CRIMES ELETRÔNICOS E LEI 14.155/2021

Rudá Figueiredo.

Mestre em Direito pela Universidade Federal da Bahia. Professor na Faculdade Baiana de Direito. Promotor de Justiça do Ministério Público do Estado da Bahia.

Sumário: 1. Introdução. 2. Invasão de dispositivo informático. 2.1. Alteração no tipo simples e na cláusula de equiparação. 2.2. Modificação na causa de aumento de pena. 2.3. Invasão de dispositivo informático qualificada: aumento da pena cominada 3. Furto qualificado pela fraude eletrônica e suas majorantes. 4. Estelionato eletrônico e suas majorantes. 5. Regra de competência para o estelionato eletrônico. Como ficam as demais hipóteses? 6. Conclusão.

1. Introdução

João procurou na *internet* por um *tablet*, visando a estudar para concursos, quando encontrou uma oferta que o agradou. Nessa senda, negociou com o dono do aparelho o valor a ser pago e avençou encontrar o indivíduo em um shopping, para recebê-lo. Efetivamente, João encontrou Pedro, dono do *tablet*, e recebeu o aparelho, que, quando da entrega, parecia estar ligado, com a tela funcionando. O vendedor, alegando estar apressado, pediu a João que transferisse a quantia de R$ 500,00 (quinhentos reais) pelo aparelho, via PIX, o que efetivamente ocorreu. Na sequência, Pedro entregou o bem e saiu do local rapidamente. João, por sua vez, dirigiu-se para casa, onde testaria melhor sua aquisição. Nada obstante, ao chegar em casa, João percebeu que o aparelho estava travado na tela inicial e, efetivamente, não funcionava.

João intentou contato com o vendedor, mas este não mais respondia nas redes sociais. Em verdade, Pedro parecia ter apagado suas páginas e desaparecido do mapa. Já achando que sofrera um golpe, João foi à assistência autorizada, descobrindo que, de fato, o aparelho que comprara estava irremediavelmente danificado. A tela inicial estava apenas congelada e seu processador não mais funcionava.

No mesmo período, em outra cidade e estado, Josefa recebeu uma mensagem de um perfil de Whatsapp de alguém que, usando a foto de sua filha, alegou precisar de

um dinheiro com urgência, para pagar uma dívida. Acreditando estar em contato com sua descendente, Josefa transferiu um valor para a conta apontada pelo perfil. Sem embargo, descobriu, após, que foi enganada, pois foi contatada por um perfil fake.

O que estes casos têm em comum?

Efetivamente, tais situações tornaram-se corriqueiras e representam fenômenos criminosos de uma sociedade altamente conectada à internet, altamente ligada a aparelhos e sistemas eletrônicos.

Com efeito, com os avanços tecnológicos, surgiram novos comportamentos lesivos a bens jurídicos e, outrossim, foram criadas novas formas para prática de crimes antigos.

Pensando em tais situações, foi positivada e publicada no último dia 28 de maio de 2021 a Lei n. 14.155 de 2021, por via da qual foram promovidas diversas modificações no Código Penal e, também, no Código de Processo Penal.

Nas linhas abaixo, tecemos algumas considerações acerca das modificações promovidas, seus contornos e repercussões.

2. Invasão de dispositivo informático

Uma das alterações promovidas pela Lei 14.155 de 2021 ocorreu no crime de invasão de dispositivo informático, previsto no art. 154-A do Código Penal.

2.1. Alteração no tipo simples e na cláusula de equiparação

O art. 154-A, *caput* do Código Penal foi criado, originariamente, pela Lei 12.737 de 2012, a qual ficou conhecida como Lei Carolina Dieckmann.

Com efeito, naquele ano, a famosa atriz teve dispositivo pessoal invadido e, na sequência, foram divulgadas fotos íntimas suas, as quais constavam no aparelho. O caso teve bastante repercussão e, em razão disso, o legislador pátrio agiu para criar um tipo penal que criminalizasse tal tipo de comportamento.

Desta feita, o legislador modificou o tipo incriminador e, também, previu maior sancionamento para o comportamento, consoante se pode observar através do quadro abaixo, no qual destaco as alterações promovidas:

Lei 12.737/2021	**Lei 14.155/2021**

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:	Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.	Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Deveras, verifica-se que o novel art. 154-A, *caput* do Código Penal não mais exige, como uma de suas elementares, que a invasão de dispositivo informático tenha ocorrido através de "violação indevida de mecanismo de segurança". Com efeito, para a prática a delitiva, agora, pouco importa a violação de mecanismo de segurança, o que implica em alteração prejudicial ao acusado e que, portanto, não pode retroagir.

Além disso, a figura típica passa a contar com pena significativamente maior, deixando de ser um crime de menor potencial ofensivo, para passar a figurar entre os crimes de médio potencial ofensivo.

Deveras, o crime, antes apenado com 03 (três) meses a 01 (um) ano de reclusão (admitindo, então, as benesses da Lei 9.099/1990), passa a ser punido com reclusão de 01 (um) a 04 (quatro) anos. Assim, considerando as normas contidas na Lei 9.099/1995, é possível a incidência tão somente da suspensão condicional do processo, em favor de delinquente que cometa aludido crime.

Noutro giro, analisando o delito à luz do Código de Processo Penal, vislumbra-se a viabilidade de ofertar acordo de não persecução penal em hipóteses deste jaez, ante a pena cominada.

Não se olvide que o art. 154-A, *caput* tem uma cláusula de equiparação, prevista em seu § 1º, que positiva o seguinte:

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012)

Deveras, o dispositivo colacionado representa a intenção do legislador de criminalizar os **atos preparatórios** concernentes ao crime de invasão de dispositivo. É dizer, há uma antecipação da punição, para reduzir as chances de execução efetiva do comportamento subsequente, a qual se afigura deveras lesiva. Trata-se de decisão político-criminal semelhante àquela adotada na criminalização dos petrechos para falsificação de moeda.

O art. 154-A, §1º consubstancia tipo misto-alternativo, praticado por quem realiza quaisquer das condutas nele previstas, ou seja, pratica o delito quem "produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no *caput*". Note-se que não basta que a conduta delitiva possibilite a invasão, mas que o agente tenha praticado o comportamento com o intuito de permitir que isso aconteça.

Nessa senda, o tipo demanda dolo específico, não bastando para sua prática a intenção de realizar a conduta nele prevista. Deveras, exige-se que o agente saiba que está, por exemplo, fornecendo um programa que será utilizado por um terceiro, para a invasão de um dispositivo. Portanto, a norma em análise representa uma exceção à teoria monista, pois o auxílio material é criminalizado de forma autônoma, o que permite a punição do agente, ainda que não ocorra a subsequente e visada invasão de dispositivo informático.

Fato é que, embora não pareça em uma leitura apressada, o art. 154-A, § 1º também foi alterado pela Lei 14.155/2021, pois, como se lê no dispositivo, àqueles comportamentos nele previstos se aplicam as mesmas penas incidentes no caso do art. 154-A, *caput*. Efetivamente, o art. 154-A, § 1º prevê o que a doutrina chama de norma penal em branco ao revés, é dizer, uma norma penal cujo preceito secundário (sanção) demanda complemento por outra norma. Trata-se de norma penal em branco homogêneo e homovitelínea, pois seu complemento é estabelecido pelo art. 154-A, *caput* do Estatuto Repressor. Sucede que as penas do art. 154-A, *caput* foram alteradas e, com isso, dessarte, foram modificadas também as sanções do § 1º. As mudanças, naturalmente, porquanto prejudiciais ao acusado, **não podem retroagir** (vide artigos 1º e 2º do Código Penal).

2.2. Modificação na causa de aumento de pena: art. 154-A, § 2º

Outra importante alteração promovida pela Lei 14.155/2021 ocorreu no art. 154-A, § 2º do Estatuto Repressor, conforme quadro abaixo:

Lei 12.737/2021	**Lei 14.155/2021**
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.	§ 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.

Deveras, o crime de invasão de dispositivo informático tem a pena aumentada, se, do comportamento delitivo, decorre prejuízo econômico para a vítima. Cumpre salientar, nesse ponto, que a causa de aumento incide em situações nas quais a conduta do agente não se enquadra nos tipos positivados para a proteção ao patrimônio, em respeito aos critérios de solução ao conflito aparente de normas e ao *ne bis in idem*.

Com efeito, se o delinquente invade o aparelho da vítima e, de posse de fotos íntimas suas, ameaça divulgar as imagens, acaso esta não lhe transfira certa quantia, o jurista estará diante de uma hipótese de extorsão e não de simples invasão de sistema informático. Nesse caso, a realização da transação bancária será exaurimento da extorsão e não hipótese de incidência da aludida majorante. A majorante, assim, é um reforço à punição do *caput*, que não desconstitui o fato deste ser residual/subsidiário em relação a outros tipos.

2.3. Invasão de dispositivo informático qualificada: aumento da pena cominada

Ainda com relação ao tratamento dado à invasão de dispositivo informático, na Lei 14.155/2021 o legislador elevou a pena cominada para sua figura qualificada, contida no art. 154-A, § 3º, conquanto tenha mantido os termos do preceito primário da norma:

Lei 12.737/2021	**Lei 14.155/2021**
§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou	§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou

industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:	industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.	Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.

De fato, por via de tal alteração, o legislador pátrio recrudesceu o tratamento dado ao comportamento previsto no art. 154-A, § 3º do Estatuto Repressor, razão pela qual a inovação normativa não retroage.

Efetivamente, o anterior regulamento dado às condutas descritas no dispositivo atraía a adoção de todas as benesses da Lei 9.099/1995, pois, por sua pena máxima cominada, qual seja, 02 (dois) anos, o art. 154-A, § 3º do Código Penal se inseria dentre as hipóteses de crimes de menor potencial ofensivo. Contudo, atualmente, nem mesmo a suspensão condicional do processo pode ser aplicada à aludida infração, pois sua pena mínima é superior a um ano.

Por outro lado, a pena cominada para o delito atende o requisito objetivo para oferta de acordo de não persecução penal, inovação inserta pelo pacote anticrime no Código de Processo Penal.

3. Furto qualificado pela fraude eletrônica e suas majorantes

Além das regras acima delineadas, a Lei 14.155/2021 criou mais uma modalidade qualificada de furto, a qual se entende por denominar de furto qualificado pela fraude eletrônica. Isso ocorreu pela inserção do art. 155, § 4º-B no Código Penal, com a seguinte redação:

> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, **se o furto mediante fraude** é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (grifos insertos)

Esta norma é uma interessante hipótese de qualificadora da qualificadora, algo que podemos chamar de superqualificadora, com aumento apenas da pena mínima correlacionada ao furto mediante fraude.

Com efeito, o art. 155, § 4º, inciso II do Código Penal qualifica o furto com emprego de fraude, prevendo uma pena, para este comportamento, de 02 (dois) a 08 (oito) anos de reclusão. Por outro lado, o art. 155, § 4º-B prevê uma pena de 04 (quatro) a 08 (oito) anos de reclusão para os furtos realizados mediante fraude eletrônica, ou seja, cometida por "meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo".

Furtar, como se sabe, é subtrair, para si ou para outrem, coisa alheia móvel (art. 155, caput do Código Penal). Praticará, assim, a modalidade qualificada em análise, quem subtrair coisa alheia móvel para si ou para outrem, mediante fraude eletrônica, conforme descrita no art. 155, § 4º-B.

Sabe-se que o furto mediante fraude, na forma do art. 155, § 4º, inciso II, é caracterizado pelo emprego de enganação. Nele, a vítima é submetida a um processo de ilusão, que permite ao delinquente acessar o bem por ele objetivado. Marca, assim, em especial, o furto mediante fraude eletrônica, o fato de a fraude ser realizada por "meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores" ou "por qualquer outro meio fraudulento análogo".

Nesse sentido, o art. 155, § 4º, inciso II se refere ao meio de execução do delito, enquanto o art. 155, § 4º-B, além de tangenciar o meio para execução, realça a uma especial importância **o instrumento empregado**. Assim, se alguém acessa uma conta bancária, por via de senha obtida através da invasão do computador da vítima, e dela retira quantias, pratica furto mediante fraude eletrônica.

Note-se que, ao final da qualificadora, o legislador previu fórmula que atrai interpretação analógica, pois a norma incide em quaisquer hipóteses de emprego de "meio fraudulento análogo". Trata-se, efetivamente, de um elemento normativo do tipo, cujo conteúdo resultará da intepretação judicial. Com isso, o legislador busca atender antecipar-se às mudanças tecnológicas, que acontecem com celeridade significativa, trazendo consigo diversas possibilidades de uso prejudicial às pessoas, muito embora impliquem, também, benefícios.

Como acima dito, é necessário anotar que o furto qualificado pelo emprego de fraude eletrônica não se confunde com a invasão de dispositivo informático com resultado de prejuízo econômico. Esta última figura é residual, aplicando-se às situações que não se enquadrem no furto ou no estelionato eletrônico, abaixo explicado.

Deveras, se o agente invade dispositivo informático para, com isso, descobrir a senha da vítima e, assim, subtrair valores de sua conta, praticará o furto qualificado descrito no art. 155, § 4º-B. Noutro giro, se o agente invade a conta, descobre a senha e a divulga na internet, fazendo com que terceiros por ele desconhecidos realizem a subtração (sem sua adesão subjetiva), praticará a invasão majorada. O terceiro, ao viso deste autor, praticará furto mediante fraude, pois utilizará senha a ele não pertencente o que, *per se*, implica emprego de fraude, pois usar a senha é prerrogativa única e exclusiva do proprietário da conta, ou seja, para a instituição financeira, este, o ofendido, está acionando o sistema e não um terceiro desconhecido.

Além de positivar o furto qualificado pela fraude eletrônica, a Lei 14.155/2021 criou causas de aumento específicas para esta modalidade de crime, a teor do art. 155, § 4º-C e seus incisos, *in verbis*:

> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
>
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
>
> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

Nota-se que o legislador, estranhamente, indicou que a causa de aumento de pena estaria condicionada à "relevância do resultado gravoso", prevendo, na sequência, no inciso I, majoração decorrente da prática do crime por via da utilização de servidor mantido fora do território nacional e, no inciso II, incremento de sanção concernente a características das vítimas.

Com todas as vênias, a expressão "relevância do resultado gravoso", representa violação ao princípio da taxatividade, pois prevê desnecessário elemento normativo do tipo. Com efeito, se o resultado gravoso não for relevante, estar-se-á diante de furto mínimo ou de furto insignificante, os quais se submetem a regras específicas. Por outro lado, o aumento de pena no caso de uso de servidor mantido fora do território nacional é cogente, pois, nessas situações, a persecução é dificultada, razão pela qual o

comportamento delitivo impacta, ainda, na Administração da Justiça. Noutro giro, a proteção de pessoas vulneráveis de forma mais pujante é também imperativa e ocorre em diversos trechos do Estatuto Repressor, sem que seja avaliada a "relevância do resultado gravoso".

Destarte, com todas as licenças, premente a interpretação da majorante à luz da Constituição, para considerar de resultado gravoso todos os furtos que não sejam mínimos (art. 155, § 2º do Código Penal) ou insignificantes. Com isso, evita-se violar não apenas a taxatividade, como também o princípio da proporcionalidade (na vertente da vedação à proteção insuficiente) e, outrossim, sobretudo, isonomia e segurança jurídica. É que já há parâmetros judiciais para definição do pequeno valor, no âmbito dos furtos, e, também, do que é insignificante, razão pela qual a adoção dos mesmos critérios para definir o resultado gravoso descrito nas majorantes em análise atenderá a igualdade e a segurança jurídica.

4. Estelionato eletrônico e suas majorantes

Além de criar a modalidade de furto mediante fraude eletrônica, a Lei 14.155 de 2021 positivou o estelionato mediante fraude eletrônica, no art. 171, § 2º-A. Cumpre salientar, neste ponto, que o estelionato tem por inerente a fraude, mesmo em sua figura simples, diferente do que acontece no furto (no qual a fraude é qualificadora e a fraude eletrônica, por via de consequência, é uma qualificadora da qualificadora, uma verdadeira superqualificadora). Veja-se o tipo simples, contido no art. 171, *caput* do 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, de quinhentos mil réis a dez contos de réis.

Deveras, no estelionato, o delinquente engana a vítima, através do emprego de artifício, ardil, ou qualquer outro meio fraudulento, fazendo com que ela lhe entregue, de bom grado, uma vantagem ilícita. Tem-se, aí, neste exato ponto, a diferença entre furto mediante fraude e estelionato, consoante se pode delinear no quadro esquemático abaixo colacionado:

Furto mediante fraude	Estelionato
Agente pratica a fraude para ele, diretamente, ou comparsa subtrair a coisa	Agente pratica a fraude para a vítima lhe entregar a coisa de bom grado

Por via do novel art. 171, § 2º-A, a pena do estelionato é sobrelevada, quando a fraude empregada pelo agente "é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo". Veja-se a norma multicitada:

> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.

Assim, pratica estelionato eletrônico quem realiza os comportamentos descritos no início do nosso texto, ou seja, por meio de rede social, vende um aparelho que não funciona, ou quem pede dinheiro à vítima, fingindo tratar-se da filha desta. Note como, nessas situações, a pessoa ofendida entrega o bem da vida (dinheiro) ao delinquente. No furto, diferentemente, o agente subtrai a coisa de forma sub-reptícia, sem intervenção da vítima.

Por representar nova norma prejudicial ao acusado (qualificadora), o art. 171, § 2º-A do Código Penal não pode retroagir para alcançar os fatos anteriores a sua vigência.

Insta registrar que o legislador previu causas de aumento específicas para os casos de estelionato eletrônico, no § 2º-B do art. 171 (as quais, naturalmente, não retroagem):

> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

A lei 14.155 mudou, ainda, o art. 171, § 4º do Código Penal, incrementando o aumento de pena nos casos de estelionato contra idoso ou vulnerável, fazendo-o nos seguintes termos:

> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso. (Redação dada pela Lei nº 14.155, de 2021)

Verifica-se que, em ambas as normas majorantes, o legislador previu que a incidência do incremento deve levar em consideração "a relevância do resultado gravoso". Trata-se de elemento normativo do tipo que, portanto, terá seu conteúdo definido por via de interpretação judicial. Novamente (à semelhança do quanto efetivado quanto ao furto), o autor pontua, com vênias, que deve ser considerado gravoso todo resultado que não se insira no estelionato de pequeno valor (art. 171, § 1º), sem olvidar que, como regra, não se admite a aplicação do princípio da insignificância nos casos de estelionato.

5. Regra de competência para o estelionato eletrônico. Como ficam as demais hipóteses?

Derradeiramente, a Lei 14.155/2021 promoveu importante modificação com relação à competência para apreciação do estelionato eletrônico, inserindo, no art. 70 do Código de Processo Penal, o § 4º, *in verbis*:

> § 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção. (Incluído pela Lei nº 14.155, de 2021)

Destarte, por força do art. 70, § 4º do Código de Processo Penal, nos casos de estelionato eletrônico, **a competência será definida pelo local do domicílio da vítima**, e, em casos de **pluralidade de vítimas, pela prevenção**.

Com esta norma, o legislador visa a robustecer a tutela das vítimas dos estelionatos eletrônicos, sobretudo diante da grande cizânia formada derredor da competência territorial para apreciação destes delitos. Com efeito, sabe-se que, a teor do

art. 70 do Código de Processo penal, a regra geral para fixação da competência territorial é do lugar da infração, mais especificamente, o lugar da consumação da infração.

Sucede que, nos crimes patrimoniais eletrônicos, surgem inúmeras dúvidas com relação ao local da consumação do crime. Por exemplo, se um indivíduo vende um carro que não lhe pertence pela *internet*, qual o local da consumação? O local de onde a vítima fez a transferência? O local da conta corrente beneficiária da transferência?

A jurisprudência vinha adotando alguns critérios para definição da competência nestes casos, consoante se extrai do julgado abaixo colacionado, o qual sintetiza a solução até então albergada:

> CONFLITO NEGATIVO DE COMPETÊNCIA. ESTELIONATO. DISSENSO ACERCA DO LOCAL DA CONSUMAÇÃO NA HIPÓTESE DE TRANSFERÊNCIA OU DEPÓSITO BANCÁRIO. DIVERGÊNCIA VERIFICADA ENTRE PRECEDENTES RECENTES DA TERCEIRA SEÇÃO. EQUACIONAMENTO DO TEMA. COMPETÊNCIA DO JUÍZO DO LOCAL DA AGÊNCIA BENEFICIÁRIA DO DEPÓSITO. 1. A jurisprudência da Terceira Seção desta Corte tem oscilado na solução dos conflitos que versam acerca de crime de estelionato no qual a vítima é induzida a efetuar depósito ou transferência bancária em prol de conta bancária do beneficiário da fraude. 2. Deve prevalecer a orientação que estabelece diferenciação entre a hipótese em que o estelionato se dá mediante cheque adulterado ou falsificado (consumação no banco sacado, onde a vítima mantém a conta bancária), do caso no qual o crime ocorre mediante depósito ou transferência bancária (consumação na agência beneficiária do depósito ou transferência bancária). 3. Se o crime de estelionato só se consuma com a efetiva obtenção da vantagem indevida pelo agente ativo, é certo que só há falar em consumação, nas hipóteses de transferência e depósito, quando o valor efetivamente ingressa na conta bancária do beneficiário do crime. 4. No caso, considerando que a vantagem indevida foi auferida mediante o depósito em contas bancárias situadas em São Paulo/SP, a competência deverá ser declarada em favor daquele Juízo (suscitado). 5. Conflito conhecido para declarar a competência do Juízo de Direito do Foro Central Criminal da Barra Funda (DIPO 4) da comarca de São Paulo/SP, o suscitado. (STJ – CC 169.053/DF 2019/0317771-7 Data do Julgamento:11/12/2019Data da Publicação:19/12/2019; Órgao Julgador: S3 - TERCEIRA SEÇÃO; Relator: Ministro SEBASTIÃO REIS JÚNIOR) (grifou-se)

Por via de tal julgado, constata-se que a definição da competência, nos casos de estelionato eletrônico, era assim efetivada:

Situação 01: Hipótese em que o estelionato se dá mediante **cheque adulterado ou falsificado** (**consumação no banco sacado**, onde a vítima mantém a conta bancária)	**Situação 02**: Crime ocorre mediante **depósito ou transferência bancária** (**consumação na agência beneficiária** do depósito ou transferência bancária)
Competência territorial: Comarca na qual inserida a agência onde a vítima mantém a conta bancária	**Competência territorial**: Comarca na qual inserida a agência beneficiária do depósito ou transferência bancária

Sucede que, com todas as vênias, as soluções anteriores não privilegiavam a vítima que, assim, por vezes, precisava adotar diversas medidas, inclusive de cunho cautelar, longe de seu domicílio. Destarte, ao viso do autor, a alteração legislativa em análise se afigura alvissareira. Nada obstante, não se entende por que o legislador restringiu a regra ao crime de estelionato eletrônico, deixando de estendê-la ao furto eletrônico. Com vênias, entende cogente a adoção do mesmo regramento no tocante ao último delito, por analogia.

Não se propõe, vale frisar, a adoção da mesma regra de competência em relação a todos os crimes cometidos por via eletrônica, em atenção à segurança jurídica, para que inúmeros processos não sejam simplesmente obliterados em discussões intermináveis sobre competência, como, aliás, desafortunadamente, ocorre em muitas situações. **Nos casos de outros delitos**, nos quais, aliás, a similitude entre tipos é muito menor (basta pensar em obtenção de imagens de crianças nuas, pela internet), **premente que o legislador preveja regra específica, para evitar a insegurança jurídica**.

Feitas tais considerações, não se pode olvidar que regras de cariz processual se aplicam de imediato, por força do art. 2º do Código de Processo Penal, segundo o qual: "A lei processual penal aplicar-se-á desde logo, sem prejuízo da validade dos atos realizados sob a vigência da lei anterior".

O que acontecerá, então, com as investigações e processos envolvendo estelionato eletrônico (e, ao viso do autor, furto eletrônico)?

Entende-se que deve ser aplicada, para solucionar a questão, a norma contida no art. 43 do Código de Processo Civil (o qual incide no processo penal de forma supletiva, por força do art. 3º do Cártula Ritualística Criminal):

> Art. 43. Determina-se a competência no momento do registro ou da distribuição da petição inicial, sendo irrelevantes as modificações do estado de fato ou de direito ocorridas posteriormente, salvo quando suprimirem órgão judiciário ou alterarem a competência absoluta.

Deveras, a norma em análise versa acerca de competência relativa (territorial) e, outrossim, não implica supressão de órgão judiciário, razão pela qual os processos em curso devem continuar a tramitar junto aos Juízos nos quais iniciados.

Note-se que a determinação da competência, por via do art. 43, não ocorre com a decisão de recebimento da denúncia, mas no momento do registro ou distribuição da petição inicial. Ou seja, não haverá modificação da competência em quaisquer casos nos quais já ofertada denúncia ou queixa-crime, mas tão somente em situações em que ainda não foi oferecida a inicial acusatória. Por outro lado, investigações em curso devem ser encaminhadas para o Juízo do domicílio da vítima, devendo ser eventual ação penal intentada em tal secção territorial.

6. Conclusão

A) A lei 14.155 de 2021 promoveu importantes alterações no tratamento de crimes cometidos no contexto da *internet*;

B) Por via da citada lei, o legislador modificou o art. 154-A do Código Penal, retirando do tipo penal a exigência de prática do crime mediante violação indevida de mecanismo de segurança, o que configura mudança prejudicial ao réu e, por isso, não pode retroagir;

C) O art. 154-A passou a ter pena incrementada, deixando de ser crime de menor potencial ofensivo e passando a ser de médio potencial ofensivo, o que é prejudicial ao réu e, por isso, não retroage;

D) O aumento de pena concernente à existência de prejuízo econômico, nos casos do art. 154-A foi incrementado;

E) Foi criada uma modalidade qualificada de furto, o furto qualificado pelo emprego de fraude eletrônica (art. 155, § 4º-B);

F) Foram criadas majorantes específicas para o furto qualificado pelo emprego de fraude eletrônica, as quais exigem, para incidência, a avaliação da gravidade do resultado (art. 155, § 4º-C, incisos I e II);

G) Premente, em respeito à taxatividade, à proporcionalidade, à isonomia e à segurança jurídica, que seja considerado gravoso, para aplicação da majorante, todo resultado que não se insira no conceito de prejuízo mínimo ou insignificante;

H) Foi criada uma modalidade qualificada de estelionato, o estelionato mediante fraude eletrônica (art. 171, §2º-A);

I) Foram criadas majorantes específicas para o estelionato eletrônico, as quais exigem, outrossim, para incidência, análise da gravidade do resultado (art. 171, §§ 2º-B e 4º);

J) Propõe-se que seja considerado grave todo resultado que não seja pequeno, para fins de aplicação da citada majorante;

K) Foi criada uma nova regra de competência (art. 70, § 4º do Código de Processo Penal) segundo a qual a competência territorial, no peculato eletrônico, é definida pelo domicílio da vítima;

L) Propõe-se que a mesma regra seja adotada no caso de furto eletrônico, por analogia, mas que isso não se estenda a outros crimes cometidos pela internet, em nome do princípio da segurança jurídica, para que os processos não sejam obliterados em intermináveis discussões acerca da competência (fincando-se a necessidade de o legislador regulamentar a matéria);

M) Com relação à aplicação da lei processual penal no tempo, premente a aplicação do art. 2º do Código de Processo Penal, em conjunto com art. 43 do Código de Processo Civil, a fim de que a modificação da competência territorial não afete casos nos quais já apresentada a inicial acusatória.