ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 11, Issue, 01, pp. 43466-43469, January, 2021
https://doi.org/10.37118/ijdr.20742.01.2021

RESEARCH ARTICLE OPEN ACCESS

O CIBERCRIME NO BRASIL: UMA ANÁLISE DA (IN) EFICÁCIA DA LEI CAROLINA DIECKMANN

***[1]Deivid Jonas Silva da Veiga, [2]Dieison Prestes da Silveira, [3]Joselia Cristina Siqueira da Silva, [4]Geovane Barbosa da Silva, [5]Etyane Goulart Soares, [6]Sirlei de Lourdes Lauxen, [7]Denise da Costa Dias Scheffer and [8]Rafael Vieira de Mello Lopes**

[1]Acadêmico de Direito da Universidade de Cruz Alta; [2]Doutorando pelo Programa de Pós-Graduação em Educação em Ciências e em Matemática, pela Universidade Federal do Paraná, Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES; [3]Doutoranda pelo Programa de Pós-Graduação em Educação em Ciências e em Matemática pela Universidade Federal do Paraná- UFPR; [4]Mestrando em Atenção Integral à saúde - UNICRUZ/UNIJUI; [5]Mestranda no Programa de Pós-Graduação em Práticas Socioculturais e Desenvolvimento Social- Unicruz. Bacharela em Direito- Unicruz; [6]Doutora em Educação pela UFRGS. Professora do PPG em Práticas Socioculturais e Desenvolvimento Social da Universidade de Cruz Alta; [7]Mestranda do Programa de Pós-Graduação em Práticas Socioculturais e Desenvolvimento Social – Unicruz; [8]Professor do Curso de Graduação em Direito da Universidade de Cruz Alta/RS. Advogado. Doutorando em Direito pela Universidade Regional Integrada Santo Ângelo (URI)

ARTICLE INFO

Article History:
Received 19th October, 2020
Received in revised form
22nd November, 2020
Accepted 22nd December, 2020
Published online 30th January, 2021

Key Words:
Crimes cibernéticos.
Segurança virtual.
Lacunas legislativas.

****Corresponding author:***
Deivid Jonas Silva da Veiga,

ABSTRACT

Esse artigo faz uma abordagem da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, a qual busca discutir as questões voltadas aos*cibercrimes*, bem como suas prováveis consequências no Brasil, revendo aspectos legais no combate aos referidos delitos. O objetivo deste estudo foi analisar situações de impunidade quanto aos cibercriminosos, bem como as lacunas na legislação penal. Por este viés, optou-se por uma investigação nos artigos da Lei nº 12.737/2012, buscando um diálogo epistêmico acerca dos *cibercrimes*. A metodologia se baseia em uma abordagem qualitativa, com foco em uma pesquisa bibliográfica, visando um debate sobre as questões legais. Pôde-se identificar lacunas na legislação penal brasileira frente a Convenção Internacional de *Cibercrime*, bem como a ausência de rigidez nas penas, demonstrando total esvaziamento na repressão aos *cibercrimes*.

Citation: ***Deivid Jonas Silva da Veiga, Dieison Prestes da Silveira, Joselia Cristina Siqueira da Silva et al.*** "O cibercrime no brasil: uma análise da (in) eficácia da lei carolina dieckmann"*, International Journal of Development Research*, 11, (01), 43466-43469.

INTRODUCTION

Sabe-se que as tecnologias fazem parte do dia a dia dos sujeitos. Os computadores, telefones, o acesso à internet, são alguns dos exemplos mais comuns quando se pensa em tecnologias. Entretanto, o surgimento do processo de globalização impulsionou a conectividade entre as pessoas, permitindo um choque sociocultural, bem como diversas interações, sejam eles sociais, econômicas e/ou políticas. Pode-se dizer que as tecnologias acompanharam o processo evolutivo do homem, visto que na antiguidade teve o surgimento de instrumentos feitos de madeira, pedra e tantos outros materiais, os quais já se configuravam tecnologias (HARARI, 2019).

No panorama atual, a velocidade da globalização e a expansão da tecnologia tem promovido a conectividade global, proporcionando constantes avanços, sejam eles econômicos, científicos, culturais, sociais e até mesmo no campo político.No entanto, em meio aos avanços da internet, ocorre a inserção e a expansão do crime em rede, sendo denominado *Cibercrime*. O conceito de *cibercrime,* segundo os parâmetros internacionais é entendido como "[...] todo o ato praticado contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta destes sistemas, rede e dados" (CONVENÇÃO SOBRE O CIBERCRIME, 2001). É plausível destacar que criminosos estão migrando seus atos, de crimes

comuns para o meio virtual, valendo-se assim, de ganhos maiores do que os proporcionados nos delitos tradicionais. A internet, em meio a tantos benefícios, tem suas falhas, podendo-se apontar problemas de segurança e facilidade do anonimato, impulsionando a impunidade de criminosos. No Brasil, os dados estatísticos demonstram-se preocupantes, visto que o país é o segundo com maior número de casos de *cibercrimes*, causando um prejuízo na economia de US$ 22 bilhões. Além do mais, a legislação que trata do assuntoé a Lei nº 12.737/2012, conhecida também como Lei Carolina Dieckmann que carece de revisões e aprimoramentos, a fim de igualar aos padrões internacionais. Diante deste contexto, a pesquisa possui o seguinte questionamento: A Lei nº 12.737/2012, que trata sobre os crimes cibernéticos, consegue cumprir sua função social de apurar e reprimir o *Cibercrime*? Pensando nisso, o presente artigo tem o objetivo de analisar situações de impunidade quanto aos*cibercriminosos*, bem como as lacunas na legislação penal. Por este viés, optou-se por uma investigação analítica nos artigos da Lei nº 12.737/2012, buscando um diálogo epistêmico acerca dos *cibercrimes.*

MATERIAIS E MÉTODOS

A metodologia aplicada apresenta abordagem metodológica do tipo qualitativa. As pesquisas qualitativas são de extrema importância no campo das ciências, haja vista que buscam compreender de forma munuciosa fatos/circunstâncias que estão presentes no meio social, promovendo um debate e uma análise crítica da realidade estudada (MINAYO, 2010). Ainda, em se tratando de metodologia para este estudo, ocorreram pesquisas em referenciais bibliográficos, por meio de pesquisa em livros, artigos e legislações relacionados ao tema. Toda a pesquisa necessita de um aporte teórico visando um fichamento de dados. As pesquisas bibliográficas são tão importantes quanto qualquer outro tipo de pesquisa, pois permitem uma atualização de informação, sendo relevante para qualquer área do conhecimento (SEVERINO, 2000).Destaca-se que o artigo apresenta o método de abordagem hipotético-dedutivo, visto que se estruturou por meio de uma hipótese que busca analisar a falta de uma legislação precisa e ampla para determinados delitos da internet, os quais favorecem a impunidade de *cibercrimes*.

RESULTADOS E DISCUSSÃO

No cenário atual, com tantas facilidades presentes no acesso à*internet*, como a possibilidade do contato virtual e imediato, a lógica do consumismo, bem como momentos de estudos, trabalho e/ou até mesmo a eficácia de transações bancárias, permitiram o despertar da atenção de criminosos, que se valem, muitas vezes, do anonimato, das falhas de segurança e inexperiências dos usuários, para cometer *cibercrimes* das mais diversas maneiras, a fim de satisfazer seus interesses, sejam eles patrimoniais, morais, ou até mesmo sexuais (BRASIL, 2012). No Brasil, é importante ressaltar que, na ausência de lei específica, tem se usado o direito penal por analogia, buscando enquadrar o máximo de delitos possíveis. Entretanto, muitas vezes essa analogia não tem tido êxito, haja vista que nosso código penal é datado da década de 40 - tendo transcorridoaproximadamente 80 anos, tornando incomum exigir da legislação penal, eficácia na abrangência dos delitos digitais (BRASIL, 2012). Insta salientar que, em contraponto a aplicação do direito penal por analogia, temos os casos que não há abrangência suficiente da carta penal, por contradizer o princípio da taxatividade. Sendo assim, nos deparamos com a impunidade, pois como punir frente ao princípio constitucional/penal, "*nulluncrimen, nulla poena sine praevia lege*", ou como consta no artigo 1º do Código PenalBrasileiro (OLIVEIRA JUNIOR, 2012, s/p)."Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal". Nesta perspectiva, é indiscutível que o princípio da legalidade seja um dos mais importantes atos do direito penal. Para Pacelli e Callegari (2016, s/p.) "[...]pela máxima do princípio da legalidade e de sua vertente do *nullum crime sine lege*, somente os fatos que encontrem uma precisa correspondência com os tipos trazidos na lei penal, adequação chamada de tipicidade, podem ser considerados crime".

Se os *cibercrimes* não forem devidamente taxados e tipificados em lei, não há o que se falar em crime digital, sendo as lacunas legislativas as maiores responsáveis pela impunidade de *cibercriminosos*.Por este viés, houve a criação da Lei n° 12.737/12, conhecida como Lei Carolina Dieckmann, consideradas um marco no direito digital brasileiro. Antes desta Lei nº 12.737/2012 entrar em vigor, é importante frisar que nenhuma das condutas nela enumeradas eram consideras crime, impondo assim, muitas dificuldades na tipificação de delitos cibernéticos (LOUREIRO, 2019). No que diz respeito a origem da Lei nº 12.737/12, compreende-se que o legislativo brasileiro vem seguindo o padrão de legislar após a ocorrência de algum fato marcante na sociedade, nomeando as leis conforme o nome das vítimas, sendo uma forma de homenagear e prestar o devido respeito a estas. Frente a isso pode-se destacar a Lei Maria da Penha e, mais tarde a Lei Carolina Dieckmann, que surgiu em razão da invasão do computador da atriz brasileira que teve seus arquivos pessoais subtraídos, tendo suas fotos íntimas vazadas e espalhadas pela internet, gerando uma grande repercussão (OLIVEIRA JUNIOR, 2012). Em consequência disso, a referida lei acrescentou os artigos 154-A e 154-B ao Código Penal, que tipifica penalmente a invasão de dispositivos informáticos alheios mediante a violação indevida de mecanismos de segurança, bem como define que os referidos delitos procedem apenas mediante representação, salvo os casos quando atentado contra a administração pública (BRASIL, 1940).

Em uma análise minuciosa do *caput* do artigo 154-A, é possível notar alguns conceitos mormente imprecisos, bem como algumas inconsistências que tornam a Lei nº 12.737/12 demasiadamente enxuta, ou seja, não cumpre seu propósito quanto lei penal, de alcançar e tipificar o maior número de crimes possíveis, não estando, portanto, em conformidade com os Parâmetros Internacionais, como a Convenção de Budapeste. Barreto; Kufa; Silva (2020, p. 131) comentam que:[...] a norma, é tortuosa, já que os tipos penais se valeram de conceitos imprecisos. [...] a sansão prevista, por sua vez, é extremamente branda, não cumprindo o desiderato de reprimir e prevenir tais espécies delitivas e apresentando grave desproporção com delitos tradicionais. De forma analítica, na primeira parte do artigo 154-A, encontra-se a expressão "invadir" que por sua aplicação, exclui uma outra modalidade de crime, que são os ataques a disponibilidade de serviços, conhecidos como DDoS, em que elevado números de acessos direcionados a uma página ou recurso de internet, tende a derrubar este serviço tornando o indisponível, logo não ocorre uma invasão propriamente dita, mas sim ataque à disponibilidade de serviço (BARRETO; KUFA; SILVA, 2020). Ainda, pode-se observar a expressão"dispositivo

informático alheio".Quanto a expressão "dispositivo informático", pode-se perceber que o legislador ignora os dispositivos biológicos, que já são objetos de estudos, tendo como por exemplo os dados armazenados em moléculas de DNA. Da mesma forma, quanto ao termo "alheio", nota-se que na aplicação prática, o agente não poderá ser punido se o dispositivo seja seu, podendo ocorrer com os donos de *Lan House*s, onde o empresário cobra um valor pelo uso dos seus computadores (BARRETO; KUFA; SILVA, 2020). No caso dos donos de *Lan Houses*, denota-se a ideia de omissão frente ao *cibercrime*, uma vez que agentes criminosos locam máquinas para fins ilícitos, valendo-se do anonimato. Logo os donos destes estabelecimentos comerciais deveriam certificar-se quanto aos limites no uso de suas máquinas, mediante instalação de mecanismos de segurança, visando impedir a utilização destas para fins ilícitos (BARRETO; KUFA; SILVA, 2020).

No que concerne a locução "rede de computadores", os autores BARRETO; KUFA; SILVA, (2020, p. 132) entende que:

> A expressão 'rede de computadores', por seu turno, sofre de grave imprecisão, deixando de lado redes formadas por outros *gadgets* (dispositivos) – especialmente diante da *Internet* das Coisas – que não se encaixam no exato conceito de computador. Isso sem falar na possibilidade de uso de redes biológicas, valendo-se de material orgânico para levar e trazer informações, comandos ou realizar tarefas.

Já quanto a expressão "mediante violação indevida de mecanismo de segurança", remete que o dispositivo violado tenha senhas ou programas de segurança, tais como antivírus ou outras ferramentas de segurança. Contudo, tal expressão ignora a existência de outros *cibercrimes* que são cometidos sem a exigência da violação de mecanismo de segurança. Assim, na visão de Barreto; Kufa e Silva (2020, p. 133) "[...] as formas de ataque, [...] são variadas, podendo explorar vulnerabilidade do sistema operacional, bugs de aplicativos, desatualização de periféricos ou mesmo engenharia social, quando a vítima inadvertidamente fornece ou facilita o acesso ao invasor", sendo comum nestes casos, a exploração de falhas encontradas em sistemas operacionais e *softwares* desatualizados, ou como na maioria dos casos, a utilização dos artifícios da engenharia social. Assim, o invasor consegue acesso ao sistema informático apenas ludibriando a vítima, que entrega o acesso a este de maneira espontânea, sem imaginar estar sendo enganada, não ocorrendo, portanto, o infringimento do requisito objetivo " violação indevida de mecanismo de segurança".

Na sequência do artigo 154-A da referida Lei, pode-se notar os elementos "com o fim de obter, adulterar ou destruir dados ou informações", contudo novamente, a expressão não consegue cumprir seu objetivo de alcançar todos os intentos possíveis, como por exemplo a conduta de expor dados ou informações. Claro que tal conduta não se confunde com elemento obtenção, no entanto, o criminoso não transfere as informações para si, mas disponibiliza elas tornando-as públicas e exploradas por terceiros. Outra conduta, é tornar os dados indisponíveis, algo semelhante a ideia de sequestro. Essa conduta ocorre por meio de *ransomware* -vírus que criptografa os dados "sequestrados" da vítima com fortes senhas, impossibilitando seu acesso usual. Nesta prática, os malfeitores exigem o pagamento de um valor especifico para o resgate dos dados criptografados (BARRETO; KUFA; SILVA, 2020).

A próxima expressão a ser analisada do artigo 154-A da Lei Carolina Dieckmann, é a locução "sem autorização expressa ou tácita do titular do dispositivo", tal expressão é extremamente limitante, haja vista que grande parte dos delitos ocorrem por meio do uso da engenharia social, na qual os malfeitores se valem da probidade e do pouco conhecimento tecnológico das vítimas, ou seja, a maioria das "invasões" ocorrem por permissões voluntárias de usuários ludibriados, concedendo acesso aos criminosos que, dentro da rede interna, conseguem alavancar permissões e causar grande prejuízo (BARRETO; KUFA; SILVA, 2020). Por fim, é plausível analisar a expressão "instalar vulnerabilidades para obter vantagem ilícita". Salienta-se que, nem sempre as vulnerabilidades são instaladas, mas muitas vezes, estas são exploradas pelos criminosos, vulnerabilidades já existentes em muitos programas e até mesmo sistemas operacionais. Logo, se a vulnerabilidade não for instalada, mas simplesmente exploradas, não há o cumprimento do requisito subjetivo, não havendo o crime.

Nesse sentido (MILAGRE, 2013, s/p.):

> A vulnerabilidade é ativada por uma ameaça, a vulnerabilidade é explorada e pode atentar contra a integridade, confidencialidade e disponibilidade da informação.Como é possível constatar, a vulnerabilidade é uma fraqueza em um sistema. Não se espera de um atacante, que acaba de invadir um sistema, que 'instale uma vulnerabilidade'. No máximo a vítima, pode instalar um sistema vulnerável, que poderá ser explorado pelo atacante. Falar em instalar vulnerabilidade, como objetivo da invasão, para um cracker, seria o mesmo que dizer ao atacante para criar uma nova porta em uma casa na qual ele já entrou, ou o mesmo que punir um ladrão de veículos que ao arrombar a porta do carro, o faz sem o objetivo de levar o bem, mas simplesmente de abrir todas as demais portas do veículo, indo embora.

É importante lembrar que grande parte dos casos, o próprio usuário cria a brecha de segurança, instalando programas e acessando *sites* de conteúdos duvidosos, sendo estas brechas exploradas por terceiros (BARRETO; KUFA; SILVA, 2020, p. 136).Quanto as penalidades impostas no referido artigo, observa-se uma grave desproporção frente aos delitos comuns, estando a lei demasiadamente branda pois, ao analisar as penas do artigo 154-A da Lei nº 12.737/12, nota-se que estas não conseguem cumprir seu papel social, de impor penas proporcionais ao lesividade dos danos causados. De modo geral, isso torna-se evidente quando observado que a pena máxima majorada para invasão de dispositivos informáticos é um ano e quatro meses, sendo uma penalidade extremamente ínfima perto dos prejuízos econômicos, sem contar a possibilidade de alcance de inúmeras vítimas. Tal desproporcionalidade torna-se mais evidente quando comparado ao delito de furto qualificado, que teria uma pena mínima de quatro anos, podendo chegar a oito anos, que a título de danos patrimoniais, muitas vezes não consegue se aproximar da lesividade econômica de um delito virtual.

Como já evidenciado anteriormente, tais mudanças adicionadas pela referida lei, não tem uma rigidez penal adequada, pois, segundo Oliveira Junior (2012, s/p.):

> Percebe-se de fato que as penas que foram cominadas a tais artigos são um tanto quanto que irrelevantes, podemos comparar a invasão a computadores ao crime de furto, pois da mesma maneira que o indivíduo invade sua casa para subtrair algo que ali está, da mesma forma ele está invadido seu computador, seu celular, seu tablete e outros equipamentos onde você guarde suas informações pessoais ou profissionais, para tirar proveito disso.

No mesmo sentido:

> Resta evidente o total esvaziamento do caráter preventivo e retributivo da sanção, que incentiva, ainda mais, o cometimento dos *cibercrimes*. Não bastassem as imensas dificuldades de se apontar a autoria delitiva dentro dos ciberespaço, a lei em comento garante a completa impunidade do cibercriminoso, pois, diante de tal pena, jamais poderia ser preso preventivamente, teria direito à transação penal, *sursis* processual, substituição por pena alternativa, garantia de regime aberto, enfim, todo aparato processual da não privação de liberdade (BARRETO; KUFA; SILVA, 2020, p. 136).

Logo, é nítido que as invasões de dispositivos são tratadas de maneira branda, haja vista que suas punições podem chegar até dois anos, sendo inclusive objetos de instrução nos Juizados Especiais Criminais.Além disso, levando-se em conta as dificuldades encontradas nas investigações dos delitos, bem como da apuração de autoria, os esforços nestes casos, tornam-se muitas vezes esvaziados, haja vista que há penalidades brandas frente ao potencial de lesividade dos delitos.

Considerações Finais

Percebe-se que o *cibercrime* é uma modalidade de crime que tem sido disseminado de maneira exponencial, apresentando impactos financeiros e econômicos. Durante a pesquisa foi demonstrado que o Brasil é o segundo país que mais recebe ataques dos referidos delitos. Além do mais, constata-se que as lacunas presentes na nossa legislação têm deixado os delitos em um verdadeiro vácuo legislativo, ao pecar no seu compromisso quanto lei penal, de alcançar e tipificar o maior número de crimes. Ademais, as penalidades da legislação brasileira são ínfimas, comparadas a lesividade dos danos, devendo o poder público compreender que o alcance e os danos provocados por um estelionatário virtual são mais abrangentes que a de um estelionatário comum. Por fim, o Brasil carece de modificações pontuais em sua legislação, a fim de suprir os anseios da sociedade, que vem sendo cada vez mais vitimada pela enxurrada de delitos que a acometem, sendo, portanto, de suma importância que novas leis sejam elaboradas com auxílio de especialistas no ramo, alinhando-se as diretrizes internacionais como a Convenção de Budapeste e priorizando um rol taxativo mais amplo, bem como dando maior ênfase na estruturação e capacitação policial, nas investigações e apurações dos delitos virtuais. Ainda, o legislador não deve deixar de zelar pelas garantias processuais decorrentes da persecução penal, assegurando a produção probatória, bem como a preservação de seus elementos. Enfim, o Brasil carece de eficácia no que tange a repressão ao *cibercrime*, haja vista a ineficácia da Lei 12.737/2012 no cumprimento de sua função penal. Além do mais, existe uma evolução constante dos meios tecnológicos de comunicação, que vem ofertando novos caminhos para a proliferação dos referidos delitos, desdobrando assim, a necessidade de atualizações constantes, seja no legislativo, bem como na polícia judiciária, que deverão agir de maneira cada vez mais coordenada, a fim de demonstrar êxito na aplicação legal, satisfazendo desta forma os anseios da sociedade por segurança virtual.

REFERÊNCIAS

BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. Cibercrimes: e seus reflexos no direito brasileiro. 1. ed. Salvador: Jus PODIVM, 2020.

BRASIL. Decreto Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Presidência da República, [1940]. Disponível em http://www.planalto.gov.br/ ccivil_03/ decreto-lei/del2848compilado.htm. Acesso em: 07 mar. 2020.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF: Presidência da República, [2012]. Disponível em http://www.planalto. gov.br/ccivil_03/_Ato 2011-2014/2012/Lei/L12735.htm. Acesso em: 28 mar. 2020.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Presidência da República, [2012]. Disponível em http://www.planalto. gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 07 mar. 2020.

CENTRAL JURÍDICA. Dicionário de Latim Forense. [S. l.], 2019. Disponível em: https://www.centraljuridica. com/dicionario/g/2/l/n/p/1/dicionario_de_latim_forense/dicionario_de_latim_forense.html. Acesso em: 27 out. 2019.

CONVENÇÃO SOBRE O CIBERCRIME, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 02 maio de 2020.

HARARI, Yuval Noah.Sapiens: uma breve história da humanidade. Tradução JanaínaMarcoantonio.Porto Alegre: L&PM, 2019.

LOUREIRO, Antonio José Cacheado; COHEN, Amanda Caroline Lima; ALVES, Gabriel Cunha. Análise da Lei Carolina Dieckmann e sua (in)eficácia no ordenamento jurídico brasileiro. Portal Jurídico Investidura, Florianópolis/SC, 01 Fev. 2019. Disponível em: investidura.com.br/biblioteca-juridica/artigos/direito-penal/337191-analise-da-lei-carolina-dieckmann-e-sua-ineficacia-no-ordenamento-juridico-brasileiro. Acesso em: 25 Abr. 2020.

MILAGRE, José Antônio. Lei Dieckmann (12.737/2012) e a invasão com objetivo de "instalar vulnerabilidades". [S. l.], 12 maio 2013. Disponível em: https://josemilagre.com.br /blog/2013/05/12/lei-dieckmann-12-7372012-e-a-invasao-com-objetivo-de-instalar-vulnerabilidades/. Acesso em: 30 abr. 2020.

MINAYO, Maria Cecília de Souza. O desafio do conhecimento. 12ª ed. São Paulo: Editora Hucitec, 2010.

OLIVEIRA JUNIOR, Eudes Quintino de. A nova lei Carolina Dieckmann. [S. l.], 6 dez. 2012. Disponível em: https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann. Acesso em: 26 out. 2019.

PACELLI, Eugênio; CALLEGARI, André. Manual de Direito Penal: parte geral. 2ª Ed. São Paulo: Atlas, 2016.

SEVERINO, Antônio Joaquim. Metodologia do trabalho científico. 21. ed. São Paulo:Cortez, 2000.

****