Display the first Tweet of many ReTweets)
10.http://tweettunnel.info/firstpre.php TweetTunnel (Display Chronological Friends)
11.http://www.conweets.com/ ConWeets (Isolate Twitter Conversations)
12.http://gwittr.com Gwittr (Twitter Profile Data)
13.http://foller.me/ FollerMe (Twitter Analytics)

Twitter API

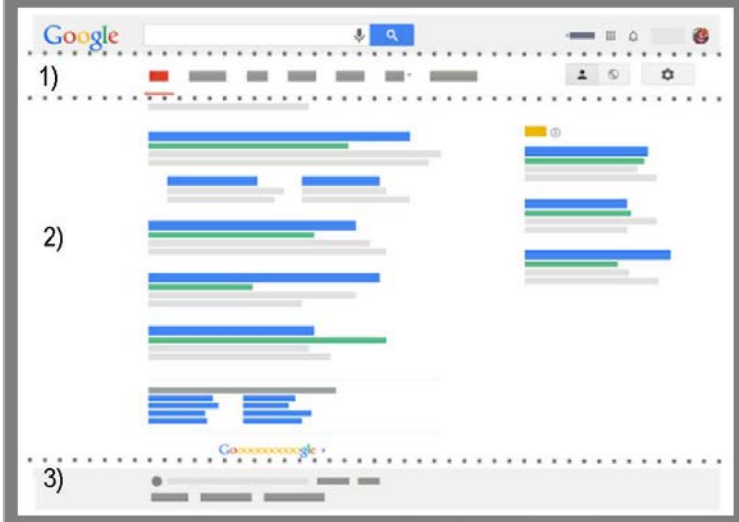
Ferramentas disponíveis

14.http://twtrland.com/ TwtrLand (Twitter Profile Data)
15.http://nearbytweets.com/ Nearby Tweets (Posts by Location)
16.http://www.geochirp.com/ GeoChirp (Twitter Mapped Data)
17.http://geosocialfootprint.com/ GeoSocial Footprint (Mapped Posts)
18.http://www.tweetpaths.com/maps TweetPaths (Mapped Tweets by User)
19.http://app.teachingprivacy.com/ TeachingPrivacy (Mapped Tweets by User)
20.https://app.echosec.net/ EchoSec (Mapped Tweets)
21.http://www.coeverywhere.com/ CoEverywhere (Mapped Posts)
22.http://nowtweets.com/ Now Tweets (Live by Location)
23.http://mapd.csail.mit.edu/tweetmap/ MIT Map (Mapped Tweets)
24.http://worldmap.harvard.edu/tweetmap/ Harvard Map (Mapped Tweets)
25.http://onemilliontweetmap.com/ OMTM (Mapped Tweets)
26.https://web.tweetdeck.com/ TweetDeck (Real Time Monitoring)
27.https://hootsuite.com/feed/TEST+Search?pfilter= HootSuite (Live Data Stream)
28.http://twitterfall.com Twitterfall (Real Time Search)


Twitter API
Ferramentas disponíveis
29.http://twitter.com/#!/who_to_follow Twitter Name Search (Twitter Name Search)
30.http://www.twellow.com/ Twellow (Twitter Search)
31.http://www.twitonomy.com/ Twitonomy (Twitter Analytics)
32.http://www.socialbakers.com/twitter/fakefollowercheck/ Fake Followers (Identifies Fake Accounts)
33.http://fakers.statuspeople.com/ Status People (Identifies Fake Accounts)
34.http://tagwalk.com/ TagWalk (Twitter Account Data)
35.http://twitalyzer.com/ Twitalyzer (Twitter Account Data)
36.http://tweetreach.com/ TweetReach (ID ReTweets)
37.http://twicsy.com/ Twicsy (Live Twitter Photos)
38.http://twitcaps.com/ TwitCaps (Twitter Photo Search)
39.http://twitpic.com/ TwitPic (Twitter Photos)
40.http://www.sleepingtime.org/ SleepingTime (Twitter Sleep Schedule)
41.http://backtweets.com/ BackTweets (Search Links Posted)
42.http://followerwonk.com/analyze Followerwonk (Analyze Associates)


Twitter API
Ferramentas disponíveis
43.http://www.tweepsect.com/ TweepSect (Analyze Associates)
44.http://followerwonk.com/compare Followerwonk (Analyze Users)
45.http://followerwonk.com/bio/?q=construction&l=nepal Followerwonk (Locate Profiles by Interest)
46.https://tweettopicexplorer.neoformix.com Tweet (Topic Explorer)
47.http://keyhole.com Keyhole (Real Time Tracking)
48.http://undetweetable.com (Historic Deleted Tweets)
49.https://twitter.com/i/directory/profiles/ Twitter Directory (Users by Name)
50.http://tweetalarm.com/ Tweet Alarm (Alerts from Twitter)

Google



1) Filtros de resultados e Ferramentas de pesquisa Resultados públicos Resultados privados Configurações

2) Resultados da pesquisa e anúncios

3) Local

Google

Funcionalidades

- Pesquisa Avançada : https://www.google.pt/advanced_search
- Histórico de Pesquisas: https://history.google.com/history/
- Pesquisa de Imagens: https://images.google.com/
- Calculadora e conversor (na língua inglesa): direta na barra de pesquisa
- Pesquisa de Vídeos: https://video.google.com/
- Pesquisa de Livros: https://books.google.com/

Google

Funcionalidades

- Tradutor: http://translate.google.com/
- Académico: http://scholar.google.pt/
- Notícias: http://news.google.com/
- Finanças: http://finance.google.com/
- Tendências: http://trends.google.com/
- Alertas: https://www.google.com/alerts
- Ngrams: https://books.google.com/ngrams/
- Google Drive: https://drive.google.com/

Google hack

Possibilidades

- Pesquisas mais assertivas.
- Menos falsos positivos.
- Acesso a dispositivos ligados à rede configurados por omissão.
- Acesso a conteúdos não disponíveis por pesquisa normal.
- Etc.

Google hack

utilização

Admite o uso de GREP(***g****lobally search a* ***r****egular* ***e****xpression* and ***p****rint*)

"password" site:www.pgr.pt

“contrato” filetype:pdf

“contrato” filetype:pdf site:asficpj.org

“PGR” AND “contrato” filetype:pdf

"vou-te matar" filetype:doc

"vou-te matar" filetype:docx Etc.

Sites de referência

http://www.inteltechniques.com/index.html

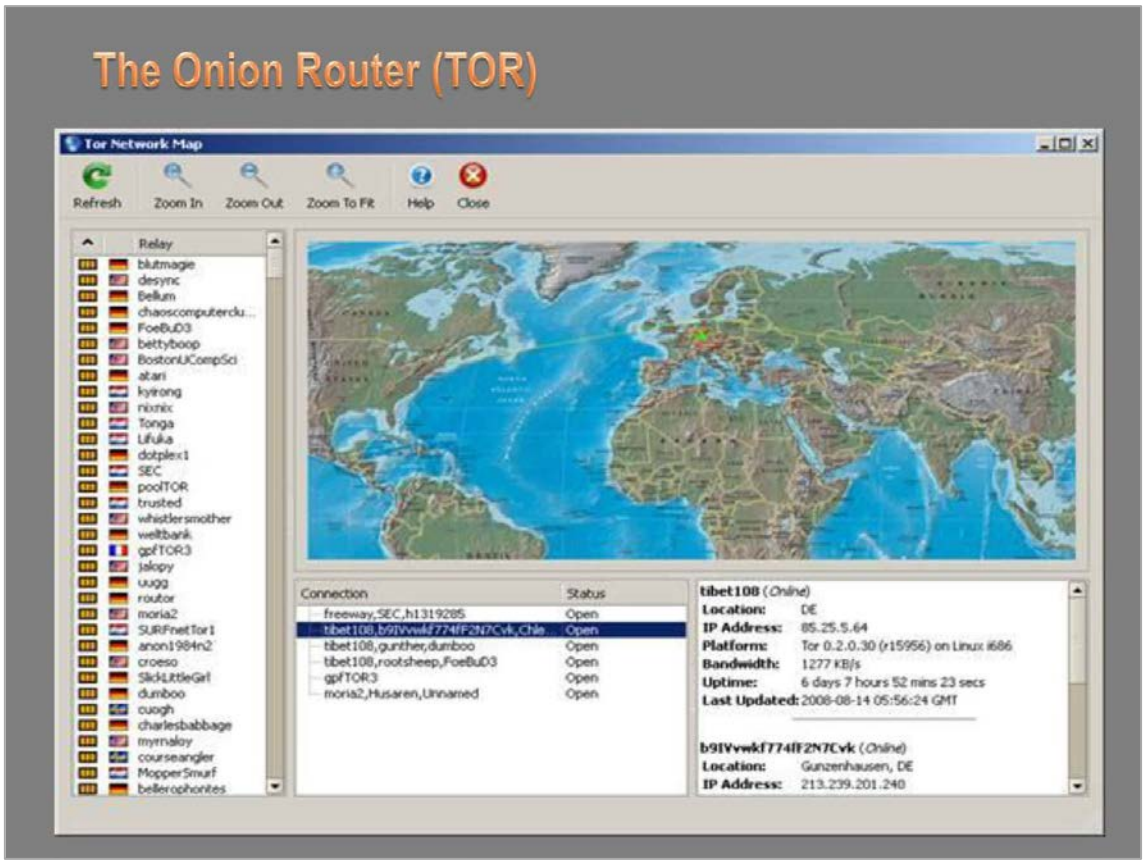
http://rr.reuser.biz/

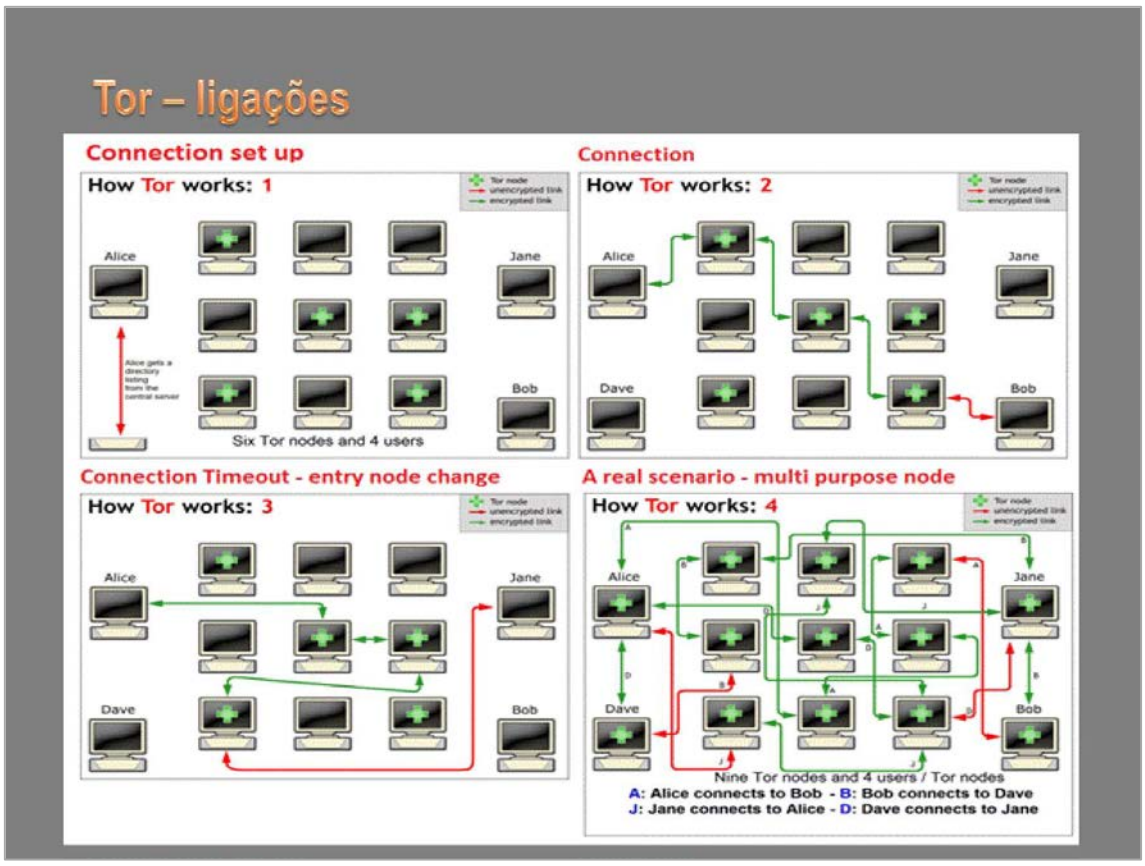
Outras Fontes abertas

Utilidades

- Whois - Central Ops
- Whois -Domain Tools
- Pipl.com
- Sync.Me
- Email Header Analyzer - WhatIsMyIP.com
- E-Mail Header Analyzer - Gaijin.at

DEEP WEB E DARK WEB

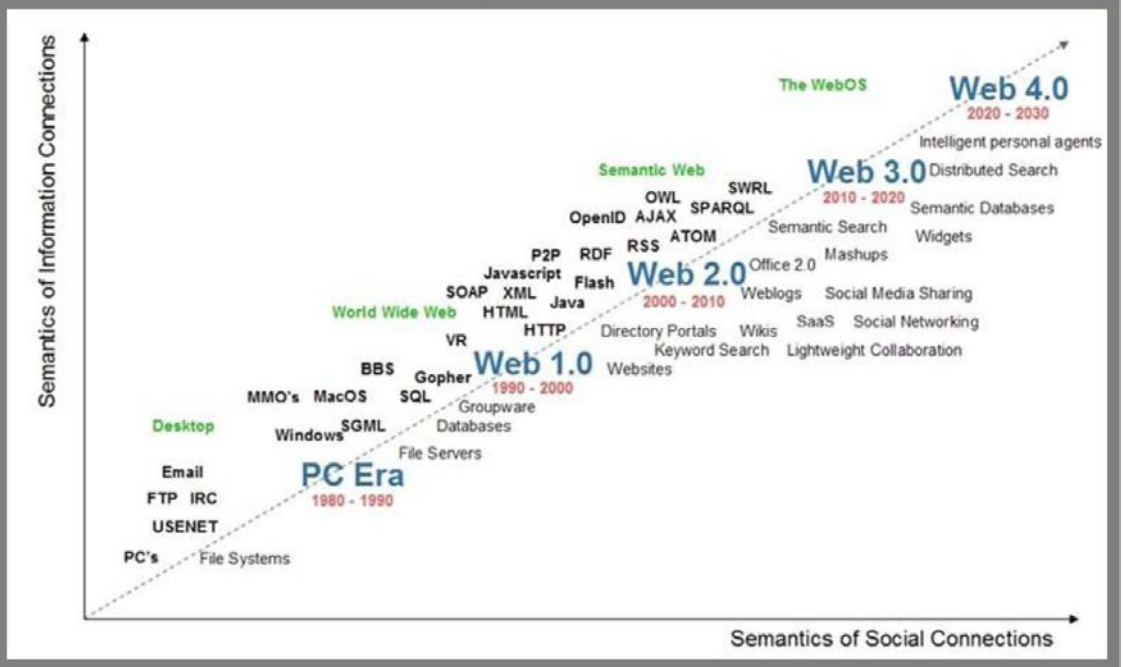

The Onion Router (TOR)
Tor Network Map
Refresh
Zoom In
Zoom Out
Zoom To Fit
Help
Close
Relay
Connection
Status
tibet108 (Online)
Location: DE
IP Address: 85.25.5.64
Platform: Tor 0.2.0.30 (r15956) on Linux i686
Bandwidth: 1277 KB/s
Uptime: 6 days 7 hours 52 mins 23 secs
Last Updated: 2008-08-14 05:56:24 GMT
b9IVvwkf774fF2N7Cvk (Online)
Location: Gunzenhausen, DE
IP Address: 213.239.201.240


Tor – ligações
Connection set up
How Tor works: 1
Alice
Jane
Bob
Six Tor nodes and 4 users
Connection
How Tor works: 2
Alice
Jane
Dave
Bob
Connection Timeout - entry node change
How Tor works: 3
Alice
Jane
Dave
Bob
A real scenario - multi purpose node
How Tor works: 4
Alice
Jane
Dave
Bob
Nine Tor nodes and 4 users / Tor nodes
A: Alice connects to Bob - B: Bob connects to Dave
J: Jane connects to Alice - D: Dave connects to Jane

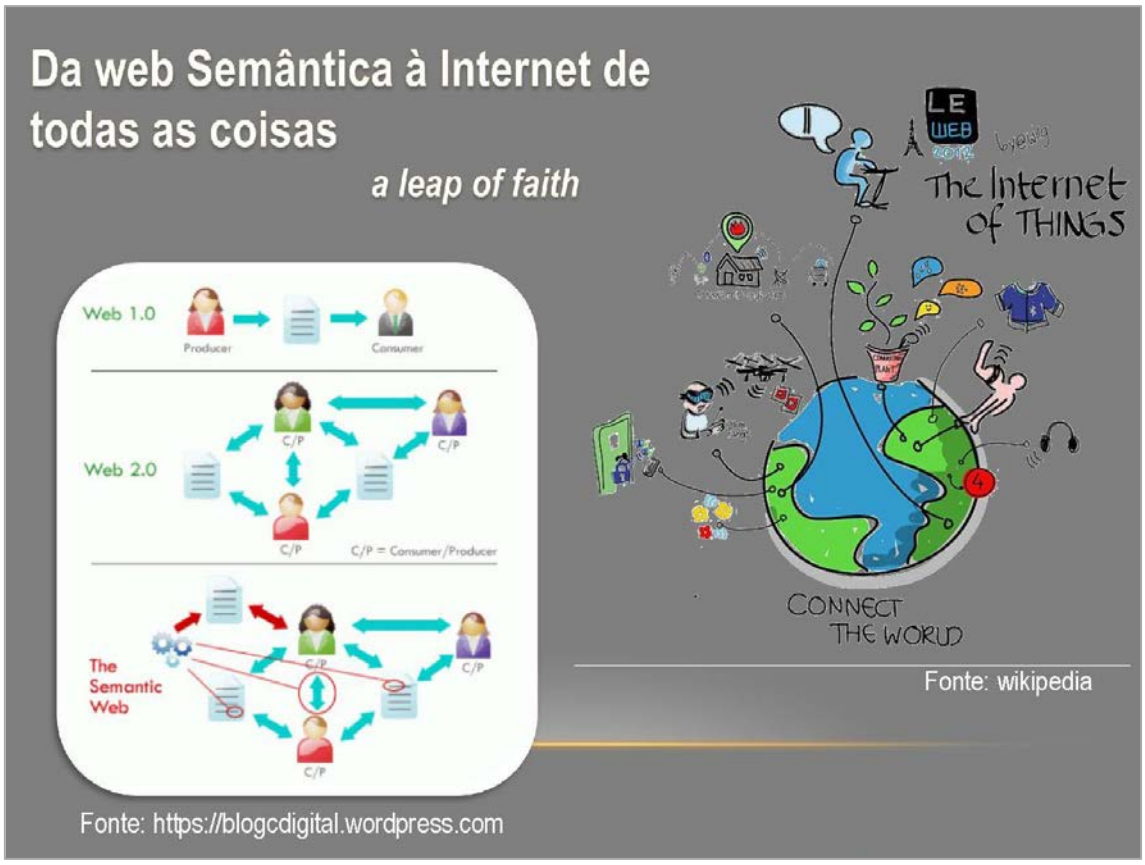
Lista de MarketPlaces , Dark Net Markets (Tor & I2P)

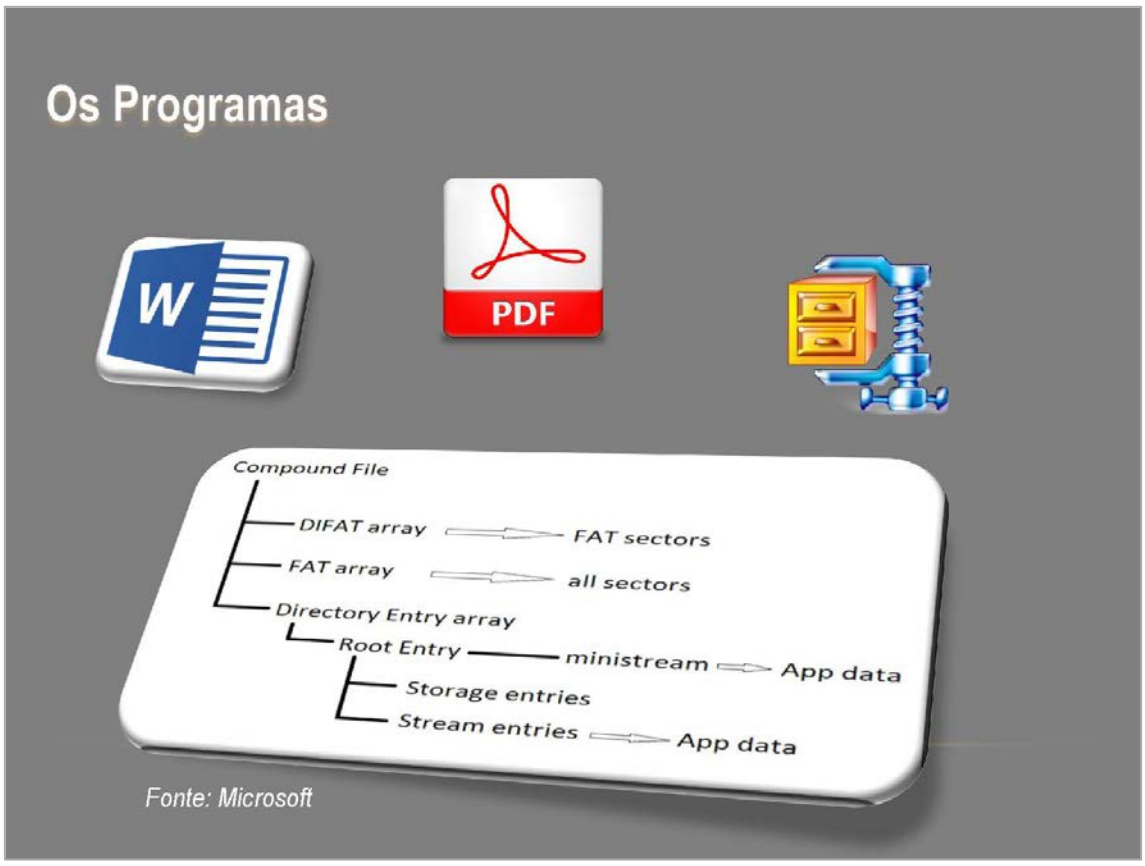
https://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/

Evolução da Web



Fonte: http://patra-wanz.exteen.com/


Da web Semântica à Internet de todas as coisas
a leap of faith
Web 1.0
Producer
Consumer
Web 2.0
C/P
C/P = Consumer/Producer
The Semantic Web
LE WEB 2014
The Internet of THINGS
CONNECT THE WORLD
Fonte: wikipedia
Fonte: https://blogcdigital.wordpress.com


Os Programas
W
PDF
Compound File
DIFAT array
FAT sectors
FAT array
all sectors
Directory Entry array
Root Entry
ministream
App data
Storage entries
Stream entries
App data
Fonte: Microsoft

Ciberterrorismo,

Forma de terrorismo que utiliza as tecnologias de informação para intimidar, coagir ou para causar danos a grupos sociais com fins político-religiosos.

Stuxnet - 2010

2007 - Estônia

2014 – Sony Pictures

Fonte: http://uterotremulo.blogspot.pt/

CIBERTERRORISMO

Cuidados

-Sistemas com total interligação com a Internet;

-Novos serviços e funcionalidades (**Bring Your Own Device (BYOD)** e **Internet of Everything (IoE)**);

- Novas vulnerabilidades e ferramentas de ataque.

Vídeo da apresentação

➔ https://educast.fccn.pt/vod/clips/2add7f7nfi/flash.html?locale=pt

Título:
O domínio do imaterial: prova digital, cibercrime e a tutela penal de direitos intelectuais

Ano de Publicação: 2018

ISBN: 978-989-8908-08-7

Série: Formação Contínua

Edição: Centro de Estudos Judiciários

Largo do Limoeiro

1149-048 Lisboa

cej@mail.cej.mj.pt