AASP
Associação dos Advogados
São Paulo - desde 1943

COMPLIANCE DIGITAL

Aspectos criminais do compliance digital

Rony Vainzof
rony@opiceblum.com.br

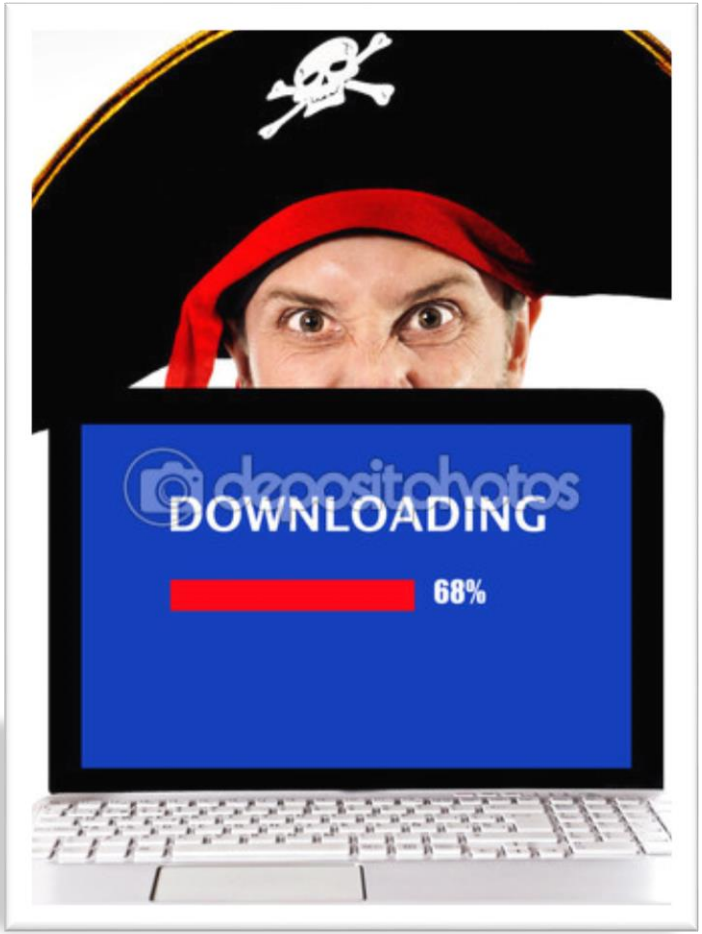
AASP
Associação dos Advogados
São Paulo - desde 1943

Quais são os nossos freios?

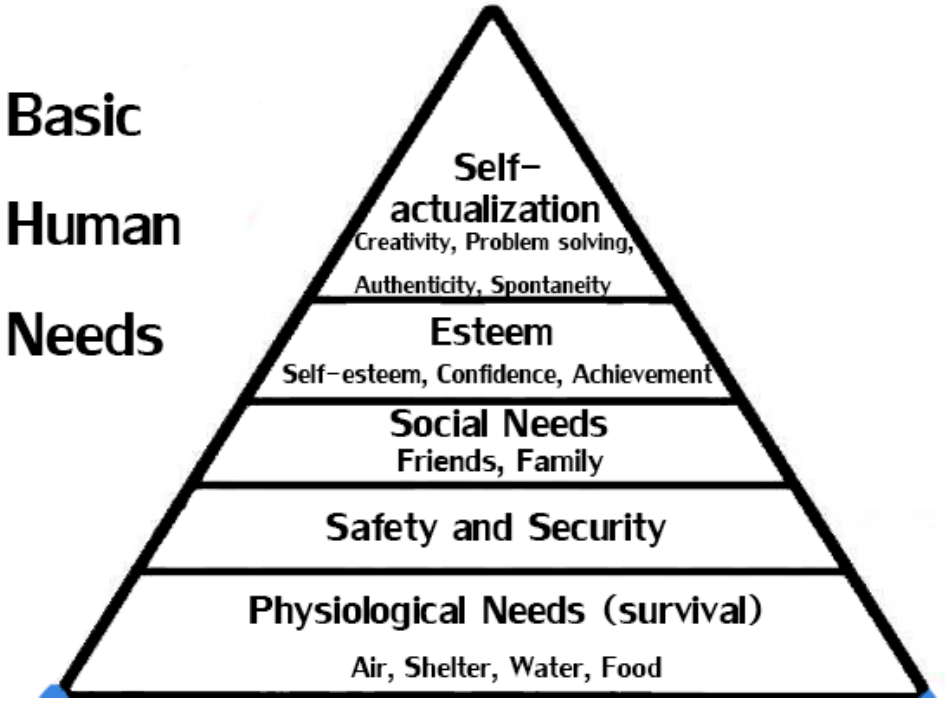
?

AASP
Associação dos Advogados
São Paulo - desde 1943

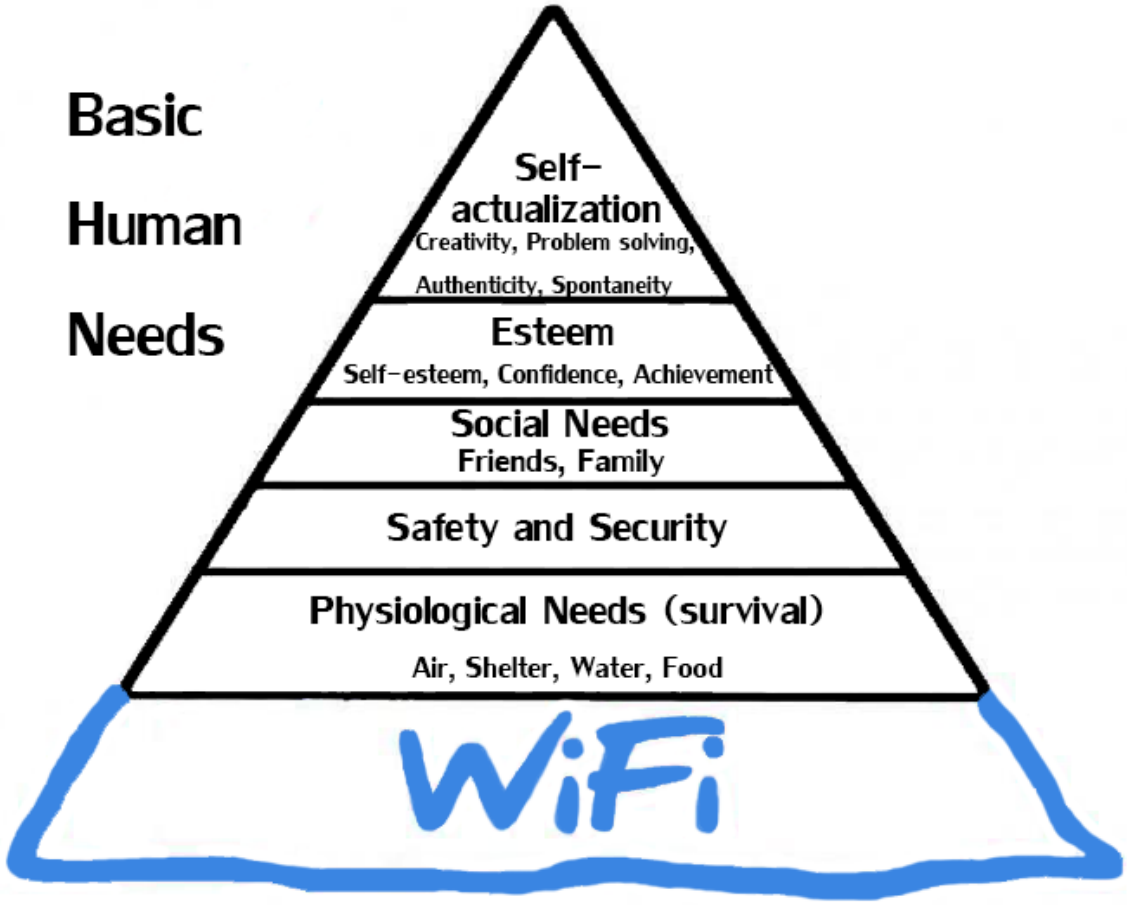
Quais são os nossos freios?



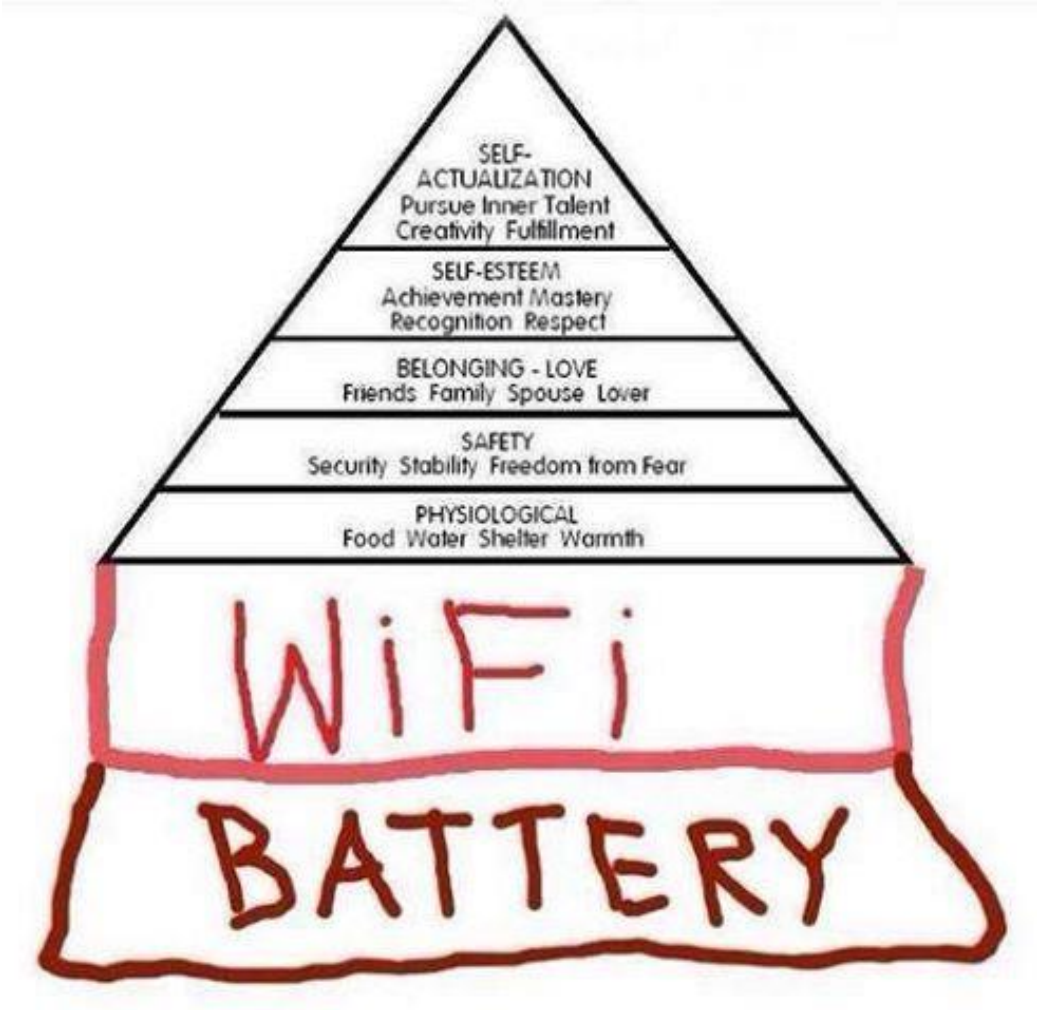
Pirâmide de Abraham Maslow



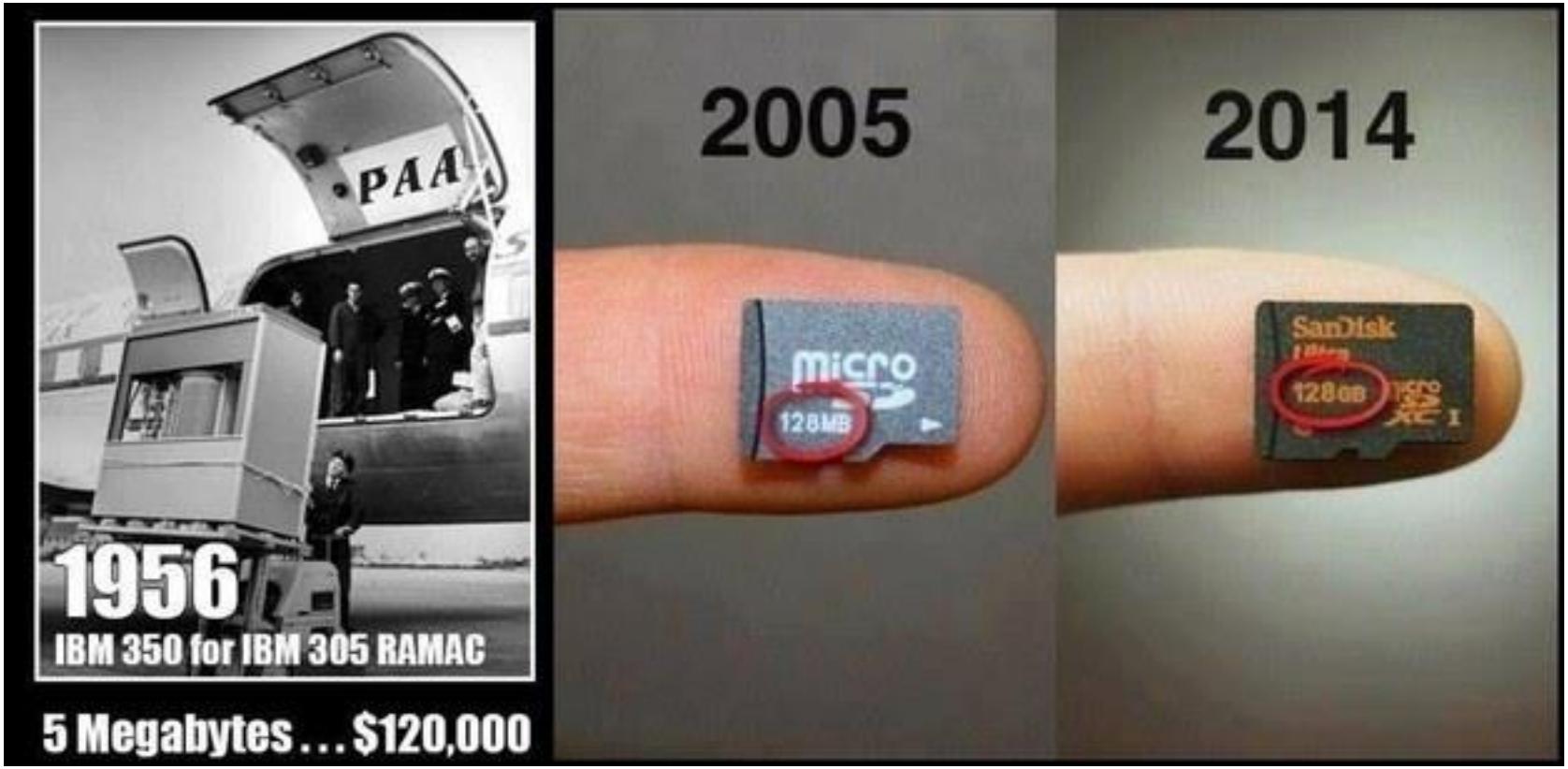
Pirâmide de Abraham Maslow



Pirâmide de Abraham Maslow



Evolução


1956
IBM 350 for IBM 305 RAMAC
5 Megabytes . . . $120,000
2005
micro
128MB
2014
SanDisk
128GB

Evolução

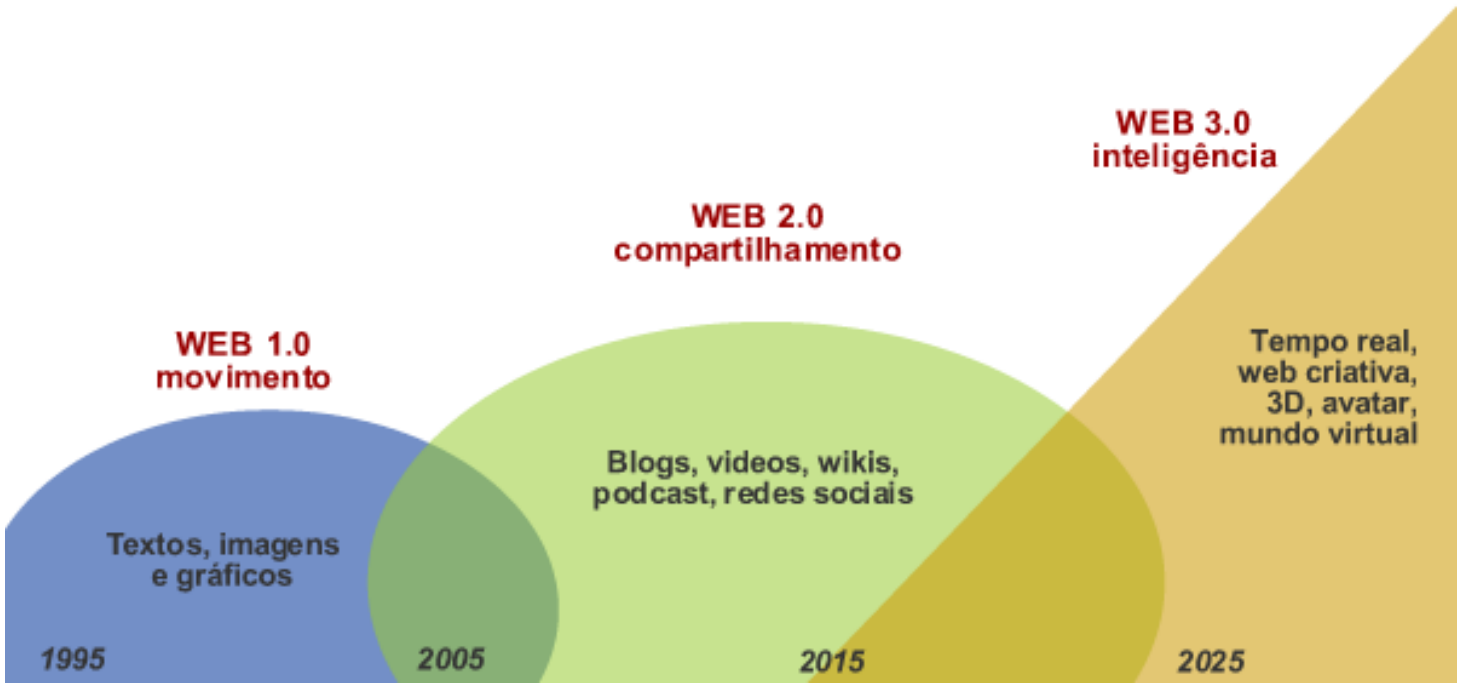
Evolução

Evolução

Ciberespaço?

Devemos encarar a tecnologia "...como um poderoso componente do ambiente no qual as crianças crescem, um componente que é tão onipresente quanto o ar que respiramos ou a água que bebemos", concluindo que "não devemos nem abraçar nem evitar as mídias, mas usá-las conscientemente e de maneira focada" e que "elas não são nem malignas nem benéficas, mas podem vir a sê-lo, dependendo de como são usadas" (Michael Rich)

Evolução da WEB



Internet, o princípio end-to-end e inovação

- Internet se limita a transmitir dados dos seus respectivos usuários, de forma livre e neutra, sem qualquer interferência.
- A rede não sabe para quais fins está sendo ou será utilizada.
- Novas ideias são testadas na Internet, sem a necessidade de prévio convencimento de qualquer pessoa, resultando em um ambiente generativo.
- Novas aplicações apenas precisam ser conectadas à Internet para funcionar, permitindo a inovação continua e permanente em seu ambiente, de forma única e universal.

AASP
Associação dos Advogados
São Paulo - desde 1943

A Declaration of the Independence of Cyberspace”, **escrito em 1996**, por John Perry Barlow.

Escola do Direito do Ciberespaço, de David Johnson e David Post

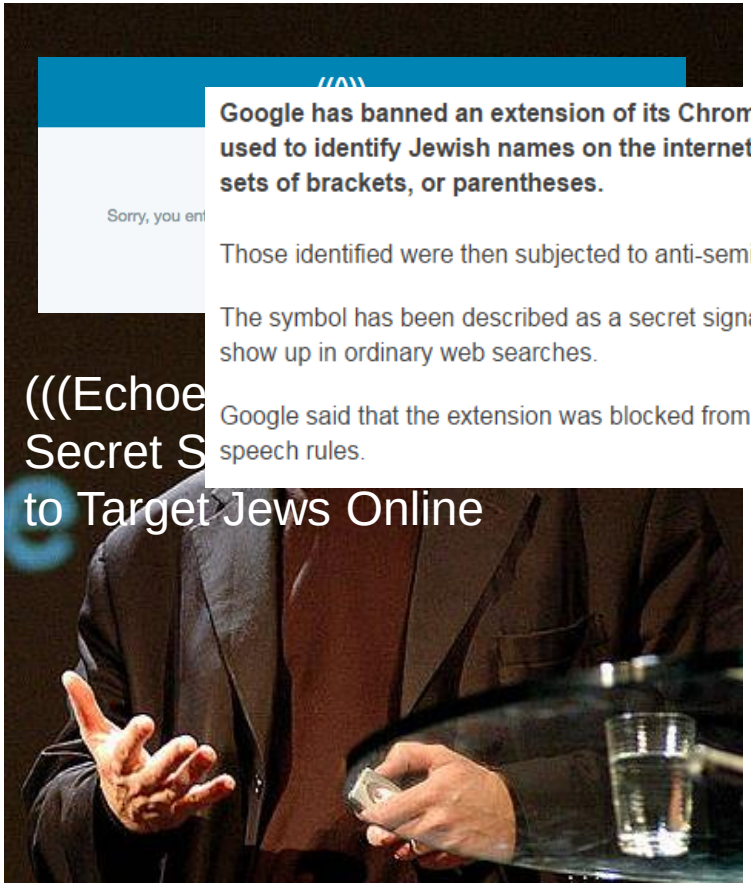
Tradicionalista

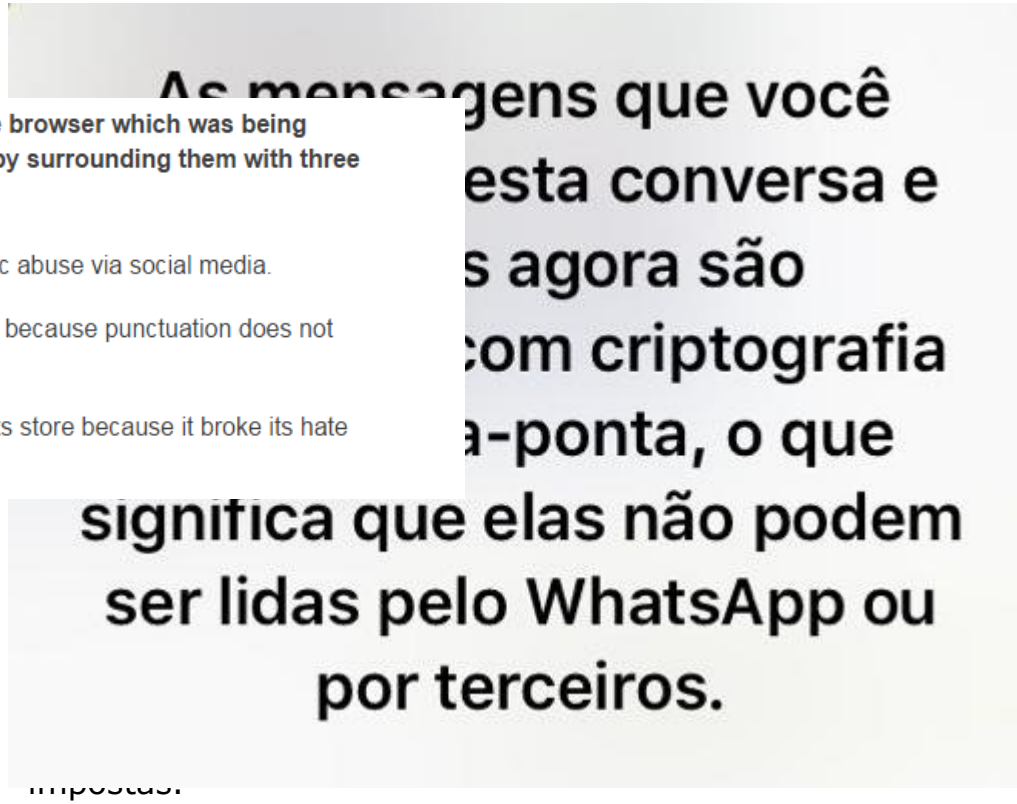
- A Internet é apenas mais um ambiente em que os cidadãos praticam atos lícitos e infelizmente ilícitos, não careceria de regulamentação específica;

- A analogia deve ser utilizada com muito cuidado em demandas do ciberespaço, pois, caso contrário, pode levar a resultados desastrosos (habeas corpus em decorrência da alegada restrição de "liberdade de locomoção virtual", alegando restrições técnicas impostas por seu provedor de acesso à Internet ao impedi-la de visitar determinados sites);

- Como apenas os dispositivos legais – o direito positivo – não dariam conta de acompanhar a evolução da tecnologia da informação e da comunicação, pois inviável criar novas regras de acordo com a revolução que presenciamos, surgiu a corrente doutrinária mista, para regulamentar, utilizando não só o sistema jurídico, mas também a própria arquitetura de Rede.

Internet e Regulação - Escola da Arquitetura da Rede, de 1999, por Lawrence Lessig.





AASP
Associação dos Advogados
São Paulo - desde 1943

Bens jurídicos tutelados

1. Homicídio?
2. Furto?
3. Difamação?
4. Contrafação?

"A Internet trouxe Novos bens jurídicos tutelados?"

(Amaro Moraes e Silva Neto, 1951-2012)

AASP
Associação dos Advogados
São Paulo - desde 1943

A internet nunca foi um mundo sem leis!!!

STF - HABEAS CORPUS: HC 76689 PB
Resumo: "crime de Computador": Publicação de Cena de Sexo Infanto-juvenil (e.c.a., Art. 241
Relator(a): SEPÚLVEDA PERTENCE
Julgamento: 21/09/1998

O tipo cogitado - na modalidade de "publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente" - ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: **basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador;**

Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminada, o meio técnico empregado para realizá- la pode até ser de invenção posterior à edição da lei penal: **a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.**

AASP
Associação dos Advogados
São Paulo - desde 1943

Evolução – Pornografia Infantil

Estatuto da Criança e do Adolescente (Lei 8.069/90):

- Art. 241. Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
- Pena - reclusão de um a quatro anos.

Lei nº 10.764/2003

- Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, **inclusive rede mundial de computadores ou internet**, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente:
- Pena - reclusão de 2 (dois) a 6 (seis) anos, e multa.
- § 1o Incorre na mesma pena quem:
- II - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo;
- III - assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do caput deste artigo.

Lei nº 11.829/2008

- Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
- Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
- Art. 241-B. **Adquirir, possuir ou armazenar**, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)
- Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

AASP
Associação dos Advogados
São Paulo - desde 1943

Extraterritorialidade e Soberania
LICRA v. Yahoo (2000)

•Código Penal francês: vedação da exibição de material nazista para fins de comércio.

•Yahoo! France: removia conteúdo nazista ocasionalmente existente em sua página francesa (www.yahoo.fr).

•Usuários franceses: continuavam podendo acessar o mesmo conteúdo removido por meio da página do Yahoo norte-americano (www.yahoo.com), motivo pelo qual foi movida ação judicial na França.

•Yahoo: alegou que os leilões eram conduzidos nos EUA, para seus cidadãos também, e que a Primeira Emenda da sua Constituição permitia tal serviço, pleiteando a incompetência da Justiça francesa para julgar o caso.

•Na França, foi negada a exceção de incompetência, adotando os seguintes fundamentos:

- Os leilões de material nazista existentes na página dos EUA também eram abertos para outros países, incluindo a França, sendo vedado referido conteúdo pela legislação francesa;
- A empresa norte-america tinha ciência da utilização de seus serviços, no caso ilícitos, por franceses.

•Yahoo moveu uma ação judicial nos EUA, requerendo a declaração judicial de que a decisão francesa não pudesse ser reconhecida e nem cumprida em seu país, pois violaria a sua Constituição.

•Juiz americano Warren J. Ferguson:

- A França está dentro dos seus direitos, como uma nação soberana, ao promulgar leis contra a distribuição de propaganda nazista em resposta à sua terrível experiência com as forcas nazistas durante e Segunda Guerra Mundial.
- A LICRA e a UEJF estão dentro dos seus direitos ao promover na França ação contra o Yahoo! por violação da lei francesa.
- A única consequência adversa experimentada pela empresa, como resultado desses atos, é que ela deve esperar que LICRA e UEJF venham aos Estados Unidos executar a decisão francesa, antes de poder arguir, como defesa, a Primeira Emenda da Constituição.
- Entretanto, não há nada de errado com a conduta das organizações francesas em colocar o Yahoo! nessa posição.
- A Yahoo! obtém vantagens comerciais pelo fato de que usuários na França são capazes de acessar seu Web site. Yahoo! não pode esperar se beneficiar do fato de que seu conteúdo pode ser visto ao redor do mundo e, ao mesmo tempo, esperar ser protegida dos custos resultantes – um dos quais é que, se Yahoo! viola as leis de liberdade de expressão de outra nação, ela deve aguardar que os litigantes estrangeiros venham aos Estados Unidos para cumprir o julgamento antes que sua defesa, fundamentada na Primeira Emenda, seja ouvida por uma corte dos Estados Unidos.

•Porém, antes mesmo do julgamento em questão na Corte norte-americana, após as decisões francesas, o Yahoo! resolveu "voluntariamente" mudar suas políticas e impedir materiais que promovam o ódio e a violência.

AASP
Associação dos Advogados
São Paulo - desde 1943

"*Right to delist*" e jurisdição

2014: Mario Costeja González e a Agência Espanhola de Proteção de Dados – AEPD x Google Spain SL (filial espanhola), a Google Inc. (matriz norte-americana) e o La Vanguardia (conhecido jornal espanhol).

12/06/15 (French regulator orders Google to expand 'right to be forgotten' beyond Europe):

- Google vai restringir acesso aos resultados de busca por meio de IPs e outras técnicas de geolocalização somente sendo aplicável ao país da pessoa que solicitou a remoção.
- Se uma URL é desindexada com base na solicitação feita por alguém que vive na França, todos os usuários franceses não serão capaz de ver a URL em qualquer Google Search (incluindo o Google.com).
- No entanto, se algum francês viajar para outro país - mesmo dentro da EU - ele será capaz de acessar o resultado, mas apenas em versões do Google de países não pertencentes à EU.

MCI – Soberania

Artigo excluído

Art. 12. O Poder Executivo, por meio de Decreto, **poderá obrigar os provedores de conexão e de aplicações de Internet** previstos no art. 11 que exerçam suas atividades de forma organizada, profissional e com finalidades econômicas **a instalarem ou utilizarem estruturas para armazenamento, gerenciamento e disseminação de dados em território nacional**, considerando o porte dos provedores, seu faturamento no Brasil e a amplitude da oferta do serviço ao público brasileiro.

Rony Vainzof
rony@opiceblum.com.br

DECRETO Nº 8.135/13 - Comunicações de dados da administração pública federal a segurança nacional

Art. 1º As **comunicações de dados da administração pública federal** deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação **fornecidos por órgãos ou entidades da administração pública federal**.

Art. 2º Com vistas à **preservação da segurança nacional**, fica dispensada a licitação para a contratação de órgãos ou entidades da administração pública federal.

§1º Enquadra-se no caput a **implementação e a operação** de redes de telecomunicações e de **serviços** de tecnologia da informação, em especial à **garantia da inviolabilidade das comunicações de dados da administração pública federal**.

Soberania e Jurisdição

Aplicação da legislação brasileira:

- **Código Penal:** de acordo com o princípio da territorialidade, previsto no Art. 5º do Código Penal, aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional, considerando praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado (art. 6º).

- **Marco Civil da Internet (Lei 12.965/14)**:

  - De acordo com art. 11, em **qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverá ser obrigatoriamente respeitada a legislação brasileira**.

  - Também para dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil, **mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior**, mas **OFERTE SERVIÇO AO PÚBLICO BRASILEIRO OU pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no brasil**.

- Conforme referido art. 11 do MCI, como todos os provedores de aplicações, invariavelmente coletam, armazenam, guardam e/ou tratam dados pessoais e registros eletrônicos, deverão respeitar a legislação brasileira, ainda que sejam estrangeiros, **bastando direcionarem (targeting) seus serviços também ao público brasileiro, mesmo que não tenham um integrante do grupo econômico no Brasil**.

EUA – 11 DE SETEMBRO DE 2001

Internet communications may also be used as a means to communicate with potential victims or to coordinate the execution of physical acts of terrorism. For example, the Internet was used extensively in the coordination of participants in the attacks of 11 September 2001 in the United States.

(fonte: THE USE OF THE INTERNET FOR TERRORIST PURPOSES - 2012)

AASP
Associação dos Advogados
São Paulo - desde 1943

Efeito Snowden – 09 de junho de 2013

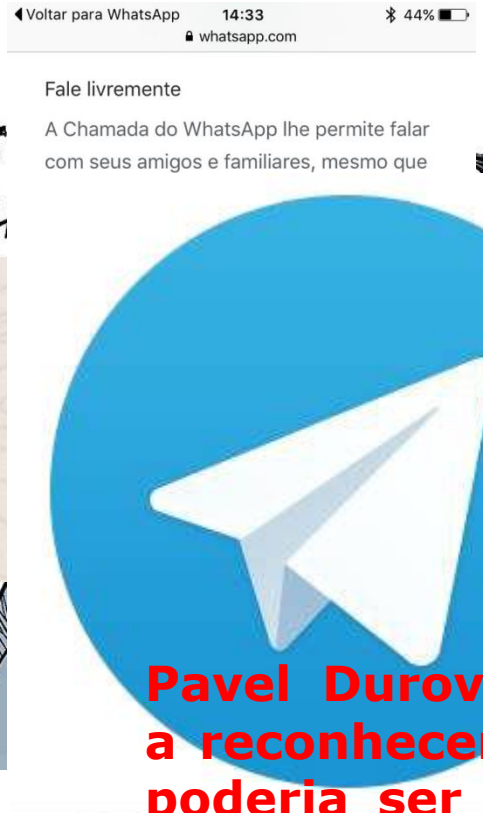
AASP
Associação dos Advogados
São Paulo - desde 1943

Efeito EI: 29.06.16

U.S. Customs Wants to Ask Travelers for Their Social Media Accounts

Written by Lilit Marcus · *June 29, 2016*

Criptografia



Telegram

FBI has accessed San Bernardino shooter's phone without Apple's help

Pavel Durov (Telegram): chegou a reconhecer que sua ferramenta poderia ser usada para o terror. Para ele, esse seria o preço a se pagar pela privacidade de usuários legítimos.

AASP
Associação dos Advogados
São Paulo - desde 1943

Snowden
17 de março de 2016

"'Going dark' é um conto de fadas: três anos após as manchetes de escuta de @dilmabr ela ainda está fazendo chamadas não criptografadas", diz a mensagem acompanhada de uma colagem de manchetes da imprensa americana de setembro de 2013 e desta quinta.

AASP
Associação dos Advogados
São Paulo - desde 1943

O que é crime de Interceptação?

CF: Art. 5º, inc. XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Lei 9.296/96: Art. 10 . Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

STJ (16/06/15) RECURSO ESPECIAL Nº 1.428.961 - SP (2014/0004168-7) RELATORA : MINISTRA MARIA THEREZA DE ASSIS MOURA
"Em casos tais de mensagem de correio eletrônico, **a interceptação da comunicação de sistema de informática pode ocorrer em qualquer etapa durante a armazenagem e o encaminhamento das mensagens pelo Provedor, antes que elas venham a ser recebidas e lidas por seus respectivos destinatários, momento em que efetivamente se encerra o processo comunicacional**.

O recorrido teria acessado diretamente o Provedor de Serviço de Correio Eletrônico UOL, monitorando as mensagens da sua ex-esposa lá armazenadas, e visualizando os seus conteúdos sem autorização judicial ou com objetivos não autorizados em lei.
Tal conduta, em tese, configura fato típico previsto no artigo 10 da Lei nº 9.296/96, consistente em "realizar interceptação de comunicação informática sem autorização judicial ou com objetivo não autorizado em lei".

Com efeito, o acesso às mensagens armazenadas diretamente no provedor de serviço de correio eletrônico, antes que elas venham a ser acessadas e 'abertas' pelo seu real destinatário, ou transferidas pelo destinatário ao seu dispositivo informático particular, ocorre durante o processo comunicativo.

Ademais, a interceptação de que cuida a norma em exame, tanto da comunicação telefônica quanto da comunicação informática ou telemática, não se confunde com sonegação ou destruição de correspondência, não suprimindo a recepção da mensagem pelo **destinatário que, apenas, deixa de recebê-la com exclusividade**.

Assim, **a captação da mensagem teria em tese ocorrido enquanto a comunicação estava acontecendo, sendo irrelevante que não tenha havido supressão do acesso ao destinatário final, que teria recebido a mensagem já aberta**.

(...)

Do exposto resulta que a conduta imputada ao réu que, segundo narra a denúncia, teria acessado o provedor de serviço de correio eletrônico da ex-esposa, abrindo as comunicações a ela dirigidas de modo reiterado e continuado, realizando monitoramento das mensagens privadas sem autorização judicial, constitui, em tese, fato típico previsto no artigo 10 da Lei nº 9.296/96 (interceptação de comunicações), cujo bem jurídico tutelado, a propósito, é tão caro à sociedade que recebeu tratamento de garantia constitucional, a inviolabilidade do sigilo das comunicações assegurada no artigo 5º, inciso XII, da Carta da República."

AASP
Associação dos Advogados
São Paulo - desde 1943

STJ decide que acesso ao WhatsApp em celular apreendido só com a autorização judicial

Em março de 2014, PM recebeu informação da Polícia Federal de que um pacote com drogas seria entregue pelos Correios em uma casa em Porto Velho.

Policiais surpreenderam o suspeito e abriram o pacote, que continha 300 comprimidos de ecstasy.

O recebedor foi preso em flagrante, oportunidade em que os policiais militares apreenderam o seu celular.

Defesa do suspeito impetrou habeas corpus para anular as provas obtidas a partir dos dados acessados no celular. Na argumentação, defendeu que eram ilegais as transcrições das conversas via WhatsApp, feitas pela perícia, pois a polícia precisaria de autorização judicial, "antes de proceder à devassa unilateral no conteúdo" do aparelho.

Para o Ministério Público de Rondônia, acessar o celular apreendido após um flagrante se trata de um "expediente comum", previsto no artigo 6º do Código de Processo Penal (CPP).

STJ: **acesso ao conteúdo de conversas pelo WhatsApp em celular apreendido durante flagrante pela polícia precisa de autorização judicial para ser considerado como prova legal**.

(processo(s): RHC 51531)

Disponível em: http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/Not%C3%ADcias/Not%C3%ADcias/Acesso-ao-Whatsapp-em-celular-apreendido,-s%C3%B3-com-a-autoriza%C3%A7%C3%A3o-judicial

Soberania, Guarda e Disponibilização de Dados ou Informações

Fonte: https://www.linkedin.com/pulse/suspens%C3%A3o-do-whatsapp-o-que-legisla%C3%A7%C3%A3o-brasileira-prev%C3%AA-rony-vainzof?trk=prof-post

1) Fornecimento de dados cadastrais (nome, RG, CPF, por exemplo):

- **Lei de Organização Criminosa (Lei 12.850/13)**: o delegado de polícia e o Ministério Público terão acesso, **independentemente de autorização judicial**, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pelos provedores de internet (art. 15), inclusive sendo crime recusar ou omitir dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou delegado de polícia, no curso de investigação ou do processo (art. 21).

- **Marco Civil da Internet (Lei 12.965/14)**: não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, **pelas autoridades administrativas que detenham competência legal para a sua requisição** (art. 10, §3º).

2) Fornecimento de registros de acesso a aplicações de Internet (IP, data e hora de acesso, por exemplo):

- **Marco Civil da Internet:** em qualquer hipótese, a disponibilização de tais registros **deverá ser precedida de autorização judicial** (art. 15, §3º).

3) Fornecimento de conteúdo de comunicações privadas já ocorridas (mensagens já recebidas no Whatsapp ou por e-mail, por exemplo):

- **Marco Civil da Internet**: o conteúdo das comunicações privadas somente poderá ser disponibilizado **mediante ordem judicial** (art. 10, §2º).

4) Interceptação do fluxo de comunicações em sistemas de informática e telemática (mensagens que ainda não ocorreram):

- **Lei 9.296/96**, que regulamenta o inciso XII, do art. 5º da Constituição Federal: entre outras questões, a interceptação das comunicações somente poderá ser determinada por ordem judicial, na investigação criminal ou na instrução processual penal, constituindo crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Soberania, Guarda e Disponibilização de Dados ou Informações

Fonte: https://www.linkedin.com/pulse/suspens%C3%A3o-do-whatsapp-o-que-legisla%C3%A7%C3%A3o-brasileira-prev%C3%AA-rony-vainzof?trk=prof-post

5) Sanções

- Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
    - § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial.
    - § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer.
    - § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
    - § 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.
- As sanções para o descumprimento dos arts. 10 e 11 do MCI, sem prejuízo das demais sanções cíveis, criminais ou administrativas, estão previstas no art. 12 do MCI, e podem ser aplicadas de forma isolada ou cumulativa, variando:
    - Advertência, com indicação de prazo para adoção de medidas corretivas;
    - Multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício;
    - Até mesmo a proibição de exercício das atividades;
    - Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa sua filial, sucursal, escritório ou estabelecimento situado no País (art. 12, parágrafo único).

CPI de Crimes Cibernéticos
PL sobre bloqueio de aplicações (05.05.16)

Do Bloqueio a Aplicações de Internet em Atendimento a Ordem Judicial

Art. 23-A O Juiz somente poderá determinar que o **provedor de conexão bloqueie o acesso a aplicação de intern representação no Brasil e que seja pr uníveis com pena mínima igual ou supe** imes contra a honra.

§ 1º Para o bloqueio de **interesse público, a proporcionalidade, a para promover a efetiva cessação da c**

§ 2º **Considera-se rep** possua responsável legalmente constituído no grupo econômico possua filial, sucursal, escritório ou estabelecimento no País.

§ 3º **As aplicações de mensagens instantâneas, de uso público geral, ficam excluídas do bloqueio de que dispõe este artigo.**

A manifestação da AGU na ADI 5.527 conclui:

"Todavia, o que requer o autor, em realidade, é impedir decisões judiciais futuras que suspendam os programas de comunicação de mensagens on line, criando uma situação absolutamente esdrúxula, concedendo verdadeira imunidade jurisdicional em favor de uma empresa que explora esse tipo de ferramenta. Ademais, o pleito, em última análise, impossibilita a atuação das autoridades judiciais, interferindo diretamente na independência constitucional garantida ao Poder Judiciário."

AASP
Associação dos Advogados
São Paulo - desde 1943

PROVAS DIGITAIS EM ATOS DE CORRUPÇÃO

Investigações internas: segurança da informação e monitoramento de comunicações.

Investigações externas:

- Utilização de servidores em nuvem
- Princípio da não autoincriminação: direito de não ser obrigada a depor contra si mesma, nem a confessar-se culpada.
- Critografia: operação Satiagraha: entendimento pela não obrigação de fornecimento, pelo banqueiro Daniel Dantas, de chave criptográfica de HDs apreendidos em sua residência
- Também atinge ao suspeito?
- O crime de falso testemunho não se configura quando, com a declaração da verdade, o depoente assume o risco de ser incriminado' (STJ – T5 – HC 20.924/SP – Rel. Min. Laurita Vaz – Votação Unânime – j. 11.03.03 – DJ 07.04.03, p. 302).

Lei Anticorrupção:

Art. 7º Serão levados em consideração na aplicação das sanções:

VII - a **cooperação da pessoa jurídica para a apuração das infrações**;
VIII - a existência de **mecanismos e procedimentos internos de integridade**, auditoria e incentivo à denúncia de irregularidades e a aplicação efetiva de códigos de ética e de conduta no âmbito da pessoa jurídica;

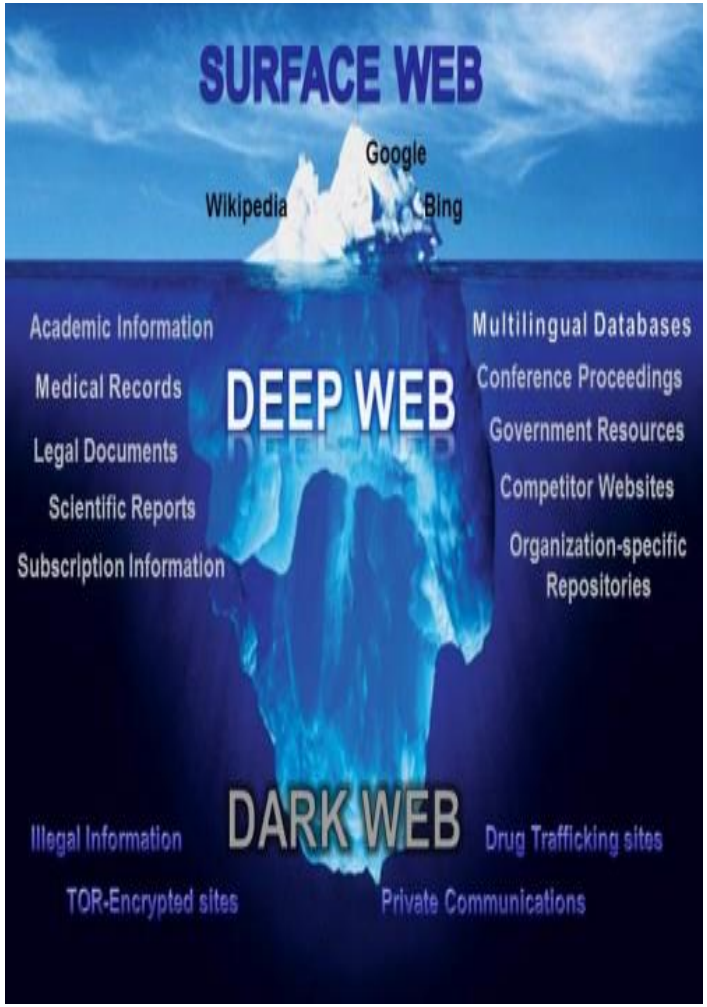
Acordo de Leniência

Colaboração resulte:

I - a pessoa jurídica seja a primeira a se manifestar sobre seu interesse em cooperar para a apuração do ato ilícito;

III - a pessoa jurídica admita sua participação no ilícito e **coopere plena e permanentemente com as investigações** e o processo administrativo, comparecendo, sob suas expensas, sempre que solicitada, a todos os atos processuais, até seu encerramento.

Organização Criminosa



Finalidade
Coleta e Disponibilização de Dados

- **INVESTIGAÇÃO DE ILÍCITOS (cooperação internacional)**

"The Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally Transnational manner"

Ban Ki-moon, Secretary-General of the United Nations

AASP
Associação dos Advogados
São Paulo - desde 1943

ONU – The use of the Internet for terrorist purposes - 2012

The development of increasingly sophisticated technologies has **created a network with a truly global reach, and relatively low barriers to entry**.

Internet technology makes it easy for an individual to **communicate with relative anonymity, quickly and effectively across borders, to an almost limitless audience**.

The same technology that facilitates such communication can also be exploited for the purposes of terrorism. **The use of the Internet for terrorist purposes creates both challenges and opportunities in the fight against terrorism**.

Six categories:

1) Propaganda (including recruitment, radicalization and incitement to terrorism);

2) Financing;

3) Training;

4) Planning (including through secret communication and open-source information);

5) Execution;

6) Cyberattacks.

RECENTES ATAQUES E O USO DE COMUNICADORES CRIPTOGRAFADOS

Terroristas de Paris usaram aplicativos para esconder plano de ataques

Jihadistas usaram WhatsApp e o Telegram, segundo investigadores

17/12/2015 – FONTE: G1

Investigadores encontraram evidências de que os terroristas que cometeram os atentados de Paris em novembro teriam usado aplicativos para esconder o planejamento dos ataques, disseram oficiais envolvidos nas investigações à rede de TV americana CNN.

Os investigadores ouvidos pela CNN não disseram que evidência específica mostra que os aplicativos foram usados para preparar os ataques. Eles foram usados em comunicações entre os terroristas por um período antes dos ataques. O que foi dito nas mensagens pode nunca ser identificado.

Os investigadores conseguiram recuperar algumas comunicações não-criptografadas em pelo menos um telefone achado, talvez uma indicação de descuido de pelo menos um dos terroristas.

Os suspeitos também usaram outros métodos para cobrir seus passos, incluindo trocar os chips de celular para evitar vigilância.

O chefe do FBI, James Comey, disse na quarta-feira (16) em Nova York que "**o uso de criptografia está no centro do terrorismo**".

AASP
Associação dos Advogados
São Paulo - desde 1943

Executivo do Google defende eliminar o Estado Islâmico da internet pública

21/01/16 – Fonte: Olhar Digital

Diretor do Google Ideas, Jared Cohen, disse que o **Estado Islâmico deveria ser trancado para fora da internet pública e restringido à deep web**.

Não será possível impedir que se comunique utilizando o Tor ou ferramentas encriptadas de comunicação.

No entanto, o essencial, **para se dificultar a disseminação das mensagens de ódio, é impedir que ela chegue à rede tradicional** - aquela que pode ser indexada por sites de busca.

Sites e redes sociais façam todo o possível para deletar contas associadas aos terroristas e eliminar sua presença digital.

- Estado Islâmico conseguiu se apropriar de técnicas de comunicação digital ocidentais para seu próprio benefício: usam redes sociais, "dominam hashtags, criam contas falsas e se proliferam na internet". Graças a isso, eles "conseguiram criar uma impressão exagerada de sua presença online".
- Os radicais islâmicos não são "particularmente hábeis com tecnologia", mas possuem um grupo de "indivíduos jovens e tecnologicamente criativos que estão a par com sua geração em termos de sofisticação tecnológica".
- Cohen considera que o Estado Islâmico "foi a primeira organização terrorista que conseguiu ocupar e manter tanto território físico como também território digital".
- Segundo o executivo do Google, embora a luta física contra a organização seja mais importante que a liuta digital, "elas não são mutuamente excludentes; o que acontece em uma se reflete na outra".

LEI Nº 13.260, DE 16 DE MARÇO DE 2016
Terrorismo

Art. 2º O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública.

§ 1º São atos de terrorismo:

IV - **sabotar o funcionamento ou apoderar-se**, com violência, grave ameaça a pessoa ou **servindo-se de mecanismos cibernéticos**, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento.

Pena - reclusão, de doze a trinta anos, além das sanções correspondentes à ameaça ou à violência.

AASP
Associação dos Advogados
São Paulo - desde 1943

Facebook, Twitter, Microsoft e YouTube ajudarão UE contra discurso de ódio

31/05/16 – UOL

Regulação proposta pela União Europeia para combater discursos de ódio e propaganda terrorista em suas páginas e redes sociais.

A partir de 24 horas contadas do recebimento da notificação, elas farão parte de um novo código de conduta destinado a lutar contra essas ofensivas criminosas.

As novas regras também obrigam essas empresas a identificar e promover "contra-narrativas independentes" para enfrentar discursos e propaganda de ódio contra minorias e governos.

Twitter: "Continuamos empenhados em deixar o fluxo de tuítes. No entanto, existe uma clara distinção entre a liberdade de expressão e a conduta que incita à violência e ódio".

Google: "Temos sistemas eficientes para rever notificações válidas em menos de 24 horas e para remover o conteúdo ilegal".

Facebook: incentivarão as pessoas a usar as ferramentas - "se encontrarem o conteúdo que eles acreditam violar nossas normas, para que possamos investigar. Nossas equipes de todo o mundo reverão esses relatórios e agirão rapidamente".

Microsoft: "Nossos termos de uso proíbem a defesa da violência e do discurso de ódio sobre os serviços Microsoft. Recentemente, anunciamos medidas para proibir a publicação de conteúdo terrorista. Continuaremos a oferecer uma maneira de nos avisar quando eles pensam que a nossa política está sendo quebrada".

AASP
Associação dos Advogados
São Paulo - desde 1943

Cooperação Internacional

Princípio constitucional: cooperação entre os povos para progresso da humanidade (art. 4º, IX).

Vladimir Aras, Secretário de Cooperação Jurídica Internacional da PGR:

- Dados de usuários de Internet e dados de acesso a aplicações de Internet mantidos no Brasil **também podem interessar a Estados estrangeiros**.

- **Dados de usuários no exterior podem ser úteis a investigações brasileiras**.

- Torna-se necessário construir um **quadro normativo adequado para a cooperação entre diferentes jurisdições, especialmente mediante a implementação de tratados de cooperação internacional, que podem ser usados para obtenção transnacional de provas, inclusive digital evidencie.**

1990: **ratificação brasileira de tratados internacionais de assistência jurídica**, surge novo instrumento cooperacional denominado "auxílio direto", que também veicularia – tal qual a carta rogatória – pedidos de assistência jurídica internacional.

2002: Convenção Interamericana contra o Terrorismo: canais de comunicação entre suas autoridades competentes, a fim de facilitar o intercâmbio seguro e rápido de informações

2005: MLAT - **tratados bilaterais de cooperação jurídica internacional em matéria penal, como também em diversos tratados multilaterais que têm por objeto de temas de cooperação jurídica internacional** em matéria penal (Decreto nº 5.639, de 26 de dezembro de 2005).
(fonte: Análise da Coexistência entre Carta Rogatória e Auxílio Direto na Assistência Jurídica Internacional - Denise Neves Abade)

INTERPOL e a Rede 24/7

Interpol:

- Em 1923, em Viena (14 países): criação da Organização Internacional de Polícia Criminal, que mais tarde viria a ser conhecida simplesmente como Interpol.

- Era comum que criminosos europeus fugissem do alcance da lei cruzando a fronteira em direção ao país vizinho. Por isso, eles resolveram formar um banco de dados que facilitasse a troca de informações sobre delitos internacionais e seus autores.

- Com sede em Lyon, na França, a Interpol conta atualmente com 190 países-membros.

- Combate aos crimes transnacionais (tráfico de drogas, armas, pessoas, obras de arte roubadas, terrorismo, contrabando, etc.).

- No Brasil, suas atribuições são desempenhadas por servidores policiais e administrativos da Polícia Federal.

- Síntese dos casos são enviados para à Secretaria-Geral da Interpol, via sistema I-24/7.

Rede 24/7:

- Ferramenta de cooperação estabelecida e implementada pelo G-8 (grupo dos sete países mais industrializados e desenvolvidos economicamente, mais a Rússia), da qual o Brasil faz parte com mais de 40 países.

- Especial utilidade: prestação de assistência em investigações que envolvam delitos cibernéticos ou colheita de provas eletrônicas.

- As comunicações podem ser feitas diretamente por telefone ou mensagens eletrônicas, porém tem uso limitado à preservação de vestígios relativos a crimes praticados por meio do espaço cibernético, com a finalidade de evitar perda de informações.

- Para obtenção propriamente dita das informações, em regra, ainda são necessários os procedimentos de cooperação jurídica internacional.

- No Brasil, é operacionalizada e representada pelo Departamento de Polícia Federal.

AASP
Associação dos Advogados
São Paulo - desde 1943

Diretiva (EU - 2016/680)

Artigo 1º Objeto e objetivos

1. A presente diretiva estabelece as **regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas AUTORIDADES COMPETENTES PARA EFEITOS DE PREVENÇÃO, INVESTIGAÇÃO, DETECÇÃO OU REPRESSÃO DE INFRAÇÕES PENAIS OU EXECUÇÃO DE SANÇÕES PENAIS**, incluindo a salvaguarda e prevenção de ameaças à segurança pública.

2. Nos termos da presente diretiva, os Estados-Membros asseguram:

a) A proteção dos direitos e das liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais; e

b) Que o intercâmbio de dados pessoais entre autoridades competentes na União, caso seja previsto pelo direito da União ou do Estado-Membro, não seja limitado nem proibido por razões relacionadas com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

3. A presente diretiva não obsta a que os Estados-Membros prevejam garantias mais elevadas do que as nela estabelecidas para a proteção dos direitos e liberdades do titular dos dados no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes.

Autoridade competente: a) Uma autoridade pública competente para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública; ou b) Qualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer a autoridade pública e os poderes públicos para efeitos de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

Autoridade de controle: uma autoridade pública independente criada por um Estado-Membro.

Phishing

- Utilização de banco de dados para a prática de fraudes eletrônicas

ter 28/01/2014 01:17
Ministerio Publico Federal <accounts@passport.com>
INTIMAÇÃO PARA COMPARECIMENTO EM AUDIÊNCIA
Para Rony Vainzof

Ministério Público Federal

PROCEDIMENTO INVESTIGATÓRIO N.º 33781M. 12/12/2013

INTIMAÇÃO PARA COMPARECIMENTO EM AUDIÊNCIA, relativa ao procedimento investigatório em epígrafe, em tramitação nesta Regional, conforme despacho em anexo.

: INTIMAÇÃO ID: - Atualizado.
: PROCESSO Nº : - 907617823M.
: PRECENÇA IT : - Desabilitado.

ANEXO INTIMAÇÃO-MPF (32K)

ANEXO: INTIMACAO-MPF.SCR" (32k)

AASP
Associação dos Advogados
São Paulo - desde 1943

Violação de Segredo

Divulgação de projeto secreto de eletrodoméstico em rede social antes do lançamento

AASP
Associação dos Advogados
São Paulo - desde 1943

Divulgação de protótipo de novo modelo de moto tirada pelo celular

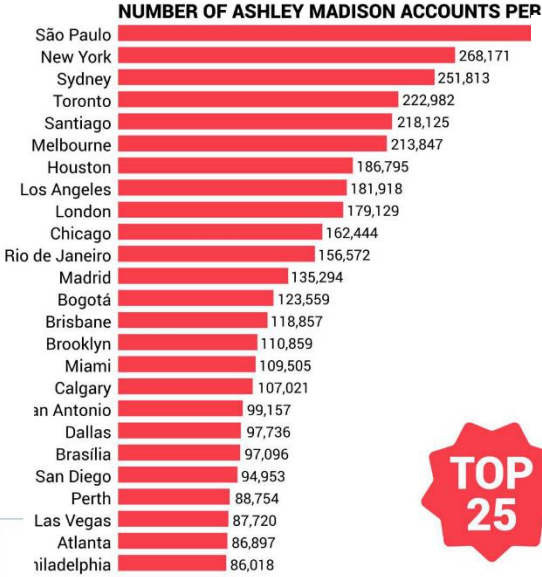
AASP
Associação dos Advogados
São Paulo - desde 1943

Polêmicas no Brasil

EXAME.COM

Tecnologia 10/12/2013 12:02

Banco do Brasil suspende aplicativo que provocou vazamento



Mas um detalhe que chama a atenção é sobre as contas de e-mails. Foram encontrados cerca 1.500 e-mails com o domínio .GOV.BR na base de dados. Dentre os diversos ramos da administração pública é possível encontrar e-mails da: camara.gov.br; senado.gov.br; planalto.gov.br e caixa.gov.br.

TOP 25

Falha no site da AES Eletropaulo permitia alterações nos cadastros de 6,4 milhões de clientes

Por: Rodrigo Ghedin
6 de setembro de 2012 às 14:35

Fichas sobre estudantes de colégio tradicional de SP vazam na internet

dadaviz.com

Colégio Bandeirantes, em SP; fichas sobre estudantes vazaram na internet

Risco de fraude para 12 milhões de estudantes

Juristas aconselham candidatos que tiveram dados expostos em página do MEC a se prevenirem contra uso indevido do nome e CPF

Os estudantes que tiveram nome, RG e CPF divulgados no site do Enem devem procurar a polícia e a Justiça para se precaver contra estelionatários. Esse é o conselho de especialistas para os 11,75 milhões de alunos inscritos nos exames de 2007, 2008 e 2009 que foram afetados por falha no banco de dados do Instituto Nacional de Educação e Pesquisa (Inep), do Ministério da Educação (MEC), e cujos dados foram disponibilizados no site da instituição.

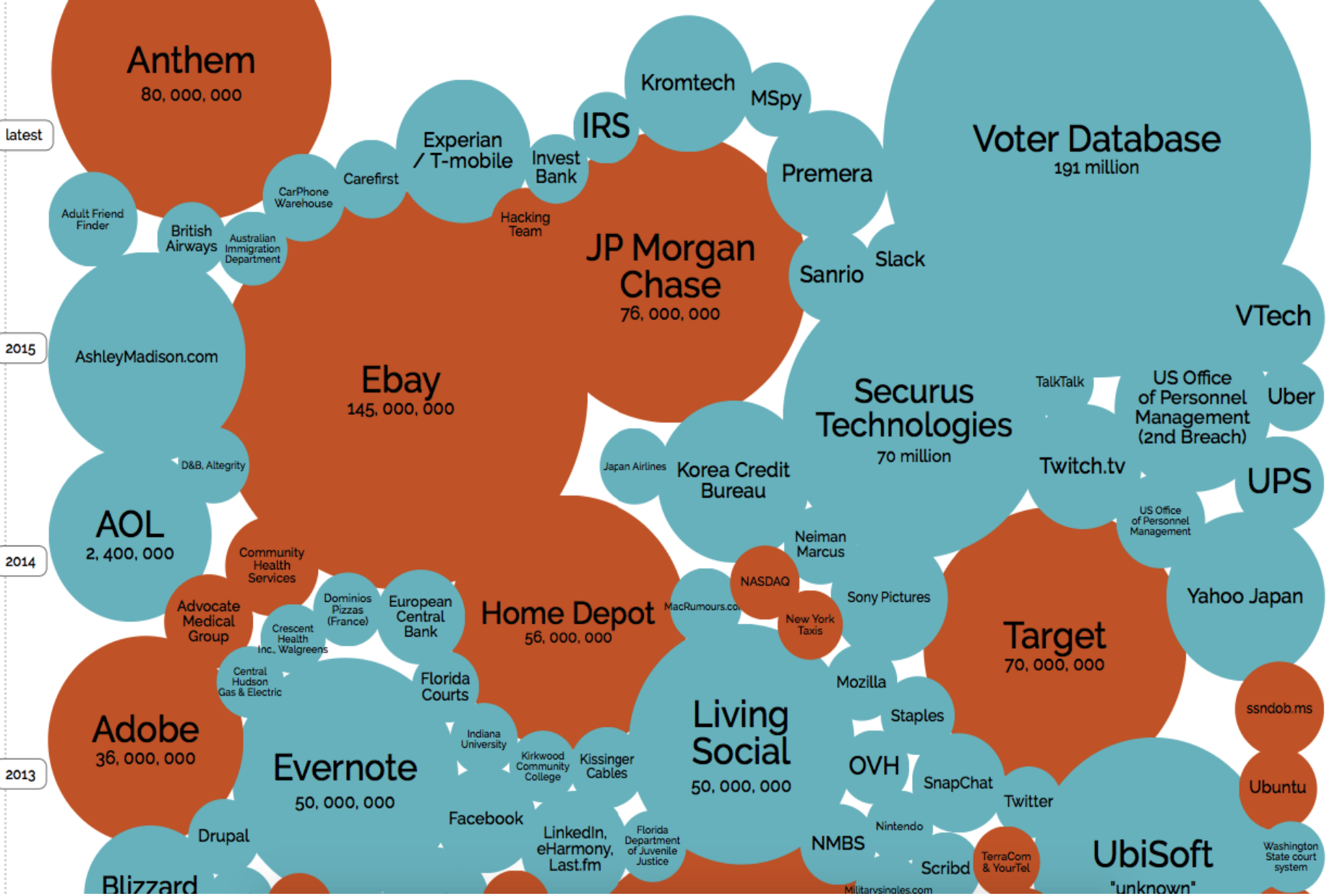
Segundo o advogado criminalista Alexandre Moura Dumans, as informações pessoais dos alunos podem ser utilizadas para criação de empresas-fantasma, obtenção de crédito

Informações podem ser usadas para abrir contas, empresas-fantasma e obter crédito

e falsificação de identidades. Por isso, o estudante cujos dados foram expostos deve guardar documentos que comprovem a inscrição no Enem e tomar algumas medidas preventivas (veja ao lado).

A presidente da Comissão de Direito e Tecnologia da Informação da OAB-RJ, Ana Amélia Menna Barreto, afirma que o incidente mostra a insegurança oferecida na Internet. "Esses dados eram sigilosos. O Ministério da Educação tinha a responsabilidade de evitar que chegassem ao conhecimento público. O vazamento desses informações cria uma base de dados de CPFs e RGs válidos que identificam os alunos," salienta, alertando para

http://exame.abril.com.br/tecnologia/noticias/banco-do-brasil-suspende-aplicativo-que-provocou-vazamento



CRIMES -SEG

Art. 153 do código penal - Divulgação de Segredo

- Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que É destinatário ou detentor, E cuja divulgação possa produzir dano A outrem:
- Pena - detenção, de 1 (um) A 6 (seis) meses, ou multa.

Art. 154 do código penal – Violação de Segredo Profissional

- Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, E cuja revelação possa produzir dano A outrem:
- Pena - detenção, de 3 (três) meses A 1 (um) ano, ou multa.

Art. 195 da lei 9279/96 - Concorrência Desleal:

- III - emprega meio fraudulento, para desviar, em proveito próprio ou alheio, clientela de outrem;
- XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais;
- Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.

Rony Vainzof
rony@opiceblum.com.br

AASP
Associação dos Advogados
São Paulo - desde 1943

Decreto MCI – SegInfo

- Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:

- I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;

- II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;

- III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014; e

- IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

AASP
Associação dos Advogados
São Paulo - desde 1943

INVASÃO FÍSICA OU ELETRÔNICA?

X

Art. 154-A:

Invadir dispositivo informático alheio +

Invadir: "1 Entrar à força[...] 2 Assumir indevidamente ou por violência; usurpar..." (Dicionário Michaelis)

Dispositivo informático: qualquer *hardware* (físico: "aquilo que você chuta") que trate de forma automatizada e tenha capacidade de armazenamento de dados ou informações (informação + automática).

Computador? Celular? Pen Drive? Relógio? Geladeira? *Software*?

- **Mediante violação indevida de mecanismo de segurança +**

Violar: "1. Infringir, quebrantar, transgredir [...] 4. Abrir uma carta destinada a outrem: Violar uma correspondência. 5 Revelar indiscretamente". (Dicionário Michaelis)

- **com o fim de** +

(i) obter
(ii) adulterar ou
(iii) destruir

dados ou informações sem autorização sem autorização do titular

Ou instalar vulnerabilidades para obter vantagem ilícita.

Art. 154-A, §3º. Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

- Se da invasão resultar:

1) A obtenção de conteúdo de comunicações eletrônicas privadas;

Atenção, não é obtenção de dado ou informação, e sim de conteúdo de comunicações.

Lembrando: Lei 9.296/96: Art. 10. Constitui crime realizar **interceptação de comunicações** telefônicas, **de informática ou telemática**, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa.

2) A obtenção de segredos comerciais ou industriais.

3) A obtenção de informações sigilosas, assim definidas em lei, ou

4) O controle remoto não autorizado do dispositivo invadido.

Art. 154-A, §4º. Na hipótese do § 3o, aumenta-se a pena de um a dois terços. Ou seja, reclusão de no mínimo 9 meses e no máximo de 3 anos e 4 meses.

Se houver, a qualquer título

1) a divulgação dos dados ou informações obtidos.

Conflito com o Art. 195 da Lei 9.279/96 (LPI)?

XI - **divulga**, explora ou utiliza-se, sem autorização, de conhecimentos, **informações ou dados confidenciais**, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato;

XII - **divulga**, explora ou utiliza-se, sem autorização, **de conhecimentos ou informações a que se refere o inciso anterior**, **obtidos por meios ilícitos ou a que teve acesso mediante fraude**.

2) comercialização dos dados ou informações obtidos ou

3) A transmissão a terceiro dos dados ou informações obtidos

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Lei 12.737/12 – INVASÃO + PREJUÍZO

Art. 154-A, § 2o Aumenta-se a pena de um sexto a um terço se **da invasão resulta prejuízo econômico.**

Ou seja, pena mínima de 3 meses e 15 dias e máxima de 1 ano e 4 meses de detenção.

- **Formas claras de prejuízo:**
  - Adulteração de um dado ou informação sem a percepção do titular
  - Destruição de um dado ou informação x crime de dano:

Dano, art. 163: destruir, inutilizar ou deteriorar coisa alheia. Pena - detenção, de um a seis meses, ou multa.

  - Invasão e prejuízo e as fraudes bancárias?

Furto simples: reclusão, de um a quatro anos, e multa.
Furto qualificado (mediante fraude): reclusão, de dois a oito anos.
Estelionato: reclusão, de um a cinco anos, e multa

CRIAÇÃO E DISSEMINAÇÃO DE CÓDIGO MALICIOSO

Art. 154-A, § 1º: na mesma pena incorre quem, **com o intuito de permitir a prática da conduta definida no caput**:

(i) **Produz** dispositivo ou programa de computador para invadir dispositivo informático alheio;

(ii) **Oferece** dispositivo ou programa de computador para invadir dispositivo informático alheio;

(iii) **Distribui** dispositivo ou programa de computador para invadir dispositivo informático alheio;

(iv) **vende** dispositivo ou programa de computador para invadir dispositivo informático alheio;

(v) **difunde** dispositivo ou programa de computador para invadir dispositivo informático alheio.

Caput: "Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita".

Interrupção ou perturbação de serviço telegráfico, telefônico, **informático, telemático ou de informação de utilidade pública**

Art. 266. .....
Pena de detenção, de um a três anos, e multa.

§ 1º Incorre na mesma pena quem **interrompe ou impede ou dificulta-lhe o restabelecimento** de:

1) **Serviço telemático**: provedor de acesso, por exemplo.

2) **Informação de utilidade pública**: site do governo, por exemplo. Serviços para os cidadãos (ex.: transporte, telefonia, energia elétrica).

Lei 12.737/12 – Falsificação de Cartão de Crédito ou Débito

Falsificação de documento particular

Art. 298. .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, **equipara-se a documento particular o cartão de crédito ou débito**.

AASP
Associação dos Advogados
São Paulo - desde 1943

O AVANÇO DA TECNOLOGIA

OBRIGADO!!!

RONY VAINZOF
rony@opiceblum.com.br
@ronyvainzof