DELITOS INFORMÁTICOS? COMENTÁRIOS AO CONFLITO DE COMPETÊNCIA Nº 67.343-GO, DO SUPERIOR TRIBUNAL DE JUSTIÇA

COMPUTER CRIMES? COMMENTS ON THE COMPETENCE CONFLICT Nº 67.343-GO, FROM THE SUPERIOR COURT OF JUSTICE

ALEX FERNANDES SANTIAGO
Promotor de Justiça
Ministério Público do Estado de Minas Gerais, Brasil
alex@mpmg.mp.br

RESUMO: O surgimento de uma nova criminalidade pelo uso de ferramenta específica, a informática, não demanda, necessariamente, a expansão do Direito Penal, de forma a exigir a criação de novas e extensas categorias delitivas. O instituto bem jurídico, adequadamente examinado, dará respostas, na maioria das vezes suficientes, ao mau uso que se pode fazer da informática, afetando valores básicos de uma sociedade. Sem embargo, alguns ajustes específicos serão necessários, como a criação de alguns tipos penais, ou modificação de outros já existentes.

PALAVRAS-CHAVE: delitos informáticos; nova criminalidade.

ABSTRACT: The development of a new type of criminality by means of using computer technology does not necessarily demand the expansion of Brazilian Criminal Law. The proper analysis of the already existent sanctions will suffice at most times. However, some modifications or the creation of new crime types may be necessary.

KEY WORDS: computer crimes; new criminality.

SUMÁRIO: 1. Introdução. 2. Delitos informáticos? 3. A adaptação das leis brasileiras. 4. Análise do acórdão. 5. Conclusão. 6. Referências.

1. Introdução

O desenvolvimento de novas tecnologias, como o da informática, além de promover profundas transformações experimentadas nos mais diversos âmbitos, veio acompanhado do surgimento de uma nova criminalidade, que originou questionamentos ao Direito Penal. Ainda que não se possa cogitar propriamente de delitos informáticos como categoria específica, é através dessa nova tecnologia que se lesionam bens jurídicos já protegidos pela mais grave das sanções, com a subsunção da conduta a tipos penais tradicionais, conforme se verifica da análise do acórdão Conflito de Competência nº 67.343-GO, de 28 de março de 2007, do Superior Tribunal de Justiça – STJ.

2. Delitos informáticos?

Não causa surpresa que o impacto da revolução no fluxo de informações venha acompanhado de uma nova criminalidade. Os mesmos computadores e internet que conectam, por seu turno, outros milhões de computadores e pessoas que os usam permitem a comissão de delitos contra milhares de pessoas distantes fisicamente.[1] Essa nova forma de delinquência utiliza o sistema informático para lesionar os mais diversos bens jurídicos, que há muito tempo gozam da proteção penal, como se nota nos atentados contra a intimidade, a propriedade, a fé pública, entre outros exemplos. Em razão disso, segundo grande parte da doutrina, é impróprio cogitar de delito

[1] Comparando essa nova delinquência com sua forma tradicional, no que concerne à prática de delitos, seja quanto à proximidade física entre autor e vítima, seja quanto à grande escala, Benjamin R. Jones (2007, p. 611-618) conclui pela necessidade de novas técnicas de investigação e estratégias preventivas, como a utilização de *softwares* abertos a todos, como o *Linux* (p. 618-630).

informático (SÁEZ CAPEL, 2001, p. 22)[2], já que os sistemas informáticos vão ser tão somente o meio para o cometimento de tais condutas. Tanto é assim que o *Department of Justice* norte-americano define os delitos informáticos também no sentido do uso do sistema informático: *any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution*[3].

Sendo o Direito Penal o ramo do Direito que se ocupa da proteção dos valores elementares da vida em comunidade[4], essa nova forma de criminalidade atiçou uma vez mais as ganas do legislador[5] nos mais diversos países para estirar o manto da *ultima ratio regum* para sua proteção, na já conhecida hipertrofia do Direito Penal. A pergunta que se faz é a seguinte: será realmente necessário?

Bem frisa a doutrina (SILVA, 2007, p. 369) que, enquanto a preocupação dirige-se à ferramenta – o computador, a informática – utilizada para a afetação do bem jurídico, o núcleo do problema queda olvidado, que é qual e como foi atingido o bem jurídico.

---

[2] Acerca da distinção entre delitos informáticos (*computer crimes*) e delitos cibernéticos (*cybercrimes*), segundo a qual estes últimos necessitam de uma rede (em geral a *Internet*), confira-se Moitra (2005, p. 438-439). No mesmo artigo (p. 436-464), o autor investiga a nova delinquência e algumas possíveis formas de controle social.

[3] Conforme Huang; Radkowski III; Roman (2007, p. 285-286), que analisam o sistema legal norte-americano que combate essa delinquência (p. 284-335). Para ver uma comparação entre alguns sistemas existentes no mundo, veja-se o artigo do professor sul-africano Cassim (2009, p. 36-79).

[4] Aceitando a clássica definição de Welzel (1956, p. 1). Com especial ênfase no conceito social, afirma Pablos de Molina: "pode-se definir o Direito penal, do ponto de vista dinâmico e social, como um dos instrumentos do controle social e formal por meio do qual o Estado, mediante um determinado sistema normativo (leia-se: mediante normas penais), castiga com sanções de particular gravidade (penas e outras consequências afins) as condutas desviadas (crimes e contravenções) mais nocivas para a convivência, visando a assegurar, dessa maneira, a necessária disciplina social bem como a convivência harmônica dos membros do grupo.". (Bianchini; García-Pablos de Molina; Gomes, 2009, p. 24).

[5] Preocupação que permeia toda a obra de Silva Sánchez (1999). É o próprio professor espanhol quem realça o descompasso entre a legislação e o que preconiza a doutrina, já em outro livro, ao afirmar que um dos aspectos que mais chama a atenção é a completa desconexão entre a evolução das leis e o desenvolvimento dos conceitos, sendo detectável um pragmatismo radical na atividade legislativa, perfeita tradução de uma práxis política sem ciência, é dizer, carente de uma racionalidade legitimadora. (SILVA SÁNCHEZ, 2010, p. XVII).

A resposta à pergunta acima apresentada é, sem embargo, simples. Definitivamente não é necessário criar nova categoria delitiva, pois o Direito Penal já protege muitos dos bens jurídicos lesionados pela nova forma delinquencial. É possível, se tanto, atualizar alguns tipos penais para abranger as condutas reprováveis que causem dano[6]. Reafirma-se, uma vez mais, a importância fundamental do bem jurídico no cenário penalista. Recorde-se, com Schunemann (2007, p. 198), que o esclarecimento de qual seja o bem jurídico encarna a questão interpretativa mais nos comentários da parte especial, "que deve se resolver com caráter geral antes de qualquer outra"[7]. (tradução nossa).

Nesse diapasão, antes de desfraldar apressadamente a bandeira de novos tipos penais que abarquem os reprováveis "delitos informáticos" (o que culminaria por incidir na "*lei da bipolaridade dos erros*"[8], consubstanciada, no caso, em tentar combater determinada delinquência gerando a hipertrofia do Direito Penal – e, quiçá, gerando nova criminalidade), vale a pena verificar se tais condutas já não são objeto de repressão penal, se já não são bens jurídicos protegidos e se a ação investigada não está emoldurada por algum tipo penal existente.

Ademais, nem sempre o Direito Penal é a resposta mais adequada, em especial no tema de delitos informáticos, pois, como já observado no exterior, a tecnologia e a lei nem sempre são os melhores parceiros de dança[9] tanto que, mais que o emprego de novas leis, reforçam alguns autores a necessidade de novas formas de prevenção, como a cooperação de particulares – especialmente empresas – com novas técnicas de investigação e utilização de ferramentas ci-

[6] Nesse sentido, ver (SÁEZ CAPEL, 2001, p. 26-27).

[7] "[...] que debe resolverse con carácter general antes que cualquier otra". (SCHUNEMANN, 2007, p. 198).

[8] Teorizada por Gaston Bachelard, consistente em não abandonar uma posição equivocada, para ocupar em seguida a posição oposta, igualmente reducionista e que divide com a primeira certo número de características essenciais, como recordam François Ost e M. van der Kerchove (1988, p. 177 ss.).

[9] Do original em inglês: "[...] one of the few constants of the Internet age is the recognition that technology and the law are not always the best dance partners".(JONES, 2006-2007, p. 601).

vis, reconhecendo que o Direito Penal não tem a bala de prata para combater os crimes informáticos (ALLAN, 2005, p. 177)[10].

3. A adaptação das leis brasileiras

Na seara da atualização da legislação penal existente, e da inserção de alguns novos tipos, podem detalhar-se algumas figuras delitivas relacionadas com a utilização do sistema informático no Direito positivo brasileiro.

É normal que sejam feitas alterações. Sendo o Direito produto histórico, realidade cultural,

> deve acompanhar o desenvolvimento social; não pode ser estático, enquanto a sociedade se revela dinâmica. A ordem jurídica que não evolui de acordo com os fatores sociais deixa de ser um instrumento de apoio e progresso, para prejudicar o avanço e o bem estar social. (NADER, 1997, p. 148).

Sem abandonar uma postura garantista, o próprio Sáez Capel reconhece que, embora não sejam necessárias grandes reformas no ordenamento jurídico substantivo para enfrentar a criminalidade informática, pode ser necessário, por seu dinamismo, criar novos tipos penais, em especial se considerada a comissão de condutas impensáveis há algumas décadas (SÁEZ CAPEL, 2001, p. 21).

Não obstante, é mister reconhecer a evolução do Direito Penal para um Direito Penal mínimo, isto é, representando a sanção penal a mais grave das consequências jurídicas que o descumprimento de um dever origina em relação a seu destinatário[11], somente pode ser manejado em casos que mereçam a mais grave das respostas: a intervenção do Direito Penal é mínima, com as máximas garantias[12].

---

[10] Sobre a preocupação da comunidade jurídica internacional, com resumo das manifestações da OECD, do Conselho Europeu, da ONU e da Association Internationale de Droit Penal, confira-se Soma; Muther Jr.; Brissete (1997, p. 358-360).

[11] Conceito de Maynez (1978, p. 295).

[12] Nessa esteira, culmina Rusconi por defender que "o direito penal deve ser visto como

Há que se compreender a lei penal como intervenção nos direitos fundamentais, pois a Constituição protege a liberdade geral de ação, que consiste na liberdade de fazer ou omitir o que se queira, com normas de direito fundamental. Se de um lado é certo que essa liberdade não é absoluta, e portanto pode ser objeto de intervenções e restrições legislativas, também é certo que a tipificação penal de uma conduta implica uma intervenção na liberdade geral de ação e que, como tal, deve estar justificada". (BERNAL PULIDO, 2005, p. 124)[13].

Vale a pena, então, transcrever as modificações legislativas.

O Código de Defesa do Consumidor (Lei nº 8.078/1990), preocupado com os bancos de dados privados, incriminou algumas condutas a eles relativas:

> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
>
> Pena - Detenção de seis meses a um ano ou multa.
>
> Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:
>
> Pena - Detenção de um a seis meses ou multa. (BRASIL, 1990a).

Na ordem tributária, externou o legislador sua preocupação com condutas reprováveis pelo uso da informática (artigo 2º, V, da Lei nº 8.137, de 1990):

---

o conjunto de limites constitucionais e derivados do sistema internacional de proteção dos direitos humanos, organizados e desenvolvidos sistematicamente em todas suas consequências como obstáculos para a aplicação de uma pena em forma legítima" [el derecho penal debe ser visto como el conjunto de límites constitucionales y derivados del sistema internacional de protección de los derechos humanos que organizados y desarrollados sistemáticamente en todas sus consecuencias como obstáculos para la aplicación de una pena en forma legítima]. (RUSCONI, 2009, p. 44).

[13] "la tipificación penal de una conducta implica una intervención en la libertad general de acción y que, como tal, debe estar justificada". (BERNAL PULIDO, 2005, p. 124).

> V – utilizar ou divulgar programa de processamento de dados que permita ao sujeito passivo da obrigação tributária possuir informação contábil diversa daquela que é, por lei, fornecida à Fazenda Pública. Pena – detenção, de 6 (seis) meses a 2 (dois) anos, e multa. (BRASIL, 1990b).

Também o Código Penal foi modificado, adaptando-se à criminalidade informática. A Lei nº 9.983, de 2000, modificou a redação de alguns tipos penais, adicionando novas letras ou parágrafos a alguns dispositivos antigos.

A Lei nº 9.983 começa por modificar o Código Penal com o fim de abrigar novos delitos contra a administração pública que podem ser cometidos com o emprego da nova tecnologia. Passou o Código Penal, portanto, a ter a seguinte redação:

> Inserção de dados falsos em sistema de informações.
>
> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
>
> Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.
>
> Modificação ou alteração não autorizada de sistema de informações.
>
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
>
> Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa.
>
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado. (BRASIL, 2000).

Também nos delitos contra a administração pública surge a figura daquele que, consoante o art. 325, § 1º:

> I- permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistema de informações ou banco de dados da Administração Pública.
>
> II – se utiliza, indevidamente, do acesso restrito. (BRASIL, 2000).

Cabe citar também, no capítulo de proteção à liberdade individual, o artigo 153, §1º-A:

> Art. 153. [...]
>
> § 1º-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:
>
> Pena - detenção, de 1 (um) a 4 (quatro) anos, e multa. (BRASIL, 2000).

Nota-se que são crimes que utilizam a informática como ferramenta para sua prática, contudo afetando bens jurídicos protegidos pelo Direito Penal, invocando, isso sim, ajustes na sua tipologia. Não é possível, nesses casos, dizer que há uma hipertrofia do Direito Penal. O que ocorre são simplesmente ajustes na sua sistemática.

Há casos, entretanto, em que vetustas figuras do Código Penal são suficientes para reprovar a conduta, quando o autor desta utilizou a inovadora ferramenta que é a informática. É o Direito, de tradição milenar, que se renova, propiciando desde seu antigo arcabouço respostas a problemas recentes, sem que se recorra à inflação normativa. Tampouco se usa qualquer recurso à analogia, em especial se se considera que Francis Bacon já advertia que "não está permitido estender as leis penais aos delitos não contemplados expressamente e é cruel atormentar o texto das leis para que estas atormentem aos cidadãos." (BACON apud FERRAJOLI, 2006, p. 382)[14].

[14] "[...] no está permitido extender las leyes penales a delitos no contemplados

Disso trata o acórdão cuja análise apresenta-se a seguir.

4. Análise do acórdão

Trata-se do acórdão Conflito de Competência n° 67.343-GO, de 28 de março de 2007, do STJ, em que é discutido conflito negativo de competência (algum dia veremos um conflito positivo?). Dois juízes federais não reconheciam sua competência: o primeiro, por entender que as transferências não autorizadas da conta-corrente da vítima, A. T., constituem estelionato contra a instituição bancária, razão pela qual o momento consumativo se opera quando se obtém a vantagem ilícita; noutro vértice, o juiz suscitado negava sua competência, por entender que ocorreu furto, na modalidade fraude, pois houve extração de dinheiro de uma conta bancária, desde seu serviço de *Internet*, sem nenhum tipo de consentimento por parte da vítima. Por conseguinte, a competência era do lugar onde foi subtraída a quantia.

Em seu voto, a relatora – Ministra Laurita Vaz – registra a existência de projetos para crimes informáticos (PL nº 89/2003, Deputados; e PL nºs 137/2000 e 76/2000), para em seguida reconhecer que a solução se encontra no próprio Código Penal pátrio.

Imperioso, nesse momento, reproduzir os dispositivos do Código Penal atinentes ao debate:

> Estelionato:
>
> 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 1 (um) a 5 (cinco) anos, e multa. [...]
>
> § 3º. A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

expresamente y es cruel atormentar el texto de las leyes para que éstas atormenten a los ciudadanos." (BACON *apud* FERRAJOLI, 2006, p. 382). Original do filósofo Francis Bacon, em *De dignitate scientiarum*, livro VIII, aforismo nº 13: "Durum est torquere leges, ad hoc ut torqueant homines. No placet egitur extende leges poenales, multo minus capitales, ad delicta nova."

> Furto:
>
> Art. 155. Subtrair, para si ou para outrem, coisa alheia móvel: Pena- reclusão, de 1 (um) a 4 (quatro) anos, e multa. [...]
>
> Furto qualificado [...]
>
> § 4º. A pena é de reclusão de 2 (dois) a 8 (oito) anos, e multa, se o crime é cometido:
>
> [...]
>
> II – com abuso de confiança, ou mediante fraude, escalada ou destreza. (BRASIL, 1940).

A distinção entre estelionato e furto mediante fraude, para a doutrina pátria, reside no fato de que neste último a vítima não sabe que dispõe da coisa, enquanto no estelionato entrega *sponte propia* a coisa ao sujeito ativo, enganada que foi por este[15].

Compreendeu o STJ que houve fraude ao sistema de vigilância e proteção do banco para furtar valores da conta-corrente de sua cliente, conforme dicção da relatora:

> Na hipótese em tela, o agente se valeu de fraude eletrônica para a retirada de R$ 2.525,15 (dois mil quinhentos e vinte e cinco reais e quinze centavos) da referida conta bancária, por meio da 'Internet Banking' da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima,

[15] "Embora a fraude seja característica inerente ao crime de estelionato,aquela que qualifica o furto não se confunde com a deste. No furto, a fraude burla a vigilância da vítima, que, assim, não percebe que a res lhe está sendo subtraída; no estelionato, ao contrário, a fraude induz a vítima a erro. Esta, voluntariamente, entrega seu patrimônio ao agente. No furto, a fraude visa desviar a oposição atenta do dono da coisa, ao passo que no estelionato o objetivo é obter seu consentimento, viciado pelo erro, logicamente. O dissenso da vítima no crime de furto, mesmo fraudulento, e sua aquiescência, embora viciada, no estelionato são dois aspectos que os tornam inconfundíveis. Examinando, com acerto, essa distinção, Fernando de Almeida Pedroso destaca 'a unilateralidade do furto majorado pela fraude, pela dissensão da vítima no apoderamento, e a bilateralidade do estelionato, pela aquiescência – embora viciada e tisnada – do lesado". (BITTENCOURT, 2006, p. 32).

> o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda.
>
> Note-se que, em nenhum momento, houve a participação de funcionários do Banco no episódio. Assim, não houve sequer a possibilidade de induzimento de 'alguém em erro', como exige o tipo penal do estelionato, que não prescinde do vínculo psicológico, e muito menos a efetiva entrega do bem com vício de consentimento. Houve, sim, a indevida transferência da titularidade – subtração – do numerário da conta bancária – coisa alheia móvel –, com a sub-reptícia quebra da vigilância eletrônica do sistema informatizado de dados – fraude –, delito que somente foi detectado pelo Banco-vítima depois de o titular da conta queixar-se. (BRASIL, 2007).

Assim foi ementada a decisão:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE.
>
> 1. O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente.
>
> 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da 'Internet Banking' da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato.

> 3. O dinheiro, bem de expressão máxima da idéia de valor econômico , hodiernamente, como se sabe, circula em boa parte no chamado 'mundo virtual' da informática. Esses valores recebidos e transferidos por meio da manipulação de dados digitais não são tangíveis, mas nem por isso deixaram de ser dinheiro. O bem, ainda que de forma virtual, circula como qualquer outra coisa, com valor econômico evidente. De fato, a informação digital e o bem material correspondente estão intrínseca e inseparavelmente ligados, se confundem. Esses registros contidos em banco de dados não possuem existência autônoma, desvinculada do bem que representam, por isso são passíveis de movimentação, com a troca de titularidade. Assim, em consonância com a melhor doutrina, é possível o crime de furto por meio do sistema informático.
>
> 4. A consumação do crime de furto ocorre no momento em que o bem é subtraído da vítima, saindo de sua esfera de disponibilidade. No caso em apreço, o desapossamento que gerou o prejuízo, embora tenha se efetivado em sistema digital de dados, ocorreu em conta-corrente da Agência Campo Mourão/PR, que se localiza na cidade de mesmo nome. Aplicação do art. 70 do Código de Processo Penal. (BRASIL, 2007).

De fato, estelionato não poderia ser, pois não se induz a vítima a realizar um ato de disposição patrimonial. A questão é enfrentada pormenorizadamente por Sáez Capel (2001, p. 55-70), em análise *de lege lata* e *de lege ferenda*, quanto ao Direito argentino, comparando-o a dispositivos espanhóis e alemães. Culmina por frisar que ademais não pode ser estelionato porque não se pode lograr uma mente equivocada, sendo uma máquina. E concorda com Gladys Romero que a tipificação adequada é a de furto.

A lei penal brasileira, sem embargo, como demonstra o acórdão do STJ, prevê um crime de furto qualificado, pela obtenção fraudulenta do dinheiro, o que se assemelha ao Código Penal alemão em seu parágrafo 265a.

É verdade que se pode questionar a solução encontrada no acórdão, quanto à fraude, já que, com Queralt Jimenez, lembrado por Sáez Capel (2001, p. 60), há de se reconhecer que as máquinas não podem ser suscetíveis de engano. Sem embargo, a Corte brasilei-

ra se aventura a dar uma resposta positiva à existência de fraude, salientando que a enganada não foi a máquina, e sim o sistema de vigilância do banco, que, em realidade, é constituído de pessoas, que exercem tal função.

O que fez o Tribunal brasileiro, de qualquer forma, foi parecido com o sucedido no apartado 2 do art. 248 do novo Código penal espanhol, pois a verdade é que não há um engano, não há um estelionato propriamente dito, e por assimilação reconhece-se uma fraude, quando o que realmente existe é uma manipulação informática ou artifício semelhante, o que se caracteriza como furto qualificado, para o STJ.

Com a amplitude da palavra fraude, conclui-se que é acertada a posição do STJ.

5. Conclusão

O surgimento de uma nova criminalidade pelo uso de ferramenta específica, a informática, não demanda, necessariamente, a expansão do Direito Penal, de forma a exigir a criação de novas e extensas categorias delitivas. O instituto bem jurídico, adequadamente examinado, dará respostas, na maioria das vezes suficientes, ao mau uso que se pode fazer da informática, afetando valores básicos de uma sociedade. Sem embargo, alguns ajustes específicos serão necessários, como a criação de alguns tipos penais, ou modificação de outros já existentes.

Exemplo de suficiente resposta penal encontra no acórdão Conflito de Competência n° 67.343-GO, de 28 de março de 2007, do Superior Tribunal de Justiça, documento em que a extração não autorizada de valores de uma conta-corrente foi tipificada como furto qualificado, pela existência de manipulação reconhecida como fraude.

6. Referências

ALLAN, Gregor. Responding to cybercrime: a delicate blend of the orthodox and the alternative. *New Zealand Law Review*, Auckland, v. 149, p. 149-178, 2005.

BERNAL PULIDO, Carlos. *El derecho de los derechos:escritos sobre la aplicación de los derechos fundamentales.* Bogotá: Universidad Externado de Colombia, 2005.

BIANCHINI, Alice; GARCÍA-PABLOS DE MOLINA, Antonio; GOMES, Luiz Flávio. *Direito penal*: introdução e princípios fundamentais. 2. ed. São Paulo: Revista dos Tribunais, 2009.

BITTENCOURT, Cezar Roberto. *Tratado de direito penal*: parte especial. 3. ed. São Paulo: Saraiva, 2006. v. 3. (Tomo III).

BRASIL. Decreto-Lei n. 2.848, de 7 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 15 maio 2014.

BRASIL. Lei n. 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 15 maio 2014. (1990a)

BRASIL. Lei n. 8.137, de 27 de dezembro de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8137.htm>. Acesso em: 15 maio 2014. (1990b)

BRASIL. Lei n. 9.983, de 14 de julho de 2000. Altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9983.htm>. Acesso em: 15 maio 2014.

BRASIL. Superior Tribunal de Justiça. Conflito de Competência n. 67.343-GO, 3ª Seção, Rel.: Min. Laurita Vaz, Brasília, DF, 28 de março de 2007. *DJ*, 11 dez. 2007, p. 170.

CASSIM, F. Formulating specialised legislation to address the growing spectre of cybercrime: a comparative study. *Potchefstroom Electronic Law Journal*, Vanderbijlpark, v. 12, n. 4, p. 36-79, 2009.

FERRAJOLI, Luigi. *Derecho y razón*: teoría del garantismo penal. 8. ed. Madri: Trotta, 2006.

HUANG, Xiaomin; RADKOWSKI III, Peter; ROMAN, Peter. Computer crimes. *American Criminal Law Review*, v. 44, 285, 2007, p. 284-335.

JONES, Benjamin R. Comment: virtual neighborhood watch: open source software and community policing against cybercrime. *The Journal of Criminal Law and Criminology*, Chicago, v. 97, n. 2, p. 601-630, 2007.

MAYNEZ, Eduardo Garcia. *Introduccíon al estudio del derecho.* 29. ed. Cidade do México, DF: Porrúa, 1978.

MOITRA, Soumyo D. Developing policies for cybercrime:some empirical issues. *European Journal of Crime, Criminal Law and Criminal Justice*, Leiden: Martinus Nijhoff Publishers, v. 13, n. 3, p. 436-464, 2005.

NADER, Paulo. *Introdução ao estudo do direito.* 14. ed. Rio de Janeiro: Forense, 1997.

OST, François; KERCHOVE, Michel van de. De la 'bipolarité dês erreurs'. In: *Archives de philosophie du droit*: banco de dados. Paris: Sirey, t. 33, 1998.

RUSCONI, Maximiliano. *Derecho Penal*: parte general. 2. ed. Buenos Aires: Ad-Hoc, 2009.

SÁEZ CAPEL, José. *Informática y delito.* 2. ed. Buenos Aires: Proa XXI, 2001.

SCHUNEMANN, Bernd. El principio de protección de bienes jurídicos como punto de fuga de los límites constitucionales de los tipos penales y de su interpretación. In: HEFENDEHL, Roland. *La teoría del bien jurídico*: fundamento de legitimación del Derecho Penal o juego de abalorios dogmático? Barcelona: Marcial Pons, 2007.

SILVA SÁNCHEZ, Jesús-Maria. *La expansión del Derecho penal*:*aspectos de la política criminal en las sociedades postindustriales.* Madrid: Cuadernos Civitas, 1999.

_____. *Aproximación al derecho penal contemporáneo*. 2. ed. ampliada e atualizada. Buenos Aires: B de F, 2010.

SILVA, Rita de Cassia Lopes da. A informação como bem jurídico -penal e o sistema informático. In: *Direito penal contemporâneo*: estudos em homenagem ao Professor José Cerezo Mir. São Paulo: Revista dos Tribunais, 2007.

SOMA, John T. et al. Transnational extradition for computer crimes: are new treaties and laws needed? *Harvard Journal on Legislation*, v. 34, p. 317-372, 1997.

WELZEL. *Derecho penal*: parte general. Buenos Aires: Roque Depalma, 1956.

Artigo recebido em: 11/10/2010.
Artigo aprovado em: 13/02/2012.

DOI: 10.5935/1809.848720140007