O ENQUADRAMENTO JURÍDICO PENAL DO PHISHING E SUAS REPERCUSSÕES NO FURTO INFORMÁTICO

Rebeca Bravo de Oliveira Gomes[1]
Marcelo Sarsur Lucas da Silva[2]
Banca examinadora**

RESUMO: A criminalidade informática é um fenômeno bastante recente que trouxe consigo modalidades criminosas que não se amoldam àquelas previstas no Código Penal brasileiro, como é o caso do ***phishing***. Desse modo, o objetivo deste estudo é tecer uma análise jurídica do tema, a fim de se estabelecer qual o tratamento penal mais adequado para a pesca de dados de identidade por meio da Internet.

PALAVRAS-CHAVE: ***Phishing***, criminalidade informática, Direito Penal, estelionato eletrônico, furto informático, tipificação penal.

1 INTRODUÇÃO

O avanço tecnológico que se tem experimentado nas últimas décadas não trouxe apenas bons frutos: ele fez também com que a criminalidade informática aumentasse exponencialmente. O Direito Penal, porém, ressalvadas algumas melhorias na legislação, não acompanhou tal progresso, de modo que os estudos jurídicos sobre o tema são extremamente escassos.

São várias as modalidades de crimes informáticos e de condutas fraudulentas cometidas com o auxílio de dispositivos informáticos que não possuem tratamento adequado no ordenamento jurídico pátrio. Optou-se, aqui, pelo estudo de uma conduta específica: a da "pesca" online de dados de identidade – o phishing.

Assim, investigar-se-á a exata natureza jurídica do phishing, a fim de lhe dar correta capitulação no âmbito do Direito Penal, abordando, ainda, quais as repercussões jurídicas deste fenômeno e estabelecendo, um tipo penal adequado para tal conduta delituosa e, por conseqüência, para o furto informático.

2 A CRIMINALIDADE INFORMÁTICA

Uma das maiores características da denominada "Era Digital", nas lições do sociólogo Ivanir Corgosinho, foi a substituição da comunicação face-a-face pela comunicação mediada por computadores. As vantagens advindas desse novo método de interação trouxeram mudanças significativas em vários setores sociais, notadamente nas relações financeiras dos indivíduos. Segundo o autor,

> *os benefícios econômicos e operacionais dos processos de transmissão de dados via computadores conectados em rede, em termos de rapidez e segurança, levou a que as principais transações comerciais do mundo passassem a operar com base em uma mesma plataforma lógica e via os mesmos tipos de equipamento. (CORGOSINHO, 2005, p. 6)*

Ainda nas lições do sociólogo, a inauguração desse novo paradigma, traduzido no uso intensivo dos recursos informáticos, vem gerando um profundo impacto no cotidiano das sociedades contemporâneas, que passa a funcionar sob a lógica da comunicação online. O Direito, por sua vez, reconhecendo esses impactos, tem empenhado um enorme esforço para assegurar que os direitos e garantias fundamentais, elencados na Constituição Federal de 1988, não deixem de ser tutelados também no ambiente virtual, conforme se extrai, por exemplo, da recentíssima Lei 12.965/2014, apelidada de Marco Civil da Internet.

No âmbito jurídico-penal, a criminalidade informática tem se mostrado como um dos vários frutos do avanço da tecnologia da informação, de tal sorte que os bens jurídicos ofendidos por essas condutas carecem igualmente da tutela penal, conforme dispõem Túlio Vianna e Felipe Machado, na obra "Crimes Informáticos":

> *a inviolabilidade de informações e de dados informáticos é decorrência natural do direito à intimidade e privacidade, devendo, portanto, ser reconhecida como direito essencial para a convivência social. Como corolário desse direito, a inviolabilidade das informações automatizadas, ou seja, daquelas armazenadas e processadas em dispositivos informáticos, surgirá então como um novo bem jurídico a ser tutelado pelo Direito Penal, de forma a se garantir a privacidade e a integridade dos dados informáticos. (VIANNA, MACHADO. 2013, p. 16)*

Dessa forma, mesmo que a Lei 12.737/2012 - Lei Carolina Dieckmann - tenha representado um avanço em termos de legislação penal, ela ainda não foi suficiente para normatizar toda a criminalidade informática, razão pela qual se torna indispensável o estudo e a reflexão do tema, sendo que se optou aqui, especificamente, pela análise de uma das várias modalidades de "cibercriminalidade", qual seja, a pesca de informações pessoais e sigilosas através de dispositivos informáticos – o ***phishing***.

3 O QUE É O *PHISHING*

Phishing é o nome dado à pesca online de identidade, praticado com o objetivo de obter-se vantagem econômica indevida por intermédio da Internet. Em geral, os ***phishers*** (nome dado aos agentes que praticam tal conduta), agem enviando e-mails fraudulentos – passando-se por instituições financeiras, ou por órgãos públicos, ou por serviços de crédito - para uma enorme quantidade de pe ssoas, tudo com o fim de "pescarem" suas informações pessoais, tais como número do cartão de crédito e senha.

Importante descrever, de modo geral, como é feita tal "pesca", já que se deve ter em mente que o ***phisher*** não invade o computador do usuário, mas sim o induz, de modo ardiloso, a conceder-lhe suas informações pessoais. Ademais, o conhecimento do caminho percorrido pelo agente até que este consiga obter a vantagem econômica da vítima irá influenciar sobremaneira na capitulação, por exemplo, do "furto informático", também objeto deste estudo.

Dessa maneira, há casos em que o criminoso envia os e-mails, se fazendo passar por uma instituição financeira e solicitando atuali-

zação de cadastro. Para tanto, será indicado um link como sendo o do site do Banco, que direcionará a vítima para um site falso idêntico ao original, onde então irá inserir seus dados pensando tratar-se de uma página confiável.

Em outras vezes, de forma um pouco diferente, mas com o mesmo objetivo, o criminoso poderá enviar e-mails contendo apenas um link ou um arquivo que descarregará um programa malicioso no computador da vítima e que nele ficará alojado até que o usuário tente acessar a página da sua instituição financeira. O programa malicioso irá substituir o atalho dos favoritos no computador do usuário, de modo que este, também nestes casos, será direcionado a uma página falsa quando tentar acessar a página do seu Banco.

4 O *PHISHING* NO ORDENAMENTO JURÍDICO BRASILEIRO

Em relatório recente[3], a Trend Micro, empresa especializada em segurança, apurou que o Brasil está entre os países que registram maior número de vítimas de phishing no mundo (8,15%), ficando atrás apenas dos EUA (38,38%) e Japão (8,28%). Não obstante, tal conduta delituosa só chega ao conhecimento do Poder Judiciário quando o furto das contas bancárias dos usuários de internet banking já foi consumado, dando a perceber que a pesca de identidade, considerada isoladamente, não vem recebendo a devida atenção da doutrina e jurisprudência, além de não ter sido ainda normatizado pelo Direito.

A conseqüência disso é que o phishing acaba sendo sempre atrelado às figuras do furto ou do estelionato, quando em outros países, por exemplo, há quem defenda que este seja um crime autônomo (em Portugal, poderia configurar-se crime de falsidade informática).

A esse respeito, chama-se atenção para o Conflito de Competência nº 72.738/RS, de Relatoria da Ministra Maria Thereza de Assis Moura, que atrela o phishing ao furto qualificado por fraude e para Projeto de Lei 5485/2013, de autoria do Deputado Eduardo Azeredo, que propõe a tipificação do phishing como estelionato, os quais serão analisados mais cuidadosamente a seguir.

5 DAS CONDUTAS CRIMINOSAS ATRELADAS AO PHISHING

5.1 Do Furto Qualificado Por Fraude

O Código Penal assim dispõe sobre o furto qualificado por fraude:

Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:

Pena - reclusão, de um a quatro anos, e multa.

[...]

§ 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:

[...]

II - com abuso de confiança, ou mediante fraude, escalada ou destreza;[...]

Nas lições de Nelson Hungria (1967, p. 43-44, apud GRECO, 2014, p. 27), pratica furto mediante fraude aquele que subtrai coisa alheia móvel, utilizando-se de ardil que provoque a ausência momentânea do ***dominus*** ou distraia a atenção da vítima para tornar mais fácil a consumação do furto. Ou seja, a fraude é praticada para que o próprio agente subtraia a coisa.

O CC nº 72.738/RS trata de transferências eletrônicas fraudulentas realizadas por meio de ***internet banking*** da Caixa Econômica Federal. No caso apresentado, houve conflito quanto à competência para processar e julgar a conduta, já que um juízo considerou ser o caso de furto qualificado por fraude, donde seria competente o lugar onde se consumar a infração, ao passo que o juízo declinado entendeu se tratar de estelionato, sendo competente, portanto, o juízo do local onde houve a obtenção da vantagem patrimonial indevida.

Em sua decisão, assim se pronunciou a Ministra Relatora:

O cerne da questão para se determinar o Juízo competente para o prosseguimento do caso em tela reside, pontualmente, na correta capitulação da conduta criminosa em comento.

O furto mediante fraude, escalada ou destreza não se confunde com o estelionato. No primeiro, a fraude visa a diminuir a vigilância da vítima, sem que esta perceba que está sendo desapossada; há discordância expressa ou presumida do titular do direito patrimonial em relação à conduta do agente. No segundo, a fraude visa a fazer com que a vítima incida em erro e, espontaneamente, entregue o bem ao agente; o consentimento da vítima integra a própria figura delituosa.

Da análise dos autos, verifica-se que trata de hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de três mil e quatrocentos reais de conta bancária situada em Porto Alegre/RS, por meio da Internet Banking da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima.

A fraude, de fato, foi usada para burlar o sistema de proteção e vigilância do Banco sobre os valores mantidos sob sua guarda, configurando, assim, crime de furto qualificado por fraude, e não estelionato (STJ, CC nº 72.738, RS 0226850-1/2006, Rel. Ministra Maria Thereza de Assis Moura, j. 08/08/2007, Dj 20/08/2007).

A importância da análise deste julgado, como já exposto, advém do fato de que o ***phishing*** é cometido sempre com o fim de obter vantagem econômica, muitas vezes com o furto das contas bancárias das vítimas.

Como não há ainda tipificação penal para a pesca dos dados de identidade, o Judiciário somente registra litígios em que há a subtração do dinheiro, pouco importando o ***modus operandi*** utilizado para tal. Dessa forma, como o real sujeito passivo do furto seria a instituição financeira (que possui os valores sob sua guarda), não há que se falar, com razão, em estelionato, que pressupõe o consentimento da vítima – o que por óbvio não houve. Conforme se extrai do voto proferido acima, o agente burlou o sistema de proteção e vigilância do banco para retirar o dinheiro mantido sob sua guarda, o que, de fato, caracterizaria fraude, assistindo razão ao Superior Tribunal de Justiça.

5.2 Do Estelionato

Em relação ao estelionato, dispõe o Código Penal:

Art. 171 - 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:

Pena - reclusão, de um a cinco anos, e multa.

A fraude para Greco (2014), ponto central do estelionato, seria "a conduta do agente com o intento de obter vantagem ilícita, em prejuízo de outrem, considerando-se vantagem ilícita, para o autor, aquela economicamente apreciável, surgindo aqui o primeiro impasse quanto à tipificação do phishing como estelionato, o que é justamente a proposta do Projeto de Lei 5485/2013, conforme se demonstra:

"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."

Justifica o autor do projeto:

A prática do estelionato informático se consubstancia no envio, com intenções fraudulentas, de e-mails que pretendem ser de empresas conceituadas, a fim de induzir as pessoas a revelar informações pessoais, como senhas e/ou números de cartão de crédito.

Essa conduta é usada para o roubo de identidade on-line, utilizando engenharia social e subterfúgios técnicos para obter, de forma indevida e fraudulenta, os dados pessoais, de identidade e as credenciais financeiras dos consumidores.

É sabido que o crime de estelionato consuma-se com a obtenção da vantagem ilícita em prejuízo da vítima. As questões que se fazem presentes, desse modo, são: o mero envio das mensagens digitais, a fim de induzir outrem a revelar informações pessoais, de identidade ou senhas de acessos, por si só, poderia ser classificada como crime contra o patrimônio? Ainda, caso o agente consiga obter essas informações, a posse dos dados de identidade dos usuários da internet pode ser considerada vantagem ilícita? Em caso positivo, qual seria então o tratamento dado ao furto das contas bancárias por meio do ***internet banking***?

De certo, caso se considere o ***phishing*** como estelionato, impossível seria a tipificação do furto propriamente dito como qualificado por fraude, sob pena de bis in idem, uma vez que se puniria duas vezes a conduta fraudulenta.

Ademais, como será demonstrado a seguir, entendemos que, muito embora a intenção dos ***phishers*** seja a de obter vantagem econômica indevida, o ***phishing*** não pode ser considerado um crime contra o patrimônio, já que a mera obtenção dos dados de identidade não resulta necessariamente um prejuízo patrimonial para as vítimas.

6 DA NECESSIDADE DE UMA LEGISLAÇÃO PENAL INFORMÁTICA

Obviamente, a Lei 12.737/2012 - Lei Carolina Dieckmann, embora constitua um avanço em termos de legislação, não resolveu todo o problema da criminalidade informática, já que não contempla todas as modalidades criminosas que podem ser cometida através da Internet ou por meio de dispositivos informáticos.

A título de ilustração, chama-se atenção para o tratamento dado aos "cibercrimes" em países como Estados Unidos, Itália, Alemanha, Áustria, França, Inglaterra, Portugal e alguns outros que, já na década de 1990 sancionaram leis e reformaram seus Códigos Penais, tipificando condutas como sabotagem informática, acesso não-autorizado a dispositivos informáticos, etc.

A fim de demonstrar a necessidade de um tratamento penal adequado à criminalidade informática e tentar estabelecer o enquadramento jurídico do phishing, utilizaremos como parâmetro a legislação portuguesa e estadunidense, especificamente a Lei nº 109/2009 – Lei do Cibercrime e os "Anti-Phishing Acts" dos Estados de Nova Iorque e da Califórnia.

Como se sustentou durante todo este trabalho, nem o tratamento dado ao ***phishing*** pelo STJ ou pelo Projeto de Lei 5485/2013 é adequado, visto que não consideram tal conduta de forma apropriada. Isso porque se as decisões do Superior Tribunal de Justiça somente apreciam o fato após a consumação do furto, o mencionado projeto de lei equivoca-se ao tipificá-lo como crime contra o patrimônio.

Para que o ***phisher*** alcance êxito na empreitada criminosa, ele passa por um longo caminho vai desde o envio em massa de emails contendo informações falsas até a manutenção de sites fraudulentos para que só então consiga, se obtiver sucesso no engano às vítimas, a vantagem patrimonial que cogitou inicialmente.

Nessa linha de raciocínio, o ***phishing*** poderia configurar-se como ato preparatório do crime de furto, já que todas essas etapas identificadas fazem parte de um processo sistematicamente desenvolvido pelo agente para que este alcance o resultado almejado. Os atos preparatórios, nas lições de MIRABETE e FABBRINI (2014) são aqueles externos ao agente, que passa da cogitação à ação objetiva e que não se submetem, em regra, à aplicação da lei penal.

Desse modo, se considerada apenas como modus operandi, a pesca de informações sigilosas feita pela Internet continuaria não sendo objeto de repressão penal.

Fica claro que ao enviar emails falsos em massa e manter sites fraudulentos o agente está ofendendo seriamente a segurança jurídica que os usuários esperam encontrar no ambiente virtual. O cerne da questão, portanto, é: as relações jurídicas travadas neste ambiente merecem a tutela penal? Defende-se enfaticamente que sim.

A seleção dos bens jurídicos a serem tutelados pelo Direito Penal, segundo GALVÃO, depende do juízo de valor dos legisladores, já que um ato só passa a ser criminoso em decorrência de norma jurídica que o qualifique como tal. A esse respeito:

> *Um juízo de valor representa o trabalho de uma apreciação subjetiva, ou seja, da participação da consciência de quem valora, no ato de vinculação do sujeito ao predicado. A gênese da norma jurídica, necessariamente, traz embutido o resultado de uma tomada de posição diante do fato social. Assim, a consideração do que seja socialmente inadequado dependerá sempre do ponto de vista daquele que detém o poder de imposição (eleição da conduta proibida).*
>
> *Pode-se observar que a criminalidade e o delito não fazem parte de uma realidade natural, mas sim da construção jurídico-social que depende dos juízos valorativos que produzem a qualidade de criminosa na conduta à qual se aplicam. [...]*
>
> *Dessa forma, a definição de crime revela-se dependente dos interesses, das crenças e da cultura dos indivíduos que usufruem posição de predomínio na determinação do que seja inadequado, ou seja, das autoridades. (GALVÃO, 2011, p. 207)*

Rogério Greco, no mesmo sentido, afirma que somente os bens jurídicos mais valiosos devem ser objeto de proteção do Direito Penal, sendo assim considerados aqueles necessários para a sobrevivência em sociedade. A seleção desses bens é feita através de um critério político, tendo em vista que a evolução da sociedade pressupõe também a mutação dos seus valores morais, que ora se extinguem, ora se criam:

> *Em virtude dessa constante mutação, bens que outrora eram considerados de extrema importância e, por conseguinte, carecedores da especial atenção do Direito Penal já não merecem, hoje, ser por ele protegidos. (GRECO, 2011, p. 3)*

Ora, não se tem por razoável que a ausência de tipificação para o ***phishing***, bem como para as diversas modalidades de crimes informáticos não previstos no ordenamento jurídico pátrio tenha como fundamento a insignificância desses bens para o Direito Penal. Prova disso é a promulgação das Leis 12.7372012 e 12.965/2014 que protegem a inviolabilidade das informações automatizadas, corroborando, assim, o entendimento de que a pesca de dados de identidade feita pela Internet e a manutenção de sites fraudulentos, ainda que o furto de dinheiro não venha a se consumar, merece ser também objeto de reprimenda na esfera criminal.

Veja-se o que a Lei 109/2009 de Portugal (Lei do Cibercrime) dispõe sobre em seu artigo 3º:

Artigo 3.º
Falsidade informática
1 — Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.
2 — Quando as acções descritas no número anterior incidirem sobre os dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, a pena é de 1 a 5 anos de prisão.
3 — Quem, actuando com intenção de causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos que foram objecto dos actos referidos no n.º 1
ou cartão ou outro dispositivo no qual se encontrem registados ou incorporados os dados objecto dos actos referidos no número anterior, é punido com as penas previstas num e noutro número, respectivamente.
4 — Quem importar, distribuir, vender ou detiver para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado, sobre o qual tenha sido praticada qualquer das acções prevista no n.º 2, é punido com pena de prisão de 1 a 5 anos.
5 — Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de 2 a 5 anos. (Art. 3º da Lei 109 de 2009 de Portugal – Lei do Cibercrime)

Para MONTEIRO e TEIXEIRA (2013), a própria criação e manutenção de um site fraudulento que preveja a possibilidade de um usuário acessá-lo pensando se tratar de site legítimo poderia ser tipificado como falsidade informática. O ***phishing***, neste caso, seria considerado um ***modus operandi*** para a realização deste delito.

Os Estados de Nova Iorque e da Califórnia, por sua vez, foram mais incisivos ao tratar do assunto, criminalizando diretamente a pesca de informações pessoais:

It is unlawful for any person, by means of a web page, electronic message, or other use of the internet to solicit, request or collect identifying information by deceptively representing himself or herself, either directly or by implication, to be a business or a governmental entity and doing so without the authority or approval of such business or such governmental entity. (Anti-Phishing Act of 2006, §390-b, "3", Estado de Nova Iorque)
It shall be unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business. (Anti-Phishing Act of 2005, 22948.2, Estado da Califórnia)

O que se depreende da leitura das legislações apresentadas é de que já há uma preocupação internacional com a efetiva regulamentação do ambiente virtual, traduzida na proteção penal dos bens jurídicos nascidos desse avanço tecnológico. No Brasil, ao revés, muito embora a Lei 12.965/2014 tenha estabelecido em seu artigo 3º que a segurança da rede, a proteção da privacidade e a proteção dos dados pessoais sejam princípios que disciplinam o uso da Internet no país, não é possível afirmar que tal segurança seja uma realidade.

7 CONSIDERAÇÕES FINAIS

Por respeito ao princípio da legalidade, não é possível falar-se em enquadramento penal do furto de informações sigilosas e de dados de identidade até que haja uma lei definindo tal conduta como crime (art 5º, XXXIX da Constituição Federal de 1988). Como exposto, o projeto de lei 5485/2014, que equipara o ***phishing*** ao estelionato apresenta grave erro do ponto de vista jurídico, já que tipifica tal conduta como crime contra o patrimônio, o que, repita-se, não seria coerente.

Por fim, enquanto não há tipificação para a pesca de dados pessoais e sigilosos, defende-se como correto o tratamento dado ao "furto informático" pelo Superior Tribunal de Justiça, que o capitula como furto qualificado por fraude – artigo 155, §4º, II do Código Penal brasileiro. Como se sustentou, ainda que nestes casos seja desconsiderado o ***iter criminis*** percorrido pelo agente, com os conseqüentes danos causados a outros bens jurídicos que não o patrimônio, o criminoso age mediante fraude ao subtrair o dinheiro da instituição financeira burlando seu sistema de vigilância, ao utilizar o login e a senha de outro usuário, assistindo razão ao Tribunal.

Assim, não obstante o envio de mensagens fraudulentas, a criação e manutenção de sites falsos ou a pesca de informações sigilosas vise quase sempre à obtenção de vantagem patrimonial ilícita, tal conduta constitui-se, claramente, como uma ofensa à inviolabilidade das informações automatizadas e da segurança jurídica no ambiente virtual, de modo que a solução que se pode apresentar, após a exposição deste breve estudo, não pode ser outra senão a criação de uma legislação penal mais efetiva e avançada que contemple as modalidades de crimes informáticos que não se amoldem à legislação penal em vigor, muito embora se tenha a consciência de que a criminalização de determinado comportamento, sem que haja política pública a respeito ou esforço integrado dos vários setores sociais, não seja suficiente para a erradicação da ocorrência de qualquer espécie de delito.

REFERÊNCIAS

AZEREDO, Eduardo. ***Projeto de Lei 5485 de 2013***. Disponível em http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=575520. Acesso em 15 de março de 2014.

BRASIL. Constituição Federal de 1988. Disponível em <http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em 27 de Nov de 2014.

BRASIL. Decreto Lei nº 2.848, de 7 de Dezembro de 1940. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em 15 de Outubro de 2014.

CORGOSINHO, Ivanir Alves. A Prática da Comunicação Face-aFace. Belo Horizonte: 2005.

FABBRINI, Renato N. e MIRABETE, Júlio Fabbrini. Manuel de Direito Penal, volume 1: parte geral, arts. 1º a 120 do CP. São Paulo: 2014.

GALVÃO, Fernando. Direito penal: parte geral. Rio de Janeiro: 2011.

GRECO, Rogério. Curso de Direito Penal: parte especial, volume III. Niterói: 2014.

MACHADO, Felipe e VIANNA, Túlio Lima. Crimes Informáticos: Conforme a Lei 12.737/2012. Belo Horizonte: Editora Fórum, 2013.

Legislação do Estado da Califórnia. Disponível em <http://www.legin-

fo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22948-22948.3>. Acesso em 24 nov. 2014.

Legislação do Estado de Nova Iorque. Disponível em: http://public.leginfo.state.ny.us/LAWSSEAF.cgi?QUERYTYPE=LAWS+&QUERYDATA=$$GBS390-B$$@TXGBS0390- &LIST=LAW+&BROWSER=01912488+&TOKEN=33260917+&TARGET=VIEW>. Acesso em 24 nov. 2014.

LEI DO CIBERCRIME. Disponível em: <http://www.cnpd.pt/bin/legis/nacional/LEI109_2009_CIBERCRIME.pdf>. Acesso em 15 de março de 2014.

MICROSOFT. O que é phishing. Disponível em: <http://www.microsoft.com/pt-br/security/resources/phishing-whatis.aspx>. Acesso em 19 set. 2014

MONTEIRO, Fernando Conde e TEIXEIRA, Alexandre Gonçalves. O Fenômeno do Phishing: Enquadramento Jurídico-Penal. 2013. 155 folhas. Dissertação (Mestrado em Direito, especialidade em Ciências Jurídico-Criminais). Universidade Autónoma de Lisboa, Lisboa. 2013.

OLHAR DIGITAL. Brasil é o 2º país mais afetado por sites phishing HTTPS, diz pesquisa. Disponível em <http://olhardigital.uol.com.br/noticia/44036/44036>. Acesso em 26 out. 2014.

PLANTULLO, Vicente Lentini, Estelionato Eletrônico – Segurança na Internet. Curitiba: Juruá, 2003.

ROSA, Fabrízio. Crimes de Informática. Campinas: 2005.

VIANNA, Túlio Lima. *Fundamentos de Direito Penal Informático.* Disponível em http://pt.scribd.com/doc/34441066/Fundamentos-de-Direito-Penal-Informatico. Acesso em 07 maio de 2014.

NOTAS DE FIM

1 Aluna do nono período do curso de Direito pelo Centro Universitário Newton Paiva.

2 Doutor em Direito pela Universidade Federal de Minas Gerais, advogado criminalista e professor do Centro Universitário Newton Paiva.

3 Disponível em: http://blog.trendmicro.com/trendlabs-security-intelligence/phishing-safety-is-https-enough/

**Marcelo Sarsur; Renato Martins Machado.