PHISHING DE INTERNET, COMO CRIMINALIZAR? ASPECTOS TÉCNICOSE JURÍDICOS DESSA AMEAÇA VIRTUAL

INTERNET PHISHING, HOW TO CRIMINALIZE IT? TECHNICAL AND LEGAL ASPECTS OF THIS VIRTUAL THREAT

Beronalda Messias da Silva[1]
Mariana Redondo de Assis[2]

RESUMO

Os crimes cometidos por meio de dispositivos tecnológicos são recheados de peculiaridades que os diferem dos delitos convencionais. O *phishing*, captação de dados eletrônicos obtidos de maneira fraudulenta através da internet, são geralmente tipificados como estelionato ou furto qualificado. Ocorre que as nuances técnicas que envolvem a prática delituosa sugerem outro tipo de tipificação penal, o da lei nº 1.521/51, que dispõe sobre os crimes contra economia popular. Diante das possíveis interpretações que esse novo fato *jus* informático apresenta, o presente artigo propõe aprofundar as características operacionais da "pesca online" de dados, interpretando-a com a idéia de crime que as legislações pátrias pretendem alcançar através de suas normas, buscando (re) pensar o direito a partir dos novos desafios que o avanço tecnológico nos propõe de necessária natureza interdisciplinar.

PALAVRAS-CHAVE: Phishing, crime, estelionato, crime contra a economia popular

ABSTRACT

Crimes committed through technology devices are filled with peculiarities that distinguish them from conventional crimes. Phishing, electronic data capture obtained in a fraudulently way through the internet, is generally typified as embezzlement or larceny. Although the technical nuances that involve criminal practice suggest another type of criminalization, described in law No. 1.521/51, which provides regulation for offenses against public economy. Given the possible interpretations of this new technologic jus facts presents, this article proposes a deeper view of the operational characteristics of "online phishing" of data, interpreting it with the idea of crime that the homeland laws aim to achieve through its standards, seeking to (re)think the law from the new challenges that technological advancement proposes us the necessary interdisciplinary nature.

KEYWORDS: Phishing, crime, embezzlement, crime against the economy

[1] Mestranda em Direito e Inovação pela Universidade Federal de Juiz de Fora.
[2] Consultora de sistemas de conteúdo online e MBA em engenharia de Software pela Universidade de São Paulo – Escola Politécnica

1. INTRODUÇÃO

Nos dias atuais pensar no acesso e na utilização da internet é também pensar em uma forma de se proteger e de tornar seguro o fluxo das informações transmitidas pela *web*. Os ataques aos sites comerciais e as fraudes cometidas aos internautas estão se tornando cada vez mais freqüentes e ardilosos.

Ocorre que nos últimos quinze anos o crime virtual deixou de ser um ato de *hackers* amadores para se transformar em uma séria e organizada indústria criminosa (MOORE, CLAYTON, ANDERSON, 2009, p. 03). Roubos de dados pessoais, senhas de cartões de crédito, furtos eletrônicos, falsidade ideológica são os golpes mais utilizados pelas quadrilhas e fraudadores especializados no ciberdelito.

Inúmeras são as ameaças eletrônicas que podemos encontrar nos ambientes virtuais interconectados, entre as quais, temos o *phishing*, fraude *online* difusa que tem gerado aos Bancos, comércios, governos e usuários comuns enormes prejuízos econômicos e sociais.

Nesse tipo de engodo eletrônico os criminosos geralmente se aproveitam da fragilidade técnica dos internautas (CGI.BR, 2012, p.05), e por meio de engenharia social, induzem os usuários a forneceralguns dados sensíveis ou pessoais, ou até mesmo executar uma série de ações que irão fazer com que o delinqüente tenha acesso às informações confidenciais (OLLMANN,2007, p. 05).

O grande desafio que envolve os novos delitos informáticos é como tipificar, de fato, o cibercrime tem abalado de maneira exorável as estruturas do Direito Penal e levado estudiosos e aplicadores do direito a pensar ou (re)pensar o direito a partir dos novos fatos sociais e informáticos.

No caso especifico do *phishing*, o que se observa é que nem o Código Penal, nem a famosa lei Carolina Dickmann ou o atual código do consumidor tiveram o condão de abarcar a ameaça em suas peculiaridades. Na falta de uma legislação mais completa e especifica, de maneira analógica, é comum que o *phishing* venha a ser enquadrado como crime de estelionato ou furto qualificado.

Dessa maneira, o presente trabalho o visa abordar, especificamente, os aspectos técnicos e jurídicos que envolvem o *phishing* de internet, buscando compreender a ligação entre a prática da “pescagem” virtual com a economia, a fim de tentar responder os seguintes

questionamentos: a tipificação do *phishing* de internet como estelionato é adequada?E como furto qualificado, é apropriada? Não estaria a pratica do *phishing* mais próximo ao crime contra economia popular? Como tipificar?

2. CRIME, ECONOMIA E TECNOLOGIA

Para estudar as origens e as causas da criminalidade, nos últimos dois séculos a criminologia se fundamentou nas descobertas advindas da biologia, da psicologia, da sociologia e da antropologia (VIAPIANA, 2006, p.09). A abordagem econômica do crime, portanto, surgiu somente no final dos anos 60 atravésde alguns estudos que procuraram analisar o comportamento do criminoso a partir do pressuposto econômicoda maximização dos ganhos adquiridos pelo infrator.

O divisor de águas da mudança do paradigma de caráter antropológico e psicológico para o econômico foi o artigo *Crime and Punishment: An Economic Approach* do economista Gary Becker que concebe o crime como u mato racional e entende que o criminoso, ao agir, analisa a probabilidade de ser condenado e a relação entre o custo e o benefício daquele ato.

Para o autor estadunidense, existem dois tipos de crimes, os que almejam vantagem econômica, como o delito de evasão fiscal, do tráfico, do colarinho branco, que se tratam de verdadeiras atividades econômicas ou industriais, e outros de natureza não lucrativa como homicídios, estupros, por exemplo (SHIKIDA, 2010, p. 319).

A partir das idéias de Becker, outros estudos empíricos baseados na teoria da escolha racional foram realizados incluindo, por sua vez, fatores mais estruturais como mercado de trabalho, renda, dissuasão policial, demografia, entre outras variáveis. (CERQUEIRA, LOBAO, 2003, p. 15).

Quando se fala em delitos informáticos, o limite entre direito e economia se apresenta ainda mais visível e indissociável em virtude dos tipos degolpes que encontramos na internet, queobjetivam, em sua grande maioria, vantagem ilícita financeira. As conseqüências desses incidentes são significativas e nos últimos tempos tem gerando profundos impactos econômicos, sociais de ordem pública e privada.

Um estudo promovido pelo CERT.BR revelou que no ano de 2010 os casos envolvendo instituições financeiras chegaram a 7.959 ocorrências no ano, enquanto em 2011 esse número

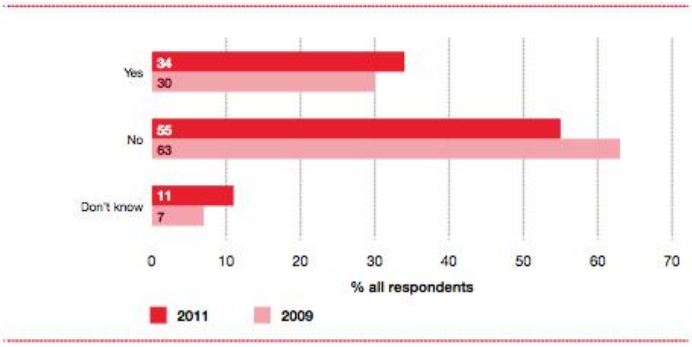
subiu para 11.659 ataques (HOEPERS, 2011, p. 09). Os prejuízos causados por esses tipos de ataques remontam milhares de cifras em todo mundo. Um relatório financiado pela empresa Mcafee revela um pouco desses dados:

Figura 1 - Estatísticas do centro de reclamações de crimes de Internet nos EUA.

Fonte: Associação de pagamentos do Reino Unido, 2007.

Conforme se observa no gráfico acima apresentado, em 2006 a perda anual do Reino Unido ocasionada pelos crimes de internet chegou ao valor aproximado de US$ 264 milhões de dólares. Outra pesquisa mais abrangente encomendada pela PWC em 2010 com 3.877 entrevistados detodo o mundo demonstrou que 34% dos entrevistados já tinham sido vítimasde crime de ordem econômica nos últimos 12 meses, o que representou um aumento de 13% desde o últimalevantamento da empresa realizado 2009:

Figura 2 – Experiência com vitima de crime digital de ordem econômica

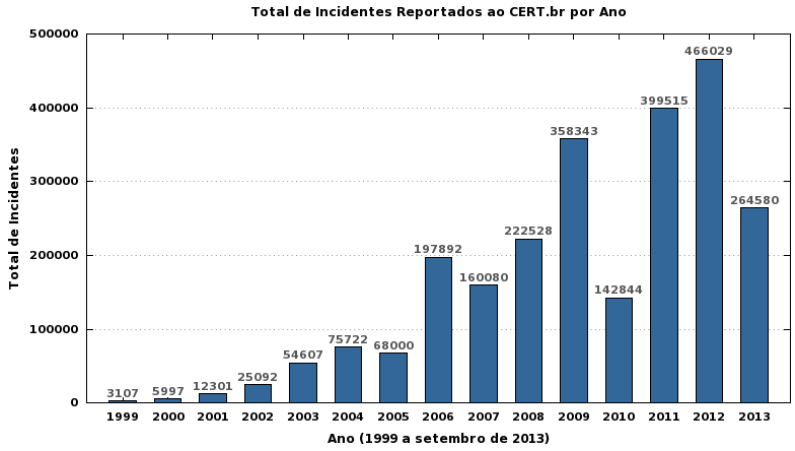


Fonte: PWC, 2011, p. 16

Embora valor da economia do crime cibernético como um todo seja ainda desconhecido, a mais recente estimativa de perdas globais corporativas é que o crime eletrônico já deu um prejuízo no valor de € 7500.00.000.000 por ano (WAINWRIGHT, 2014, texto digital), sendo que os Estados Unidos registraram em 2009 perdas no valor US$ 560 milhões, acima US$ 265 milhões dólares do ano anterior (MISHA, BRYAN, HYPPONEN, WAINWRIGHT, 2010, p.02).

No Brasil, segundo a Federação Brasileira de Bancos (FEBRABAN), os prejuízos financeiros decorrentes das fraudes eletrônicas chegaram a 1 bilhão de reais (2012, p. 42) e osnúmeros de ataques e golpes virtuais no país vem crescendo de maneira alarmante. De acordo com o relatório do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), do ano de 2011 para 2012 os problemas relacionados à segurança da rede passaram399.512 incidentes para 466.029 ocorrências por ano, conforme podemos observar por meio do seguinte gráfico:

Figura 3 – Relatório de incidentes do CERT.BR referente aos valores acumulados: 1999 a setembro de 2013.



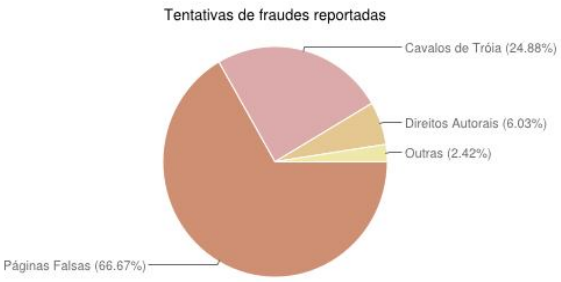
Fonte: CERT.br, 2013

Apesar do ano de 2013 ter tido um relevante decréscimo nos números de incidentes, tal fato não significou necessariamente no aumento da confiança da *web*, vez que a questão concernente à segurança é ainda um problema que aflige as empresas, o governo e, sobretudo, os internautas domésticos.

O relatório CERT.br revelou, ainda, que com relação ao *phishing*de internetno segundo trimestre de 2013 ocorreu um aumento de 41% no número de notificações de páginas falsas de bancos e sites de comércio virtual. Já em relação ao mesmo período de 2012, o aumento

representou quase 63% com relação ao ano anterior. A conclusão do estudoretro mencionado é que o *phishing* clássico continua representando mais da metade das notificações da categoria referenciada, conforme é possível perceber na imagem abaixo:

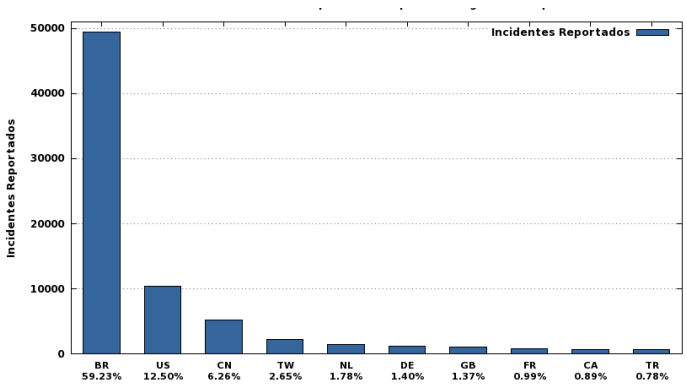
Figura 4 – Gráfico de tentativas de fraudes do CERT.BR referente à' julho a setembro de 2013



Fonte: CERT.br, 2013

E o Brasil é o país que mais aloca IP, ou seja, terminais identificáveis que hospedam esse tipo de fraude:

Figura 5 – Gráfico de origem dos ataques do CERT.BR referente à' julho a setembro de 2013



Fonte: CERT.br, 2013

Da forma que se observa por meio dos dados apresentados, o fenômeno criminal não constitui apenas um problema político e social, mas com muita freqüência os delitos, sobretudos aqueles cometidos pelos meios digitais, atinge de maneira direta a economia do um povo e aquela global.

O fato é que o surgimento de um mercado de *malwares* tem se mostrado algo altamente rentável (MOORE, CLAYTON, ANDERSON, 2009, p. 04) O exponencial e irreversível crescimento dos negócios cibernéticos tem atraído oportunistas, fraudadores e até mesmo criminosos que vêem na internet um campo fértil para as realizações de suas condutas ilegais.

Por ser a internet uma gigantesca e complexa rede virtual, com milhares de rotas e computadores interligados, os crimes cometidos são geralmente difusos e atinge um número indeterminado de usuários. Apesar de o cibercrime ter efeitos abrangentes e esparsos, observa-se muitas vezes que, atrás dos grandes e famosos ataques,encontram-se pequenos grupos e quadrilhas especializadas (ANDERSON, *et al*., 2011, p. 70)

Diante das transformações que os novos meios eletrônicos trouxeram para a vida do consumidor, para uma apropriada análise das implicações jurídicas aos novos fatos jurídico-informáticos, convém abarcar são só os aspectos sociais e jurídicos do crime, visto que, alémdos aspectos técnicos e estruturais da internet, convém abranger também os aspectos micro e macroeconômicos que envolvem os delitos na atualidade.

3. CRIME CONTRA A ECONOMIA POPULAR: UMA LEI QUE PAROU NO TEMPO

A lei que protege a economia popular, inspirada nos moldes do sistema italiano (HORN, 2013. p. 99) surgiu no ano de 1951 com o objetivo de proteger o patrimônio de um número indeterminado de pessoas face às condutas desleais e fraudulentas cometidas por meio deartifícios, monopólios, abusos e especulações (*ibidem*, p. 101) que poderiam lesar o interesse econômicoe o direito patrimonial individual e do povo.

A referida norma foi registrada sob a lei nº 1.521/51 e é um texto composto por 34 artigos no qual estabelecia hipóteses criminosas de ordem econômica popular como, por exemplo,asonegação de mercadoria (I, Art. 2º), além do favorecimento ou preferênciade comprador ou freguês em detrimento de outro (II, Art. 2º),ou mesmo a ausência de nota relativa ao produto ou prestação do serviço (IV, Art. 2º),entre outros tipos penais.

Vários dispositivos da lei, como os acima citados, foram revogados em razão de leis posteriores que prescreveram condutas similares, como a lei nº 8.176/91 que define crimes contra a ordem econômica e cria o sistema de estoques de combustíveis, bem como a lei

7.492/86,que estabelece critérios pra criminalização de atos contra o sistema financeiro nacional, esobretudo pelo surgimento Código de Defesa do Consumidor que fez com que vários incisos e artigos da lei fossem definitivamente revogados.

Diante de tantas normas esparsas que vieram posteriormente à lei de crimes contra economia popular, prevendo situações análogas ou similares, em que pese a sua importância para a tutela econômica do cidadão e do povo, umas das conseqüências desse sobrestamento legislativo foram o fato da norma ser deixada de lado e transformada em uma lei sem muita importância, (BATISTI, 2009, p. 20), tornando-se uma norma relegada ao esquecimento (FRAGOSO, 1980, p. 05), fato este culminado com surgimento de novas leis esparsas no lugar.

Apesar de ser não mais utilizada em sua plenitude, cumpre destacar que a lei de crimes contra a economia popular não foi totalmente revogada, e do ponto de vista da técnica jurídica, ela é perfeitamente válida. O fato é que a lei n. 8.137/90 e as demais normas espalhadas não tiveram força suficiente para expelir de vez a lei n. 1.521/51 do ordenamento jurídico brasileiro. Entre alguns dos importantes dispositivos que ainda estão em vigor, destacamos o IX do artigo 2º que trata do ilícito contra o povo mediante especulações e fraudes em desfavor da economia popular:

> Art. 2º. São crimes desta natureza:
>
> IX - obter ou tentar obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos ("bola de neve", "cadeias", "pichardismo" e quaisquer outros equivalentes); (BRASIL, 1951).

Sobre a referida previsão, inobstante osupracitado artigo citar três tipos de fraudes, a saber: “bola de neve”, “cadeias” e “pichardismo”, o entendimento doutrinário e jurisprudencial predominante é no sentido de abranger outras espécies além destas (FERNANDES, 1990, p. 86), tornando, portando, abrangente a sua aplicação e proteção.

Outrossim, em que pese previsão descrita no inciso IX do artigo 2º lei n. 1.521/51 ser muito semelhante ao crime estelionato previsto no art. 171 do Código Penal (“obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento”), elas diferem uma da outra em uma questão nuclear referente ao sujeito passivo da ação.

De fato, no caso do estelionato, pra que seja caracterizada a conduta, é necessário que o sujeito passivo seja pessoa determinada, caso contrário, o delito poderá ser classificado e

adequado na lei de economia popular ou até interpretada à luz do código de defesa do consumidor (GRECO, 2000, p. 241)

Diante de todo esse histórico legislativo apresentando, a questão quem vem à tona é se, com as transformações que os novos meios eletrônicos trouxeram para a vida contemporânea, é possível saber se as leis acompanharam o tempo e se estão adequadas.

No caso da lei n. 1.521/51, embora tenha sido relegada ao esquecimento, quando se trata dos novos fatos delituosos informáticos, haja vista a *intentio legis* da proteção contra processos fraudulentos contra pessoas indeterminadas, a lei se apresenta mais do que nunca atual e adequada.O motivo se dá sobretudo pelo fato da arquitetura da internet facilitar condutas criminosas esparsas e indiscriminadas

4.*PHISHING*, COMO CRIMINALIZAR?

Consoante foi explicado anteriormente, *phishing* é um delito informático que consiste na obtenção fraudulenta de informações confidenciais dos usuários da internet. A expressão deriva do inglês *fishing*, que na língua portuguesa significa pescar.

São diferentes os modos pelos quais os cibercriminosos agem, mas em linhas gerais, a conduta consiste na captação ilícita mediante especulações ou processos fraudulentos onde o internauta é induzido a acreditar que necessita fornecer dados que posteriormente são utilizados por quadrilhas ou pessoa mal intencionada.

Os meios mais utilizados nesse tipo de fraude são a aparente comunicação oficial, geralmente realizada por e-mail, bem como as páginas falsas ou clonadas da internet onde a vítima, sem ter a consciência do perigo, acaba passando dados sensíveis e confidencias, ou até mesmoquando o internauta, seja por curiosidade, por caridade ou pela possibilidadede obter alguma vantagem financeira (CGI.BR, 2012, p. 09) acaba sendo vítima de golpe eletrônico.

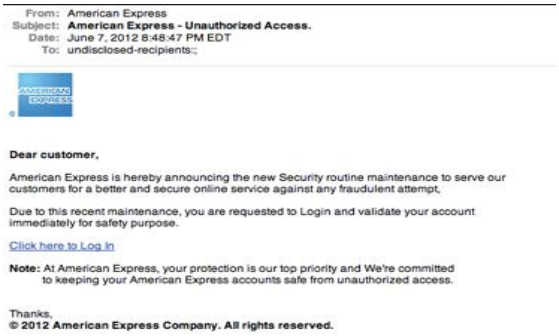
Outros ataques que nãosão muito conhecidos, mas que também acontecem, são os voltados para o sistema de SMS, conhecido como *smishing*, ou aqueles feitos por meio de telefonema, batizado, por sua vez, de*vishing* (DIEZ, 2013, texto digital).

Registra-se, também, que os ataques não se restringem aos computadores pessoais de usuários domésticos, existe ainda outro tipo do *phishing* conhecido como *pharming* no qual o servidor DNS (*Domain Name System*) é "envenenado" e as configurações relativas ao

endereço *web* são alteradas e os internautas, mesmo digitando o endereço correto, poderão ser direcionados para um site falso (CGI.BR, 2012, p. 11).

Em virtude características arquitetônicas e globalizadas da internet, que permite que criminosos cheguem a um maior número de potenciais vítimas (EETEN, BAUER 2008, p. 16), assim acontecem com os *spams,*o envio de mensagens no *phishing* são feitas de maneira massiva e sem saber ao certo que é o titular daquele e-mail ou quem esta atrás do IP do usuário, o que resulta na de difícil a identificação dos afetados.Portanto, na prática de *phinshing*, as vitimas são, *a priori*, não identificadas, e nos casos do delito praticado por meio do correio eletrônico, apesar de parecer pessoal, os envios dessas mensagens são geralmente indiscriminadas:

Figura 6 – Exemplo de envio de *phishing* encaminhado por e-mail



Fonte: DEGRIPPO, 2013.

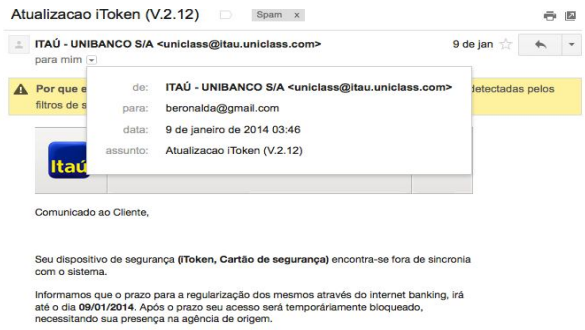
Observa-se na imagem acima que no campo dedicado ao destinatário, expresso em inglês pela palavra “to”, encontramos escrito “undisclosed recipients”, que significa que os destinatários do e-mail foram ocultados, alem do mais, o e-mail não foi verdadeiramente destinado ao usuário,vez que aparece na mensagem “dear customer” (caro cliente), ao invés do nome do titular do e-mail enviado.

Contudo, destaca-se que na medida em que tais artimanhas estão sendo descobertas, os *phishing*tem se utilizado de técnicas de programação e outros tipos de ameaças a fim de ludibriar ainda mais internauta e fazer que todo o procedimento executado pareça legitimo.

Uma das estratégicas utilizadas é através do emprego de spam “zombies”, que são computadores que foram comprometidos por códigos maliciosos como *worms*, *bots*, vírus ou cavalos de tróia (CERT.br, 2012, p.120)e que permitem que criminosos utilizem as máquinas afetadas para o envio de mensagens, utilizando muitas vezes a lista de contato pessoal do

internauta. Na imagem abaixo tem um e-mail *phishing*supostamente enviado pelo Banco Itaú para um e-mail existente e pessoal, mas que na verdade foi enviado de maneira indistinta para vários usuários.

Figura 7 – Email phishing enviado supostamente pelo Banco Itaú



Fonte: *print screen* da aplicação no sistema operacional Mac OS X 10.9.1

Independente da técnica utilizada, o fato é que, quando se fala de *phishing*,o intuito de quem produziu o ataque é sempre mal intencionado (MOORE, CLAYTON, ANDERSON, 2009, p. 04). Diante do crescimento da ameaça que a prática de apreensão ilegal de dados tem gerado, alguns países correram no sentido de estabelecer duras regras para esse tipo de atentado, tutelando de maneira direta os *phishingonline*. Nos EUA, por exemplo, alguns estados já procuram criar uma proteção legal contra a fraude:

Quadro1 – legislação sobre o *phishing* em alguns estados americanos

ESTADO	LEI	TUTELA	PENA/RESPONSABILIZACAO
Alabama	Código Alabama Secção 13A-8-114	Direta (protege contra o crime de *phishing*)	Penal e Cível no valor de (US$ 25.000), ou o que for maior
Arkansas	Código Arcak§ 4-111-102, 4-111-103	Direta (protege contra o crime de *phishing*)	É culpado com a classe 5 de crime e reparação civil por perdas e danos
Califórnia	Código Cal. § § 22948-22.948,3	Direta (protege contra o crime de *phishing*)	Penal e Cível no valor de US$ 5.000 até US$ 500.000, ou no valor ou três vezes a mais do dano.
Geórgia	Código Ga § 16-9-93.1	Proteção dos dados	Passível de responsabilização penal e reparação cível monetária
Illinois	Lei Anti-Phishing. (740 ILCS 7 /)	Direta (protege contra o crime de *phishing*)	Penal e Cível no valor de US$ 5.000 até US$ 500.000, ou no valor ou três vezes a mais do dano.
Michigan	MCL § 445.67[a]	Direta (protege contra o crime de *phishing)*	US$ 5.000,00 por infração. (Ii) $ 250.000,00 para cada dia em que ocorrer uma violação.
Nova Iorque	NY general§ 390-b anti-phishing	Direta (protege contra o crime de *phishing*)	Ressarcimento, podendo ser multiplicado por 3, ou 10 mil dólares para cada instância em que a identificação informações são

			solicitadas ,
Rhode Island	RI Gn Leis §§ 11-52.1-1 a -5	Crime de deturpação Internet da Lei Afiliação negócio.	Pena de prisão não superior a cinco (5) anos, ou multa de não mais de cinco mil dólares (US$ 5.000) por ofensa , ou ambos.
Tennessee	Código Tennessee§ 47-18-5201 a 47-18-5205	Proteção dos dados	crime declasse 5. Seo roubo deserviços de informáticaestá avaliada emUS$ 2.500 oumais, eleé culpado de umcrime de Classe6. Ressarcimento por danos e lucros cessantes

Fonte: NCSL, 2013.

Da mesma forma a União Européia (UE) há anos tem procurado combater os delitos informáticos e um dos passos mais significativos foi em 2001 quando o Conselho da Europa, juntamente com a participação de alguns Estados signatários, na ocasião Canadá, Japão, África do Sul e USA, reuniram-se em Budapeste para discutir os problemas que envolviam os crimes cibernéticos.

Nesse encontro restou decidido que cada estado membro adotaria as medidas legislativas necessárias (UNIAO EUROPÉIA, 2001, p. 04) e dariam apoio colaborativo para combater o cibercrime sempre que fosse necessário. Atendência internacional se desenvolve no sentido da aplicação de leis cada vez mais duras diante da tomada de consciência das graves conseqüências que ciberdelito traz.

No Brasil um marco contra os crimes praticados na internet foi com a promulgação da lei nº 2.737/2012, conhecida também como lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de delitos informáticos e inseriu no Código Penal mais três previsões delitivas, a saber: a) invasão de dispositivo informático (art. 154-A); b) interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (art. 154-B); c) falsificação de documento particular de cartão (art. 266, §1º §2º e art. 298, respectivamente).

A norma ganhou popularmente o nome da atriz em razão de algumas fotos íntimas que foram furtadas do seu computador pessoal e divulgadas na internet, tratando-se, portanto, de um caso de foro pessoal com repercussão nacional em razão da sua fama. Nessa lei, a preocupação do legislador foi de proteger a intimidade, bem como a proteção dos dados contra invasão eletrônica, todavia, conceito de invasão não se encaixa perfeitamente na idéia *phishing*, vez que, nesse caso, a fraude eletrônica ocorre na medida em que o internauta é levado a acreditar na legitimidade da mensagem ou do site, e passa, com isso, a fornecer os seus dados.

Foi em razão da falta de alcance lei n. 2.737/2012 na proteção de vários crimes virtuais que o deputado Eduardo Azeredo apresentou na Câmera dos Deputados o Projeto de Lei n. 5.485/2013 que dispõe sobre a tipificação criminal do estelionato informático. Em suas razões legislativas, o deputado afirma:

> Essas novas tecnologias se valem de vulnerabilidades dos navegadores de Internet que permitem o download e a execução de programas de computador hospedados em *web sites* hostis. Sendo assim, fica evidente a necessidade de uma atualização do Código Penal Brasileiro que venha a estabelecer uma tipificação penal relativa ao *phishing*, ou estelionato informático, de forma a desencorajar esse tipode prática.Uma disposição dessa natureza não foi estabelecida nas recentes legislações editadas sobre o assunto - Lei nº 12.737, de 2012 –conhecida como Lei Carolina Dieckmann, e Lei nº 12.735, de 2012. Este Projeto de Lei, portanto, introduz no Código Penal uma tipificação penal específica que tipifica como crime a prática de difusão de mensagens eletrônicas com o intuito de obter dados pessoais, números de cartão de crédito, senhas, usuários de acesso, de forma fraudulenta (CONGRESSO NACIONAL, 2010)

Nesse projeto de lei a proposta é inserir no artigo 171 do Código penal Brasileiro, que prevê o estelionato, a punição para a pratica de *phishing*, conforme o texto abaixo.

> Art. 2º O artigo 171 do Decreto Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) passa a vigorar acrescido do inciso VII, com a seguinte redação
> "Estelionato informático
> Art.
> 171.....
> §2º Nas mesmas penas incorre quem:
> .....
> VII – envia mensagens digitais de qualquer espécie,fazendo-se passar por empresas, instituições ou pessoas a fim de induzir outrem a revelar informações pessoais, de identidade, ou senhas de acesso ."((CONGRESSO NACIONAL, 2010).

Ocorre que as características técnicas que envolvem os *phishing* de internet são importantes para repensar essa visão que o projeto de lei nos dá. Como já comentado por diversas vezes no presente artigo, o *phishing* é processo fraudulento para obtenção de ganhos ilícitos de um número indeterminado de pessoas, e por essa razão, ele não pode ser interpretado como estelionato, uma vez que, para que ocorra a caracterização descrita no art. 171 do Código penal, é necessário que a que as vítimas sejam pessoas determinadas, e em caso contrário, deverão ser enquadradas no crime contra economia popular (GRECO, 2000, p. 241) ou eventualmente adaptadas na lógica da relação de consumo, quando aplicável.

Outro entendimento que tem se cristalizado, dessa vez pela orientação jurisprudencialdo Superior Tribunal de Justiça (STJ), é no sentido de considerar as fraudes cometidas pela internet como furto qualificado, sobretudo, nas hipóteses de estornos criminosos nas contas bancaria e mediante a clonagem de cartão de credito do usuário.

Contudo, é importante destacar que na maioria dos casos julgados pelo STJ não há a participação da vitima no golpe, que percebe que foi furtada eletronicamente no momento ulterior ao fato (CABETTE, 2012, texto digital). Por essa razão, não podemos confundir com a pratica de *phishing*, nem mesmo com o estelionato.

Por fim, diante de todas as questões de natureza interdisciplinar levantadas, no caso de *phishing*, passamos a adotar o art. 2º, inciso IX, da lei n. 1.521/51 como a norma mais adequada, considerando a sua intenção de tutela ao patrimônio de um número indeterminado de pessoas contra especulaçõese processos fraudulentos contrária à economia popular.

Porém, o entendimento aqui apresentado possui uma gama de obstáculos pragmáticos, entre elas, a relação do valor da pena com a importância do crime comentado. A pena quem incide o art. 2, inciso IX, é de 6 (seis) meses a 2 (dois) de detenção mais multa de dois mil a cinqüenta mil cruzeiros. Antes de tudo, para ser aplicada, a lei precisa ser atualizada.

Além disso, no caso do *phishing*, os crimes causam impactos vultuosos e estamos tratando, muitas vezes, de crimes praticados por quadrilhas especializadas. Se observarmos as atuais legislações dos outros países, como os Estados Unidos, por exemplo, iremos constatarque a média de punição é de cinco anos, além da compensação monetária.

Na aplicação do concurso de crime, a lei contra o sistema financeira necessita também se atualizada e antenada aos novos delitos informáticos. A lei n. 7.492, que define os crimes contra o sistema financeiro nacional, é de 1986, ou seja, muito antes da explosão das novas facetas dos delitos que passaram a ser digitais.

Talvez a saída interpretativa de enquadrar o *phishing* como estelionato ou furto qualificado se deu em razão da ausência de legislação adequada e atualizada. Porém, (re)pensar o direito nessa perspectivaé refletir sobre asmudanças queavançotecnológico nos propõe na contemporânea era digital.

5. CONCLUSÃO

Da mesma forma que o surgimento da internet trouxe comodidade e facilidadepara a vida do homem contemporâneo, a maior rede de computadores fez com que os usuários na rede começassem a conhecer um universo novo de ameaças e vulnerabilidades

A virtualização da vida e da explosão da denominada economia “sem papel” têm trazido reflexos concretos no âmbito penal e do fenômeno da criminalidade com a formação de verdadeiras quadrilhas organizadas que tem abalado as estruturas econômicas e sociais na contemporaneidade.

A *priori*, pelas razões anteriormente apresentadas, em decorrência das nuances técnicas que envolvem o *phishing*, que atinge um número indeterminado de pessoas através de processos fraudulentos eletrônicos onde o internauta é induzido a acreditar que necessita fornecer dados, o ataque virtual sugere outro tipo de tipificação penal diferente do estelionato, que para a sua caracterização necessita que o sujeito passivo seja pessoa determinada, e o furto qualificado, que pressupõe a não participação efetiva da vítima durante o ato.

Portanto, em alguns casos que envolvem o *phishing*, a interpretação que nos parece mais apropriada é o da lei nº 1.521/51 por ser o crime caracterizado pela obtenção ou tentativa, mediante especulações ou processos fraudulentos, de obtenção de ganhos ilícitos em detrimento do povo ou de número de pessoas indeterminadas.

Sobre a adequada interpretação com relação ao *phishing*, o presente artigo não teve a pretensão de encerrar o assunto sobre a temática, nem mesmo esgotar a literatura existente sobre a referida prática, mas o objetivo aqui foi de levantar algumas problemáticas acerca das características técnicas do delito, propondo uma visão mais orgânica e interdisciplinar sobre um fenômeno que vem perturbando a macro economia, tanto quanto a economia popular.

6. REFERENCIAS BIBLIOGRÁFICAS

ANDERSON, Ross, BARTON, Chris, BOHME, Rainer, etc all. **Measuring the black web; cybercrime. (How big is criminality on the web?)**The Economist [0013-0613] ano: 2011 vol: 401 fasc: 8755 pág: 69. Disponível em: <http://www.economist.com/node/21532263>. Acesso em: 10 jan 2014.

BECKER, Gary S. Crime and Punishment: aneconomic approach. In: BECKER, Gary S; LANDES, William M. (Eds.) Essays **in the Economicsof crime and Punishment [S.l.]: National of Economic Research,** 1974. p. 154. Disponível em: http://www.nber.org/chapters/c3625.pdf
Acesso em: 12 dez 2013.

BRASIL. Lei nº 12.412/12, de 9 de junho de 2011. **Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Portal da Legislação**. 10 jun. 2011. Disponívelem: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm>. Acesso em: 10 jan 2014.

BATISTI, Leonir. **Curso de Direito Processual Penal.** Curitiba: Juruá, 2009. 4 vol.

CABETTE, Eduardo Luiz Santos. **Furto mediante fraude e estelionato no uso de cartões de crédito e/ou débito subtraídos ou clonados,** 2012. Disponível em: http://www.egov.ufsc.br/portal/conteudo/furto-mediante-fraude-e-estelionato-no-uso-de-cart%C3%B5es-de-cr%C3%A9dito-eou-d%C3%A9bito-subtra%C3%ADdos-ou-c

CERQUEIRA, Daniel. LOBÃO, Waldir. **Determinantes da criminalidade: uma resenha dos modelos teóricos e resultados empíricos. IPEA - exto para discussão nº 956. Rio de janeiro**, jun. 2003. Disponível em: <http://www.ipea.gov.br/portal/images/stories/PDFs/TDs/td_0956.pdf> Acesso em: 12 dez. 2013

CERT.br. **Índices reportados ao CERT.br.** Juho a Setembro de 2013. Disponível em: <http://www.cert.br/stats/incidentes/2006-jan-dec/tipos-ataque-acumulado.html>. Acesso em 15 jan 2014.

CGI.BR. **Cartilha de Segurança para Internet. Comitê Gestor da Internet no Brasil,** 2012. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf >. Acesso em: 11 dez. 2013.

CONGRESSO NACIONAL. Projeto de Lei nº PL 84/99. **Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providência**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>.
Acesso em: 18 nov. 2013.

FEBRABAN, Federação Brasileira de Bancos. **CIAB FEBRABAN 2012 – A Sociedade Conectada,** 2012. Disponível em: http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Pesquisa%20CIAB%20FEBRABAN%202012.pdf.> Acesso em: 11 dez. 2013.

DEGRIPPO, Sherrod. **Phishing Protip: Don't Send to All, 2013**. Disponível em: <http://www.sherrod.im/89/phishing-protip-dont-send-to-all/>. Acesso em: 07 jan 2014.

DIEZ, Almudena Congil. **Phishing. Problemática relativa a la calificación jurídica de laparticipación de los denominados "mulerosbancarios". Estado actual de nuestra doctrina y jurisprudência.** 2013, Disponivel em: http://www.elderecho.com/penal/Phising-

Problematica-calificacion-participacion-jurisprudencia_11_533680004.html*f*>. Acesso em: 11 dez 2013. 2013.

EETEN, Michel J. G., BAUER, Johannes M Economics **of Malware: Security Decisions, Incentives and Externalities, (2008).**Report for the Organization of Co-operation and Development (OECD). Disponível em: <http://www.oecd.org/internet/ieconomy/40722462.pdf>. Acesso em: 11 dez. 2013.

FRAGOSO, Heleno Cláudio. **Direito penal econômico e direito penal dos negócios**, 1980. Disponivel em:<http://www.egov.ufsc.br/portal/sites/default/files/anexos/11344-11344-1-PB.pdf> Acesso em: 07 jan 2014.

FERNANDES, Antonio Scarance . **Considerações sobre o vídeo pôquer como atividade criminal.** Justitia (São Paulo), v. 52, p. 84-92, 1990. Disponível em: http://www.justitia.com.br/revistas/x722dx.pdf. Acesso em 15 jan 2014.

GRECO FILHO, Vicente . **Algumas observações sobre o direito penal e a internet**. Revista de Direito Mackenzie, v. 1, p. 35-39, 2000.
HOEPERS, Cristine. **Fraudes via Internet –. *Estatísticas e Tendências.*** 2011. Disponível em: <http://www.cert.br/docs/palestras/certbr-forum-comercio-eletronico2011.pdf>

HORN. Manuela Bittar. **O duplo nível de legalidade e os crimes contra a economia popular no direito penal autoritário.** Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Jurídicas, Programa de Pós-Graduação em Direito, Florianópolis, 2013.

OLLMANN, Gunter. **The phishing guide: understanding & preventing phishing attacks.**2007, Disponível me: < http://www-935.ibm.com/services/us/iss/pdf/phishing-guide-wp.pdf>. Acesso em: 15 jan 2014.

MOORE, Tyler.; CLAYTON, Richard .; ANDERSON, Ross. The Economics of online crime. **Journal of Economic Perspectives,** v. 23, n. 3, p. 3-20, nov./dec. (2009)

MISHA, lenny, BRYAN, Glick, HYPPONEN, Mikko H.; WAINWRIGHT. **Robert Cybercrime, Cybers security and the Future of the Internet. Session Handouts, Global Economic Symposium** 2010 (GES), 27-29 September 2010, Istanbul, Turkey. Disponível em: http://www.econstor.eu/bitstream/10419/79125/1/729547698.pdf> Acesso em: 01 fev 2014.

NCSL, **State Laws Addressing "Phishing**", 2013 Disponível em:<http://www.ncsl.org/research/telecommunications-and-information-technology/state-phishing-laws.aspx>. Acesso em: 01 fev 2014.

PWC. **Cybercrime: protecting against the growing thre a Global Economic Crime Survey** 2011 Disponível em: <https://www.pwc.com/en_GX/gx/economic-crime-survey/assets/GECS_GLOBAL_REPORT.pdf>

UNIAO EUROPEIA, **Convenção sobre o cibercrime**, 2001, Disponivel em: <http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/ETS_185_Portugese.pdf>. Acesso em: 02 fev 2014. Acesso em: 01 fev 2014.

VIAPIANA, Luiz Tadeu. **Economia do Crime: Uma Explicação para a Formação do Criminoso**, Porto Alegre: 2006, AGE Editor

SHIKIDA, Pery Francisco Assis. In: **Economic Analysis of Law Review**. Brasília, v 1 n 2 p. 424-jul-dez.2010. Disponível em: <http://portalrevistas.ucb.br/index.php/EALR/ article/viewArticle/ 1%20EALR%20318.>. Acesso em: 15 jan 2014.

WAINWRIGHT, Robert. Proposal – **Dealing with Cyber crime – Challenges and Solutions.** Disponível em http://www.global-economic-symposium.org/knowledgebase/the-global-polity/cybercrime-cybersecurity-and-the-future-of-the-internet/proposals/dealing-with-cyber-crime-2013-challenges-and-solutions. Acesso em: 01 fev 2014