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.

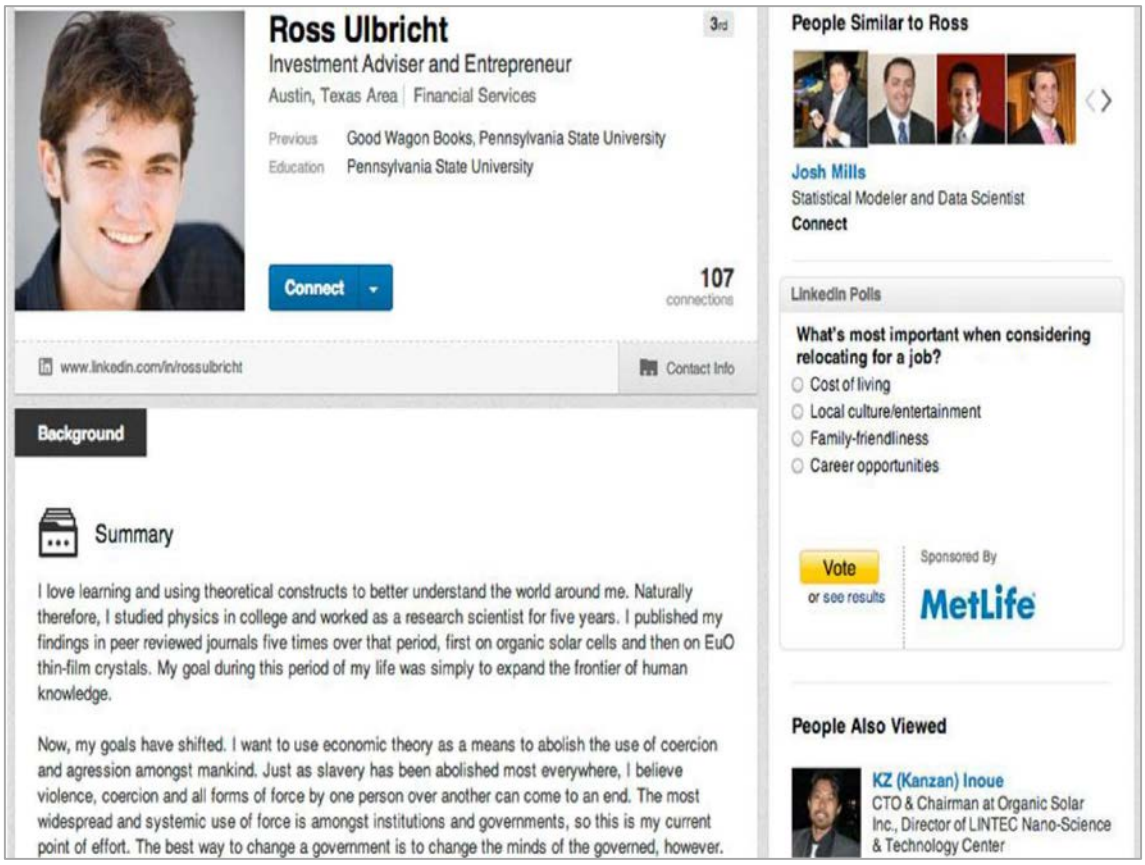
Métodos ocultos de investigação criminal em ambiente digital

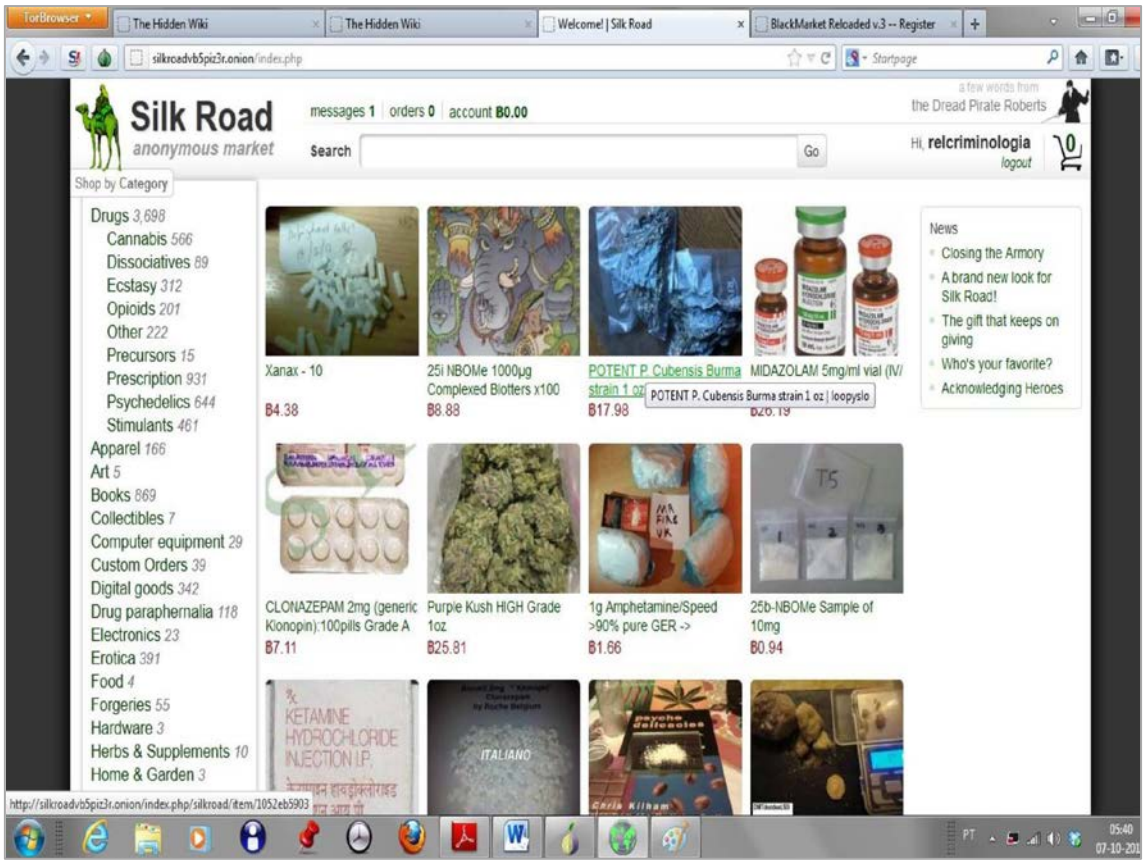
1. Dificuldades da investigação criminal em ambiente digital.
2. O recurso a métodos ocultos de investigação criminal.
3. O acesso oculto a dados informáticos armazenados.
4. As acções encobertas em ambiente digital.
5. *Hacking* e o uso de *malware*

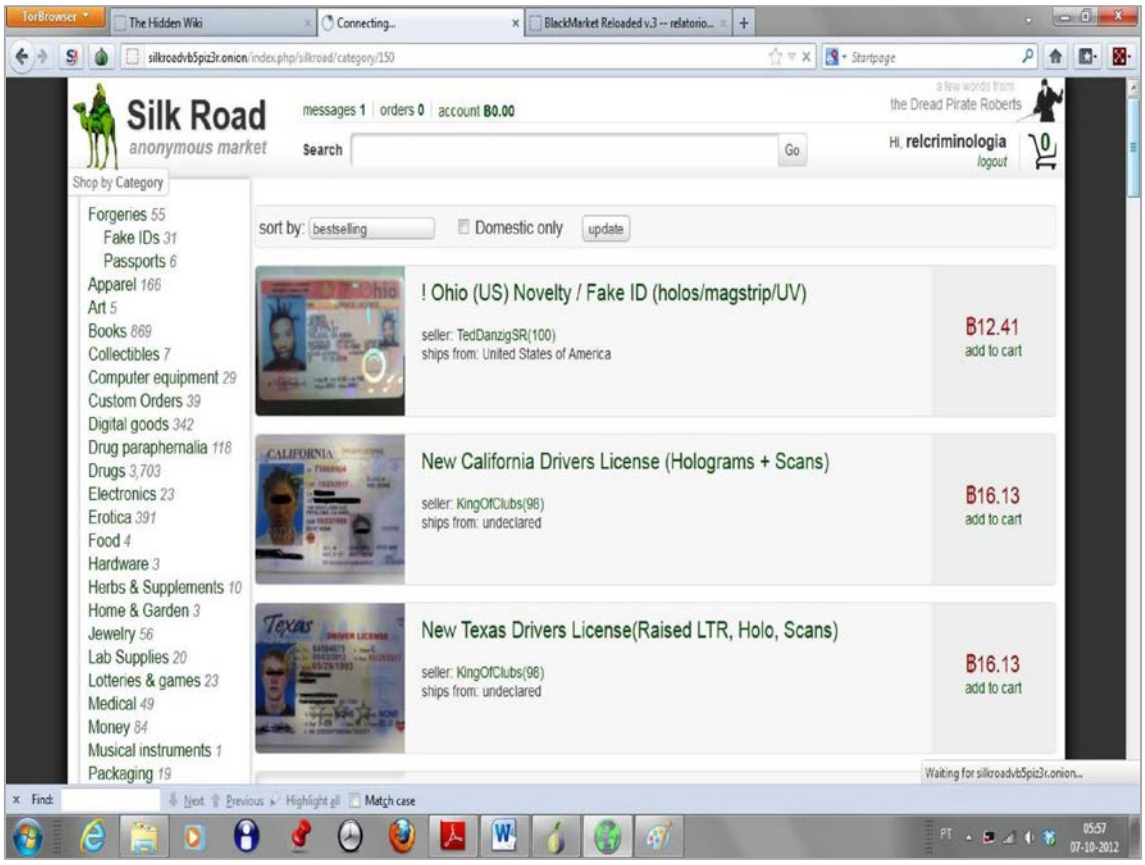
CENTRO DE ESTUDOS JUDICIÁRIOS

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/
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
News
Closing the Armory
A brand new look for Silk Road!
The gift that keeps on giving
Who's your favorite?
Acknowledging Heroes
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

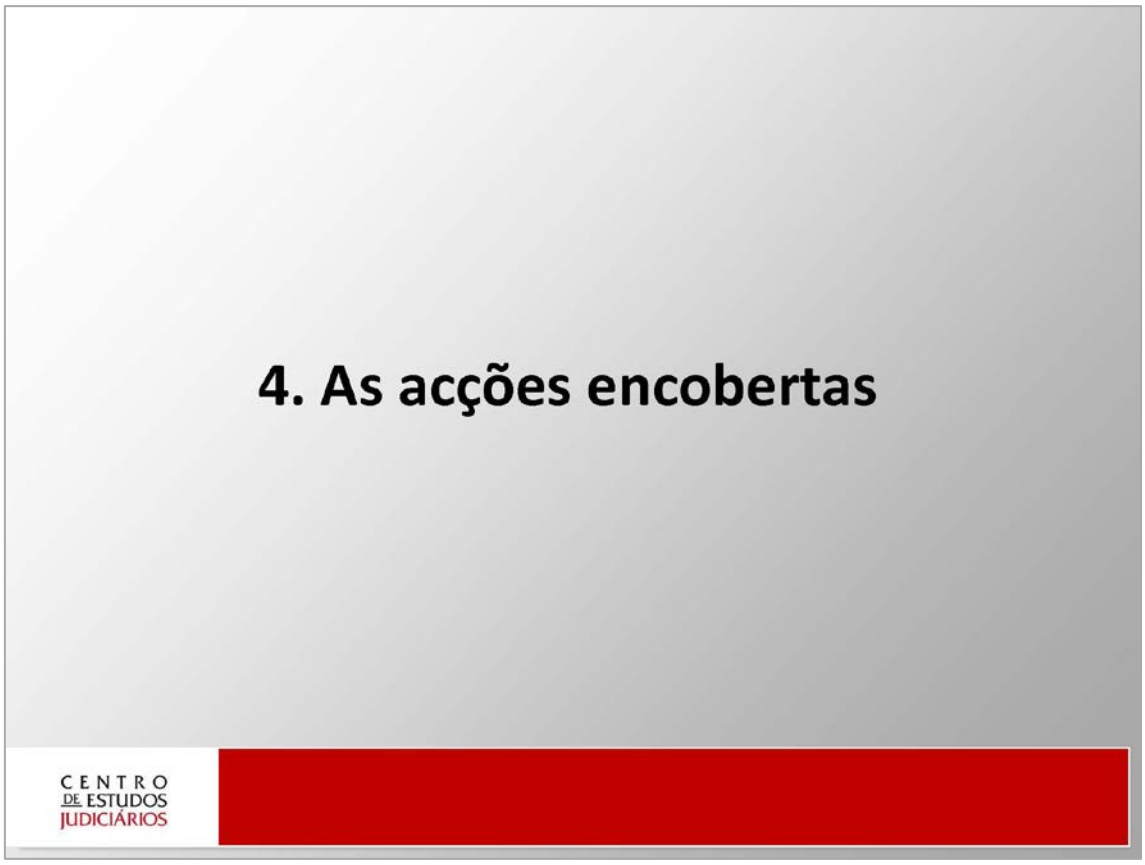
- Se não for admissível, será que apenas se pode aceder a outro Sistema a partir do 15/5 da LC?
- Obrigação de recorrer à injunção para apresentação ou concessão do acesso a dados?

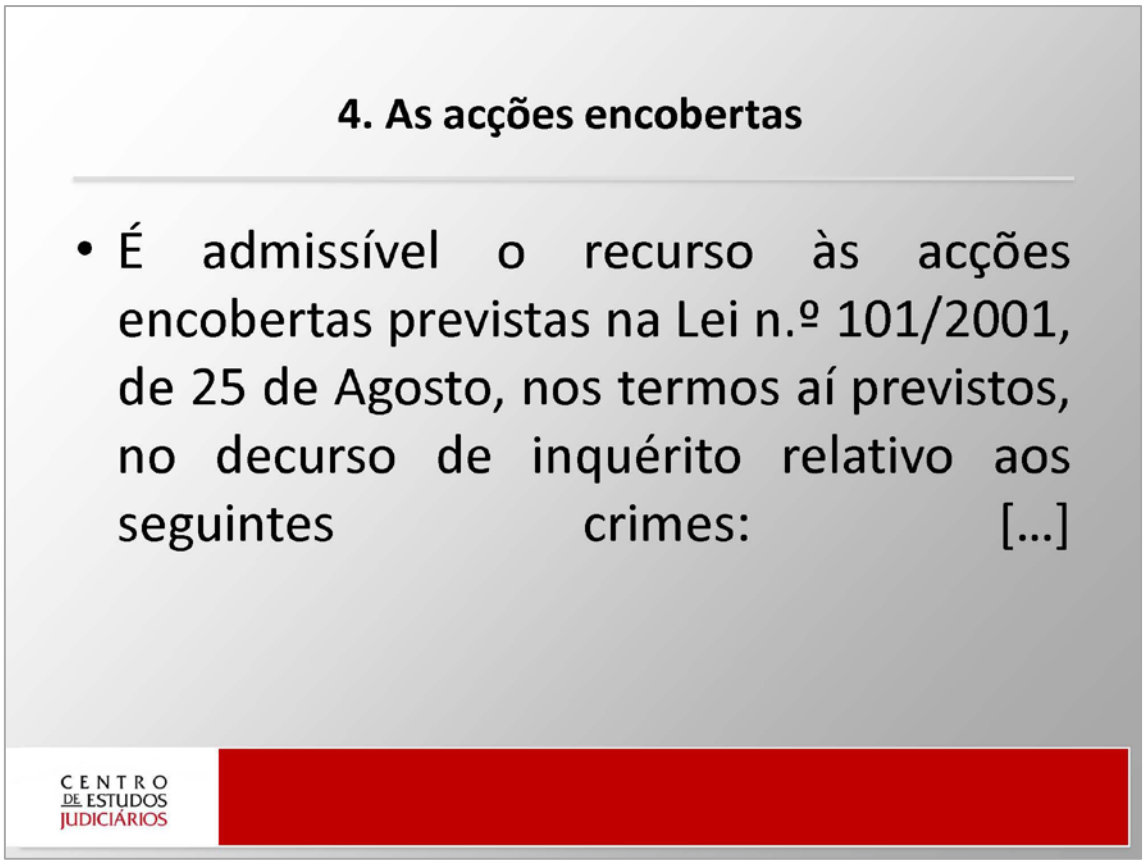
CENTRO DE ESTUDOS JUDICIÁRIOS

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