ETIC 2015 - Encontro de Iniciação Científica
ISSN 21-76-8498

# LEI CAROLINA DIECKMANN: ATUALIZAÇÃO JURÍDICO-NORMATIVA BRASILEIRA

Laís Baptista Toledo DURAN[1]
Laryssa Vicente Kretchetoff BARBOSA[2]

**RESUMO:** O presente trabalho busca analisar a importância de uma lei especifica de combate aos crimes da internet, para que acompanhe o desenvolvimento da sociedade. A lacuna legislativa faz com exista violação de direitos, e que, por consequência a criação de delitos. Os delitos que surgiram com a era digital não poderiam ser compreendidos como sinônimos de delitos cometidos no mundo concreto, isto porque, possui características próprias, tem um *modus operandi* especifico o que dificulta ainda mais a punição, já que um crime cometido no meio não virtual é mais fácil de se punir. A lei 12.737/2012 com o seu artigo 154-A solucionou esse buraco normativo, pois tipificou tal crime, de modo que trouxe uma solução ao problema antes enfrentado.

**Palavras-chave:** Internet. Direitos Fundamentais. Crimes virtuais.

## 1 INTRODUÇÃO

O presente trabalho abordou o desenvolvimento da internet na década de 60,70 e 80, analisando toda a progressão que ocorreu para chegar até a presente formação.

Toda essa evolução da chamada rede criou uma “nova sociedade”, onde as relações pessoais se aproximaram devido ao encurtamento de fronteiras que esse novo sistema trouxe.

Devido a essa grande evolução, sentiu-se a necessidade de aprimoramento normativo, isso porque, além dos benefícios de obter tudo de um modo mais rápido e fácil, a internet trouxe consigo o ônus, a criação de vírus que invadem dados pessoais, trazendo lesão ao direito dos usuários.

[1] Discente do 3º ano do curso de Direito do Centro Universitário “Antonio Eufrásio de Toledo” de Presidente Prudente. e-mail@ laisbtoledoduran@hotmail.com
[2] Discente do 3º ano do curso de Direito do Centro Universitário “Antonio Eufrásio de Toledo” de Presidente Prudente. e-mail@ laryssavkb@yahoo.com.br

Por serem direitos tutelados pela constituição federal, inclusive chamado de direitos fundamentais, muito se criticava sobre a inexistência de uma legislação que acompanhasse o progresso da sociedade.

Depois de muitas críticas sobre o atraso da legislação, surgiu a lei 12.737/2012 apelidada de “lei Carolina Dieckmann”, que veio para suprir a deficiência existente no ordenamento jurídico brasileiro, e que por consequência veio acompanhar o momento tecnológico vivido.

## 2. Origem Da Internet

A criação da internet modificou tão intensamente a relação entre as pessoas, que talvez o mundo não estivesse preparado para tal transformação. O telégrafo, o telefone, a máquina de escrever, e o rádio foram um meio de preparar a sociedade para aquilo que estava por vir, uma era de inter-relacionamentos virtuais.

A criação dessa rede chamada internet derivou da criação de uma máquina muito avançada para época, o computador. Este surgiu por uma necessidade da época, e hoje é sem dúvida a prioridade dos últimos anos, pois as pessoas dependem tanto dos seus computadores, *notebooks, smartphones, tablets*, que esses tipos de equipamentos não são mais “artigos de luxo” e sim “essenciais” para a vida em sociedade.

### 2.1 Do Computador

O primeiro computador digital foi criado em 1946 por cientistas norte-americanos. Recebeu o nome de ENIAC (*Electrical Numerical Integrator and Computer*). Este nada mais era do que uma grande máquina de realizar cálculo (pesava 30 toneladas e ocupava 180m²) e quase não tinha armazenador ou transmissor de dados, funções que foram posteriormente adquiridas.

### 2.2 Da Internet

A Guerra Fria criou uma grande conturbação na história na década de 1960. O conflito entre Estados Unidos e União Soviética atingiu seu ápice. Não ocorreu na verdade nenhum conflito bélico, a intenção na verdade era causar medo ao inimigo.

Assim, qualquer detalhe era um passo na frente do rival. A União Soviética saiu na frente ao criar o primeiro satélite artificial em 1957, o Sputnik. Do outro lado, os Estados Unidos buscou outra estratégia através da ARPA (*Advanced Research Project Agency*, ou Agência de Pesquisas em Projetos Avançados), que era um órgão cientifico militar criado em 1957, que tinha por função cuidar dos avanços tecnológicos e, posteriormente, da primeira rede.

Para prevenir um possível combate no território que pudesse acabar com toda a sua comunicação e o trabalho desenvolvido, os norte-americanos colocam em prática a ARPANET, que nada mais era do que uma rede de armazenamento de dados que inicialmente conectou algumas universidades e centros de pesquisas.

Já na década de 70, merece destaque Vinton Cerf e sua equipe que tentou conectar três redes distintas em um processo descrito como "*interneting"*, termo que hoje conhecemos como rede.

Apesar de tantos avanços, nem tudo foi benéfico. Bob Thomas, em 1971, criou o maior problema para os usuários de computadores: o vírus. Ele servia para quebrar o sistema de segurança da máquina.

No mesmo ano, Ray Tomlinson começou a desenvolver o tão indispensável e-mail. A ARPANET possuía alguns métodos de transmissão de mensagem entre o mesmo computador, mas havia a necessidade de um sistema que integrasse toda a ARPANET.

Em 1980 a internet já havia se desenvolvido bastante. Os chamados programadores expandiam as fronteiras da rede, criando novas funções.

## 3 Direitos Fundamentais

Em linhas gerais, os direitos e garantias fundamentais podem ser considerados os pilares do Estado de direito.

Os Direitos e garantias fundamentais são o conjunto de dispositivos da Constituição Federal que se destinam a oferecer, direitos, garantias e deveres aos cidadãos. São os dispositivos compreendidos entre o art. 5º ao 17º que sistematizam as noções básicas e centrais modulando a vida social, politica e jurídica de todo cidadão.

Como esses direitos foram surgindo de forma gradativa e de acordo com um determinado período histórico, os autores começaram a reuni-los em gerações ou dimensões, podendo ser sintetizado em:

O direito de primeira geração surgiu no século XVII e cuida dos direitos individuais. Seria o direito que é inerente ao homem, como o direito à liberdade, à vida, à propriedade, à manifestação, etc.

Os da segunda geração são também chamados de direitos sociais, econômicos e culturais. Nesse período passou-se a exigir uma maior intervenção do Estado para que a liberdade fosse protegida. Essa geração esta ligada ao direito à saúde, ao trabalho, a educação, etc.

Os direitos chamados de solidariedade, fraternidade compreendem a terceira geração, e são voltados a coletividade, ou seja, preocupou-se mais com o meio ambiente, patrimônio histórico e cultural.

O professor Paulo Bonavides é o defensor da quarta geração, que seria o resultado da universalização dos direitos fundamentais. Seria o exemplo do direito à democracia, à informação, ao comércio eletrônico entre os Estados.

Defendida por poucos autores para tentar justificar os avanços tecnológicos, criou-se o direito de quinta geração, que cuida das questões da cibernética ou da internet.

### 3.1 Dos Principais Direitos Fundamentais Violados Pelos Cibercrimes.

O direito a intimidade é configurado como um direito fundamental, ao qual confere ao individuo enquanto cidadão, o direito de se resguardar de ações praticadas por terceiros contra a sua pessoa, mais precisamente resguardando sua esfera intima e privada.

Para definir o que significa intimidade, há que se considerar vários aspectos, tais como o lugar, a época, bem como os valores sociais, políticos e

morais. Por não existir um conceito absoluto surge a dificuldade de uma definição precisa do termo.

A intimidade caracteriza-se como um direito personalíssimo, e que portanto é irrenunciável, o que significa que o detentor desse direito não pode abrir mão, devendo resguarda-lo de todas as maneiras.

Esse direito encontra respaldo no art. 5º, inciso X da CF:

> Art.5º: X- São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação.

Diante do artigo, percebe-se que houve uma preocupação do constituinte em proteger uma gama muito maior que só o direito a intimidade. No mesmo sentido, o legislador tutela direitos como a privacidade, a honra e a imagem, que assim como a intimidade possuem um conceito muito amplo e de difícil limitação jurídica.

Há quem confunda o direito de intimidade com o direito de privacidade pela intima relação que eles compreendem. Apesar da linha tênue entre ambos, existem características distintas que não permite tal confusão.

René Ariel Dotii de uma maneira matemática explica a distinção entre esses dois direitos fundamentais através da chamada teoria dos círculos concêntricos. Pela sua teoria a intimidade seria um circulo concêntrico e de menor raio que a vida privada.

No mesmo sentido Darcy Arruda Miranda propõe que devem ser considerados como pertencentes à Vida Privada da pessoa, "não só os fatos da vida íntima, como todos aqueles em que seja nenhum o interesse da sociedade de que faz parte". Dessa forma, a intimidade seria uma espécie do gênero privacidade.

Pode-se entender que o direito a intimidade se configura numa esfera mais intima que o individuo tem, abrange uma parte restrita e profunda de cada individuo.

Ao contrário, a vida privada caracteriza-se por um caráter mais amplo que a intimidade, ou seja, seriam as relações com a sociedade, com familiares, amigos, estando, portanto mais suscetível as regras do convívio social.

## 4. Conceito Do Crime De Informática

A conceituação é matéria importante sob o aspecto cientifico, pois é capaz de localizar o tema dentro do universo jurídico a que pertence.

De acordo com Carla Rodrigues Araújo de Castro (2003, p.9):

> "Os crimes de informática são aqueles perpetrados através dos computadores, contra os mesmos, ou através dele. A maioria dos crimes são praticados através da internet, e o meio usualmente utilizado é o computador".

Nesse mesmo sentido, de acordo com Patrícia Peck Pinheiro (2010, p.46):

> "Os Crimes digitais podem ser conceituados como sendo às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros".

Os chamados cibercrimes nada mais são que os crimes praticados no mundo real de uma forma mais avançada, o que dificulta muitas vezes a identificação do agente causador de dano. Esses crimes da internet podem derivar de diversas condutas, podendo se caracterizar desde uma ofensa, um preconceito, até uma clonagem de informações bancárias, ou acesso a documentos particulares.

Nos últimos tempos, tem sido comum o envio de e-mails simulando ser o remetente um órgão estatal conhecido, como por exemplo, Receita Federal, Tribunal Superior Eleitoral, Policia Federal, Serasa. O objetivo é enganar o destinatário alegando constar uma pendencia, e que para solucioná-la é só clicar no link indicado na mensagem. Ao efetuar o procedimento indicado, automaticamente se instala um programa que coleta dados pessoais do usuário da rede.

Diante de toda essa problemática que a internet trouxe foi que surgiu a necessidade de criação de uma lei que pudesse se adequar a essa nova era, para que não ficássemos presos a analogias jurídicas na hora de analisar os crimes virtuais.

## 5. Atualidade Legislativa

A grande crítica existente, antes da criação da lei 12.737/2012, era a deficiência legislativa acerca da falta de legislação sobre crimes da internet, já que os direitos que são protegidos pela lei, já guardavam respaldo na Constituição Federal, principalmente com o artigo 5º. Como exemplo podemos citar o inciso X que fala sobre a intimidade, a privacidade, a honra e a imagem. O inciso XII que fala sobre o sigilo das correspondências, comunicações telegráficas e telefônicas.

Vale ressaltar que o avanço dessa rede chamada internet, não era algo esperado pela sociedade de uma maneira geral, tanto que haviam críticas a respeito da lacuna penal sobre o tema. O avanço desse sistema era muito superior ao da sociedade, e esta caminhava a passos longos para acompanhar a velocidade da rede.

Interessante verificar que, o surgimento da lei apelidada "Carolina Dieckmann" muito tem a ver com a Teoria Tridimensional do Direito, criada por Miguel Reale, já que sua criação adveio da adequação do direito a sociedade, exatamente o que a teoria idealizava.

A teoria trazida por Reale parte do pressuposto que o fenômeno jurídico deve ser analisado e compreendido sob uma visão que engloba três aspectos: o fato jurídico, o valor e a norma propriamente dita.

Para Reale (2000, s/p):

> "O Direito não é apenas a norma ou a letra da lei, pois é muito mais do que a mera vontade do Estado ou do povo, é o reflexo de um ambiente cultural de determinado lugar e época, em que os três aspectos – fático, axiológico e normativo – se entrelaçam e se influenciam mutuamente numa relação dialética na estrutura histórica".

Diante do exposto, percebe-se a intima relação da criação da lei 12.737/2012 com o contexto social vivido. Já que a lei surgiu de um fato ocorrido com a atriz brasileira Carolina Dieckmann, que foi a mola propulsora para a criação da lei, tanto foi assim, que o diploma foi apelidado com o nome da famosa.

## 5.1 Análise Tipológica

Muitos acreditavam que os crimes ocorridos na internet pudessem ser combatidos com os tipos penais já existentes, e que a única diferença seria a

nomenclatura, como por exemplo, o estelionato ocorrido no mundo real, quando ocorresse no mundo virtual seria estelionato virtual.

Acreditavam que não era necessária a existência de uma lei especifica para a regulagem dos chamados crimes cibernéticos, pensavam que seria apenas um inchaço à legislação. Percebeu-se com o avanço da sociedade a necessidade de regulamentação, nascendo então a lei 12.737/2012.

Estabelece o artigo 154–A:

> 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.
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa

O tipo visa tutelar a liberdade individual, mais especificamente o sigilo de dados armazenados em dispositivos informáticos.

O delito pode ser classificado como “comum”, o que significa que o sujeito passivo pode ser qualquer pessoa, não se exigindo uma qualidade especifica do agente. Assim como o sujeito ativo, o passivo pode ser qualquer pessoa, em especial o proprietário ou possuidor do dispositivo informático, e inclusive terceiros que eventualmente podem ser atingidos pela conduta delituosa.

Pela análise objetiva do tipo penal, o verbo “invadir” é a figura nuclear do tipo, e deve ser entendido como “entrar sem direito ou sem autorização”. É o tipo comissivo em que o agente realiza uma conduta. O fato de se colocar um aviso “APENAS PESSOA AUTORIZADA” ou “CONFIDENCIAL” já deve ser considerado como mecanismo de segurança, não havendo a necessidade de existência de cadeado ou esconder num cofre para tipificar a invasão ou violação do sigilo.

Por “dispositivo informático” Pablo Guillermo Lucero e Alejandro Andrés Kohen (s/a, p. 15/16) definem como: “a ciência aplicada que trata do estudo e aplicação do processamento automático da informação, mediante a utilização de elementos eletrônicos e sistemas de computação”.

Esse dispositivo informático é conhecido por hardware, que significa qualquer dispositivo apto a armazenar dados para posterior consulta ou uso, e que “pode ou não estar ligado a rede de computadores”, denominada software. Esse

dispositivo informático deve ser alheio, o que significa que não deve pertencer ao agente que o utiliza.

É um crime de ação vinculada, o que significa que para ser caracterizado o crime, a conduta deve ser praticada “mediante violação indevida de mecanismo de segurança” (barreiras físicas ou virtuais que impedem ou limitam o acesso à informação por parte de terceiros mal intencionados), sendo que o termo indevido constitui elementar do tipo normativo.

Não basta a vontade livre e consciente de invadir dispositivo alheio, devendo a conduta ter uma das finalidades descritas na norma, sendo classificado pela doutrina, como um dolo específico.

O primeiro especial fim de agir, elencado de forma alternativa, seria aquele consistente em obter (assenhorear, alcançar, tomar posse), adulterar (alterar, corromper, viciar) ou destruir (eliminar, destruir, deteriorar por completo) dados ou informações (sequência de símbolos minimamente quantificada, processados por uma entrada em um dispositivo, aptos a serem armazenados, usados, ou transmitidos para outro dispositivo). Além disso, o legislador exige que esta conduta deva se dar “sem autorização expressa ou tácita do titular do dispositivo”.

O segundo especial fim de agir, previsto alternativamente pelo legislador penal, corresponde a instalar (processo destinado a colocar todos os dados necessários em um hardware para que determinado software possa ser executado) vulnerabilidades (abertura ou brecha em um sistema operacional, normalmente indesejada e oculta, que pode ser utilizada pelo invasor para executar códigos maliciosos) para obter vantagem ilícita (patrimonial ou extrapatrimonial).

Por ser um crime formal, a consumação ocorrerá com violação indevida de mecanismos de segurança, e a consequente entrada em dispositivo alheio sem autorização, independentemente de qualquer resultado naturalístico.

A tentativa é tecnicamente admitida, por ser um crime plurissubsistente, nas hipóteses em que por circunstâncias alheias a vontade do agente, o mecanismo de segurança não é violado, e ele não logra seu intento de invadir dispositivo informático alheio.

A ação penal do crime descrito no “caput” é pública condicionada a representação da vítima, exceto quando for praticado contra a Administração Pública direta ou indireta de qualquer dos Poderes da União, Estados, Municípios e Distrito Federal ou contra empresas concessionárias de serviços públicos.

Os dois parágrafos subsequente implicam em condutas equiparadas. O legislador ao criar o parágrafo primeiro quis sancionar a conduta do agente que desenvolve, difunde, distribui de forma gratuita ou onerosa o software malicioso. O parágrafo segundo majorou a pena se houver algum prejuízo econômico a vítima.

Já no parágrafo terceiro o legislador criou uma figura qualificada, onde dispõe uma pena própria se a obtenção de conteúdo for segredos comerciais ou industriais, informações sigilosas. Se o conteúdo contido no parágrafo terceiro for divulgado, comercializado ou transmitido a terceiro, haverá um aumento de pena previsto no parágrafo quarto.

Há uma causa de aumento de pena, no parágrafo quinto, se o crime for praticado contra: o Presidente da República, governadores e prefeitos; Presidente do Supremo Tribunal Federal; Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa do Estado, da Câmara Legislativa do Distrito Federal ou da Câmara Municipal; ou dirigente máximo da Administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

## 5. Conclusão

O presente trabalho analisou a evolução da internet, o conflito desta com os direitos fundamentais e a necessidade de uma norma que evitasse o uso de analogias pelo magistrado no julgamento dos crimes virtuais.

Comprovou-se que é necessária uma adequação do direito ao contexto social, e que o ordenamento jurídico não é um conglomerado de leis acabados em si, mas sim uma análise que deriva de três aspectos: de fato, valor e norma, assim como preconiza a Teoria Tridimensional do Direito, de Miguel Reale.

A existência de crimes que violam direitos tidos como fundamentais pela própria legislação pátria não poderiam passar despercebido pelo legislador. Diante da analise do tipo penal e da circunstância tecnológica que a sociedade moderna vive, entendeu-se que a lei 12.737 de 2012 que introduziu o artigo 154-A no Código Penal era necessária ao sistema brasileiro para a solução desses conflitos que o mundo jurídico, até então, não estava preparado para lhe dar.

**REFERÊNCIAS BIBLIOGRÁFICAS**


http://albertodiwan.jusbrasil.com.br/artigos/199631200/o-crime-de-invasao-de-dispositivo-de-informatica-art-154-a-do-codigo-penal?ref=topic_feed acesso em 14/08/2015

http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11825 acesso em 17/08/2015

http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=9963&revista_caderno=17 acesso em 10/08/2015

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília: Senado, 1988.

BRASIL. Código Penal (1940). **Constituição da República Federativa do Brasil.** Brasília: Senado, 1988.

http://www.cartaforense.com.br/conteudo/artigos/as-modificacoes-promovidas-pela-lei-carolina-dieckmann-no-codigo-penal/9986 acesso em 19/08/2015

CENTRO UNIVERSITÁRIO "ANTONIO EUFRÁSIO DE TOLEDO". **Normalização de apresentação de monografias e trabalhos de conclusão de curso.** 2007 – Presidente Prudente, 2007, 110p.

http://www.ebah.com.br/content/ABAAAeoVwAL/conceitos-iniciais-sobre-os-direitos-garantias-fundamentais-na-constituicao acesso em 19/08/2015

http://jus.com.br/artigos/24406/lei-carolina-dieckmann-e-a-definicao-de-crimes-virtuais acesso em 14/08/2015

http://jus.com.br/artigos/29647/delitos-ciberneticos-implicacoes-da-lei-12-737-12 acesso em 10/08/2015

http://www.rogeriogreco.com.br/?p=2183 acesso em 18/08/2015

http://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada-de-60-ate-anos-80-infografico-.htm acesso em 20/08/2015

http://www.tjdft.jus.br/institucional/imprensa/artigos/2010/direito-a-intimidade-e-privacidade-andrea-neves-gonzaga-marques acesso em 20/08/2015