Pesquisas:

Crimes de Violação de Sigilo Funcional.

Crimes Cibernéticos. Sigilo Profissional x Ética.

Liberdade de Expressão x Desinformação. Espionagem Industrial

1. Violação do Segredo Profissional

Por ACS —

Para a hipótese de divulgação de informações que a lei determine que são sigilosas, a pena prevista é de detenção de 1 a 4 anos e multa.

A norma tem o intuito de proteger o caráter de confiança nas relações profissionais.

Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: **Pena** - detenção, de três meses a um ano, ou multa.

Parágrafo único - Somente se procede mediante representação.

(Fonte: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/discriminacao-ou-preconceito#:~:text=Art.,a%20um%20ano%2C%20ou%20multa, data de acesso: 15/09/2020)

2. Sigilo profissional é uma preocupação

A preservação do sigilo das informações de uma empresa tem levado muitos empregadores a buscar soluções para proteger dados considerados secretos e estratégicos. A ideia é também evitar que eles caiam nas mãos de colaboradores mal-intencionados, visto que ética profissional é um atributo cada vez mais escasso no mercado corporativo.

A definição de sigilo profissional baseia-se no fato de o empregado preservar e não divulgar para terceiros, toda a informação que seja importante e fundamental para a operação da empresa, como dados de planejamentos, informações pessoais e financeiras de colaboradores e patrões.

Quebrar o sigilo profissional poderá representar um delito, conforme o art. 154 do Código Penal: *"Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a alguém".*

A pena cominada é detenção, de três meses a um ano, ou multa.

Para ser considerada quebra de sigilo, as informações divulgadas somente podem ter sido obtidas através da função ou ofício que empregado possui.

No artigo 482, letra "g", da Consolidação das Leis do Trabalho (CLT), encontramos também nesta outra base legal, sustentação para que o empregador possa obter o direito em mover uma ação pelos prejuízos causados por empregados que quebram o sigilo profissional, mas não podemos esquecer que o empregador deve inserir cláusula específica nos contratos de trabalho, na contratação de seus empregados.

O empregador deve inserir cláusulas de confidencialidade em seu contrato de trabalho, dando a ciência desta cláusula, bem como, formulando-a com clareza, quanto à importância de que o empregado deve manter o sigilo profissional, a partir da data de sua contratação.

Deverá ser estendido o prazo desta condição de sigilo profissional, inclusive até o período após seu desligamento da empresa, podendo até se tratar de um prazo indeterminado, o que seria o ideal, sendo assim, se o ex-empregado, segredos da ex-empresa.

Todo o profissional deve ter uma postura ética, guardando toda a informação de seu empregador/empresa, ou seja, a empresa lhe dá a confiança, lhes fornecendo toda informação necessária para que seu labor atinja o máximo em resultado, com a obtenção de todos os dados importantes de sua operação.

Mas atualmente temos visto muitos casos de quebra de sigilo por parte dos empregados, que revelam o *know-how* de suas empresas.

Escolhas são feitas na vida profissional, e sempre podemos dizer: "Quem planta colhe". Enfim, CUIDADO com o seu sigilo profissional.

Marco Antonio Granado é empresário contábil, contador, bacharel em direito, pós-graduado em direito tributário e consultor tributário e contábil do SINFAC-SP – Sindicato das Sociedades de Fomento Mercantil Factoring do Estado de São Paulo.

(Fonte: https://www.sinfacsp.com.br/conteudo/sigilo-profissional-e-uma-preocupacao, data de acesso: 15/09/2020)

3. Espionagem industrial, você sabe o que significa?

Publicado por Suellen Rodrigues Viana

A espionagem é a prática de obter informações de caráter secreto ou confidencial sobre governos, organizações, empresas ou até mesmo pessoas físicas, sem autorização

destes, para alcançar certa vantagem política, econômica, tecnológica ou social. A prática manifesta-se geralmente como parte de um esforço organizado e, em relação a empresas, tem-se a prática de espionagem industrial.

Contudo, a espionagem não tem um tratamento específico na legislação brasileira, sendo tratada de maneira esparsa na legislação penal, geralmente referenciada à espionagem militar, isto é, ao acesso e apropriação desautorizados de informações e dados atinentes à defesa. Entretanto, os efeitos jurídicos da espionagem não se cingem à esfera do direito penal, podendo também repercutir em outras instâncias do direito, como a civil e a administrativa.

Em relação a estes casos, tem-se a Lei nº 9.279/1996 (Lei da Propriedade Industrial) que protege segredos industriais, reputando concorrência desleal do seu uso desautorizado. A legislação impede, de forma ampla, o uso de dados de natureza confidencial que tenham sido obtidos durante relação contratual ou empregatícia, ou que tenham sido obtidos de forma ilícita ou fraudulenta (artigo 195, incisos XI e XII).

Temos, assim, uma legislação que oferece proteção aos segredos industriais e que permite que qualquer tipo de informação possa ser considerado como tal, desde que não seja pública, tenha relevância comercial e tenha sido objeto de medidas para resguardar sua confidencialidade. Dentre as informações mais comumente incluídas nesse rol, destacam-se listas de clientes, fornecedores, documentos contábeis, fiscais, financeiros, remuneração de funcionários, manuais, especificação de produtos, fórmulas, entre outros.

Já na jurisprudência, constata-se que caso seja comprovada a prática de espionagem industrial, o ensejo a uma ação de indenização é plenamente possível.

Verificada a prática do ato ilícito, a Lei de Propriedade Industrial oferece os instrumentos necessários para fazer cessar imediatamente a violação, como também para obter reparação pelos danos sofridos. Além disso, a possibilidade de que haja uma decisão liminar para impedir ou coibir tal prática é expressamente prevista, bem como a respectiva indenização pelos prejuízos causados (artigo 209 e 210 da referida lei).

Assim, a empresa poderá ingressar com uma Ação de Indenização por Danos Morais, fundada em violação de segredo empresarial e em concorrência desleal, com menção ao artigo 195, incisos XI e XII, da Lei de Propriedade Industrial.

Todavia, é imprescindível que se possa comprovar as alegações de espionagem do antigo funcionário ou de um funcionário atual através de provas, sejam elas através de documentos, oitivas de testemunhas, pericias. Caso contrário o dano moral não poderia ser comprovado e não estaria caracterizado.

Já na esfera penal, também se pode pensar na abertura de um inquérito policial, para a apuração da prática de crime de espionagem industrial e indicar os prováveis

envolvidos, dando ensejo ao início das investigações policiais e posterior oferecimento de denúncia pelo Ministério Público.

De outro modo, a empresa poderá tomar medidas preventivas mais eficazes, de forma que se possa combater a prática da espionagem, tais como:

- Assinatura de termos de confidencialidade com fornecedores, empregados e colaboradores que tenham acesso aos segredos, estabelecendo claramente a confidencialidade das informações e as práticas vedadas pela empresa;
- Adoção de ferramentas tecnológicas que limitem o acesso às informações, bem como identifiquem rapidamente qualquer acesso indevido. Para isso, é importante que se mantenha o registro (*back-up*) dos acessos por períodos longos, pois não raro o ilícito se da de forma contínua. A repetição da conduta pode constituir elemento importante para comprovar a intenção de apropriação indevida;
- Treinamento constante de fornecedores, funcionários e colaboradores, para que adotem práticas aptas a proteger os segredos a que têm acesso. É importante ter em mente que o vazamento de informações pode ocorrer não só em vista de indivíduos imbuídos de má-fé, mas também em decorrência de condutas inadequadas que permitam o acesso a informações tanto interna quanto externamente. Esse é o caso de compartilhamento de dados através de e-mails, mídias sociais, dispositivos móveis, ou até mesmo locais de frequência pública;
- Adoção de uma política interna que permita não só avaliar constantemente as medidas adotadas para a proteção de informações, como também identificar eventuais atos ilícitos e
- É importante que sejam rapidamente adotadas medidas extrajudiciais e judiciais, a fim de evitar ou mesmo mitigar os prejuízos causados pela violação. Tal política também tem como efeito positivo desencorajar novas práticas dentro da empresa.

Ressalta-se que essas medidas são apenas sugestões que contribuirão para um melhor controle dos dados da empresa, de forma que ignorar os fatos, deixando de adotar medidas que os protejam, pode comprometer de forma irreversível o futuro da empresa.

Suellen Rodrigues Viana
Advogada, graduada pela Universidade do Extremo Sul de Santa Catarina - UNESC. Pós-graduada em Direito Imobiliário pela Escola Paulista de Direito. Advogada atuante nas áreas de Direito do Consumidor, Direito Civil, Empresarial e Direito Imobiliário. Realiza diligências (em geral) nos Órgãos Judiciais e Cartórios Extrajudiciais nas Comarcas de Criciúma e Região. Contato: suellenrviana.adv@gmail.com

(Fonte: https://suellenrvianaa.jusbrasil.com.br/artigos/432306800/espionagem-industrial-voce-sabe-o-que-significa#:~:text=A%20espionagem%20%C3%A9%20a%20pr%C3%A1tica,%2C%20econ%C3%B4mica%2C%20tecnol%C3%B3gica%20ou%20social, data de acesso: 15/09/2020)

4. Lei que torna crime invadir celulares, tablets e computadores entra em vigor

Edição do dia 02/04/2013
02/04/2013 21h21 - Atualizado em 02/04/2013 21h49
Lei 12.737 ganhou o nome de Carolina Dieckmann porque a atriz denunciou o caso do qual foi vítima de roubo e divulgação de fotos íntimas. Se houver furto e divulgação de dados, a pena pode chegar a dois anos de prisão.

Entrou em vigor, nesta terça-feira (2), a lei que torna crime invadir computadores, celulares e tablets.

Se houver furto e divulgação de dados, a pena pode chegar a dois anos de prisão.

Ex-namorados vingativos, mulheres ciumentas, colegas difamadores. Muita gente assim já usou computadores e celulares para bisbilhotar ou agir contra seus desafetos. Agora isso é crime.

"Essa lei vem resolver um problema, que é a lacuna relacionada à invasão", avalia o advogado Renato Ópice Blum

A Lei 12.737 ganhou o nome de Carolina Dieckmann porque a atriz denunciou o caso do qual foi vítima de roubo e divulgação de fotos íntimas.

Agora quem invadir equipamentos de informática alheios para obter, adulterar ou destruir informações está sujeito a multa e prisão de três meses a um ano, podendo chegar a dois anos se forem roubados segredos comerciais, industriais - informações sigilosas. O crime fica mais grave se for cometido contra autoridades ou contra serviços públicos.

Mas para fazer uso da nova lei é preciso antes proteger computadores, tablets e celulares com programas de segurança ou ao menos uma senha porque é a quebra dessa proteção que caracteriza o crime. Quem se tornar vítima precisa tomar providências rapidamente.

O ideal é parar de usar e encaminhar o dispositivo violado para perícia, o conteúdo deve ser guardado como prova. É preciso comunicar o provedor ou a operadora e pedir preservação das provas, depois fazer o boletim de ocorrência.

"Pode ser tanto delegacia especializada em crimes eletrônicos ou, se não tiver na cidade dela, a delegacia comum. Tem que fazer o boletim de ocorrência nessa lei específica", explica a advogada Patricia Peck.

A nova lei também equiparou cartão de crédito e débito a documento particular. Clonar e vender as informações, como aconteceu com Roberto, é crime tipificado. Roberto já foi vítima também de invasão de email e teve sua identidade em uma rede social roubada.

"Ele me disse o seguinte: 'Você quer seu Twitter de volta? Custa 1,5 mil'. A sensação de insegurança é muito grande. Acredito que com a lei nova talvez as coisas mudem", ele diz.

Correção: Na reportagem que foi ao ar e no vídeo aqui publicado, identificamos incorretamente que a advogada Patricia Peck como Roberta Peck.

(Fonte: http://g1.globo.com/jornal-nacional/noticia/2013/04/lei-que-torna-crime-invadir-celulares-tablets-e-computadores-entra-em-vigor.html, data de acesso: 15/09/2020)

5. A obrigação de manter o segredo profissional: razão e consequências

JUL 5, 2018
Por Maria Luiza Gorga

Em nosso ordenamento, o sigilo profissional goza de relevância tal que sua revelação constitui crime, conforme previsto no art. 154 do Código Penal[1], servindo como verdadeiro corolário da garantia constitucional de intimidade, valendo esclarecer que a proibição de divulgação recai não apenas sobre a revelação verbal, mas inclusive sobre o fornecimento de documentação ou de esclarecimentos escritos, inclusive a autoridades.

A razão desta proteção é o fato de que, durante a vida em sociedade, os indivíduos deparam-se com questões de cunho pessoal que só podem ser resolvidas mediante o auxílio de terceiros tecnicamente qualificados, os quais então passam a ser confidentes do indivíduo, de modo que tais segredos e intimidades devem ser preservados não apenas em favor do indivíduo, como também de todo o tecido social, pois do contrário tais profissões perderiam seu prestígio e sua atividade estaria impossibilitada[2], bem como a revelação de inúmeros segredos poderia levar ao caos em núcleos sociais e familiares.

Esse dever de sigilo, contudo, não é limitador da obrigação do profissional de saúde em levar a conhecimento das autoridades o crime de ação pública de que tenha conhecimento em razão da função e que envolva o paciente como vítima, posto que a inação neste caso é tutelada no art. 66 da Lei de Contravenções Penais[3]. Também no próprio Código Penal, no art. 269, há caso expresso de obrigatoriedade de quebra do sigilo profissional, e de relevância tal que também foi alçado à seara criminal, que é o fato de "deixar o médico de denunciar à autoridade pública doença cuja notificação é compulsória" – neste caso, a saúde pública afigura-se interesse superior àqueles protegidos pela guarda do segredo, em tal grau que não apenas afasta o dever de sigilo, como também configura novo tipo penal.

Outra exceção possível é o estado de necessidade, de modo que a revelação do segredo profissional não constitui crime quando motivada pela necessidade de salvaguarda de um interesse contrário, cujo sacrifício, nas circunstâncias do caso concreto, não é razoavelmente exigível. Nesse sentido o CREMESP já deu pareceres no sentido de que em

caso de suspeita de crime de abuso sexual por parte do genitor do paciente, é possível a revelação ao Ministério Público[4]. De outro lado, já definiu que diante de abortamento, ainda que provocado, não pode o profissional comunicar o fato às autoridades, pois neste caso se caracteriza o sigilo[5].

De fato, o sigilo profissional não é absoluto, mas deve respeitar limites que não se confundem com a simples consciência individual do profissional – dessa forma, se é possível a violação do segredo para a proteção do paciente, esta é punida no caso do médico que quebra seu sigilo em caso que estará apenas prejudicando indivíduo que lhe procurou em razão de apuro médico, não importando eventual julgamento moral do profissional pois deve prevalecer a ordem social e a confiança na profissão como um todo.

O próprio Código de Ética Médica[6] dispõe longamente sobre o tema, prevendo que o motivo justo pode também incluir a defesa da saúde pública, em uma acepção ampla, indo além das moléstias de notificação compulsória. Há caso concreto interessante no qual se afastou o dever de sigilo pelo fato de que as condições de saúde de um paciente, em confronto com seu histórico pessoal e de trabalho, indicavam a possibilidade de vazamento de um reator nuclear, situação que "extrapola os limites da empresa, caracterizando uma catástrofe."[7].

Em resumo, a grande razão de ser do sigilo médico é a proteção à intimidade, à vida privada e à honra, constitucionalmente garantidas em nosso ordenamento, preceito que remonta às épocas antigas, já constando do juramento de Hipócrates que "o que, no exercício ou fora do exercício e no comércio da vida, eu vir ou ouvir, que não seja necessário revelar, conservarei como segredo", sendo assim uma das reservas morais da medicina e que, felizmente, conta com proteção legal.

A questão, contudo, não é sem percalços, sendo comum o pedido judicial ou administrativo de dados de pacientes e procedimentos, inclusive afirmando a autoridade que o profissional poderá sofrer as penas do crime de desobediência.

Na década de 1960 o Supremo Tribunal Federal posicionou-se que seria constrangimento ilegal exigir do profissional a violação do segredo sobre a documentação de paciente[8]. Nos anos 1980 a temática voltou à pauta do STF, em caso envolvendo a Santa Casa de Misericórdia de São Paulo que a Santa Casa negou-se a fornecer ficha clínica solicitada pela Justiça, alegando o sigilo profissional[9].

Neste último caso a Corte entendeu que o meio-termo proposto pela Santa Casa, de fornecer o laudo apenas ao perito, estaria satisfatoriamente resguardando o sigilo profissional e, ao mesmo tempo, permitindo a colheita probatória.

Outro caso resolvido pela Corte Paulistana, em 2011, também estabelece a viabilidade de um meio-termo segundo o qual o prontuário ficaria "disponível para ser analisado nas dependências do hospital em qualquer dia útil, em horário comercial, por

médico ou outro profissional da área de saúde sujeito a obrigação de manutenção do segredo profissional, nomeado por quem de direito, para colher as informações das quais necessita"[10].

Em um último exemplo, temos decisão da 15ª Câmara de Direito Criminal do Tribunal de Justiça do Estado de São Paulo que, voltando à linha adotada pelo STF em 1962, trancou ação penal apresentada em face de mulher que fora denunciada pela prática do aborto com base em relatos da profissional que a atendeu no hospital público[11].

Percebe-se, portanto, que a questão é complexa e sujeita a divergências de interpretação pelos magistrados. Assim, é importante o profissional ter em mente que as autoridades Judiciárias e Policiais têm o poder de requisitar a documentação se munidos de decisão judicial que os autorize, sendo recomendado, para se evitar litígios, a colaboração com as investigações, solicitando que se decrete sigilo sobre os autos, pelo conteúdo sensível do material fornecido. Ao agir dessa forma, o profissional estará respeitando as normativas sobre o sigilo profissional e, ao mesmo tempo, preservando-se de qualquer acusação de desobediência.

Já em situações em que não se tenha uma ordem judicial, bem como não se enquadre em hipóteses de divulgação necessária conforme salientado acima, o segredo deve permanecer, sob pena de responsabilização criminal e civil, inclusive com indenização pelos danos morais e materiais sofridos pelo indivíduo atingido – e isso inclui divulgações em redes sociais e aplicativos de mensagens instantâneas, devendo o profissional, caso deseje discutir algum caso específico, faze-lo apenas em grupo fechado e composto por médicos, sem elementos que permitam a identificação do paciente.

Notas

[1] "Art. 154 – Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena – detenção, de três meses a um ano, ou multa."

[2] Deve haver um nexo causal entre a atividade e o segredo a ser guardado. Por exemplo, não basta ser médico para que todos os segredos a si confiados tomem relevância penal, devendo estes terem relação com a atividade profissional médica.

[3] "Art. 66. Deixar de comunicar à autoridade competente:

(…)

II – crime de ação pública, de que teve conhecimento no exercício da medicina ou de outra profissão sanitária, desde que a ação penal não dependa de representação e a comunicação não exponha o cliente a procedimento criminal"

[4] CREMESP – Consulta n. 158.626/2012.

[5] CREMESP, Consulta n. 151.842/2016.

[6] "É vedado ao médico:

Art. 73. Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente.

Parágrafo único. Permanece essa proibição: a) mesmo que o fato seja de conhecimento público ou o paciente tenha falecido; b) quando de seu depoimento como testemunha. Nessa hipótese, o médico comparecerá perante a autoridade e declarará seu impedimento; c) na investigação de suspeita de crime, o médico estará impedido de revelar segredo que possa expor o paciente a processo penal.

Art. 74. Revelar sigilo profissional relacionado a paciente menor de idade, inclusive a seus pais ou representantes legais, desde que o menor tenha capacidade de discernimento, salvo quando a não revelação possa acarretar dano ao paciente.

Art. 75. Fazer referência a casos clínicos identificáveis, exibir pacientes ou seus retratos em anúncios profissionais ou na divulgação de assuntos médicos, em meios de comunicação em geral, mesmo com autorização do paciente.

Art. 76. Revelar informações confidenciais obtidas quando do exame médico de trabalhadores, inclusive por exigência dos dirigentes de empresas ou de instituições, salvo se o silêncio puser em risco a saúde dos empregados ou da comunidade.

Art. 77. Prestar informações a empresas seguradoras sobre as circunstâncias da morte do paciente sob seus cuidados, além das contidas na declaração de óbito.

Art. 78. Deixar de orientar seus auxiliares e alunos a respeitar o sigilo profissional e zelar para que seja por eles mantido.

Art. 79. Deixar de guardar o sigilo profissional na cobrança de honorários por meio judicial ou extrajudicial.

[7] CREMESP, Consulta n. 151.000/2011.

[8] STF, Pleno, HC 39.308, Rel. Min. Pedro Chaves, j. 19.09.1962.

[9] STF, RE 91.218, Rel. Min. Djaci Falcão, j. 10.11.1981.

[10] TJSP, Mandado de Segurança 0062265-58.2011.8.26.0000, Rel. Des. Vico Mañas, j. 1.6.2011.

[11] Cf.: https://www.conjur.com.br/2018-mar-13/ilicita-prova-aborto-obtida-denuncia-medico-tj-sp. Acessado em: 19.04.2018. Infelizmente o caso não é de todo incomum, sendo que a maioria das investigações por aborto no Brasil iniciam-se após denúncias do próprio médico. Cf.: http://www1.folha.uol.com.br/cotidiano/2015/02/1592839-medico-chama-policia-apos-atender-jovem-que-fez-aborto-na-grande-sp.shtml. Acessado em: 19.04.2018.

(Fonte: http://www.ibdee.org.br/a-obrigacao-de-manter-o-segredo-profissional-razao-e-consequencias/, data de acesso: 15/09/2020)

6. Crimes Cibernéticos e Invasão de Privacidade à luz da Lei Carolina Dieckmann

Neil Silveira | Mirian Lima de Sousa | Antonia Morgana de Alcântara Jorge Melo

Publicado em 10/2017. Elaborado em 10/2017.

O crime virtual foi surgindo e houve a necessidade de regular os delitos informáticos. Assim, foi criada Lei 12.737/2012, chamada de lei Carolina Dieckmann advinda dessa necessidade de tutelar os bens jurídicos advindos do mundo virtual.

INTRODUÇÃO

Esse estudo tem por escopo a análise dos Crimes Cibernéticos ou Cibercrimes no Brasil, frente ao avanço tecnológico ocorrido nos últimos anos, e que o Direito necessita moldar e deixar-se moldar para acompanhar e solucionar tais conflitos provindos dessa significativa mudança.

Com o passar do tempo, a sociedade sofreu mudanças radicais em sua forma de ser e existir, principalmente de se comunicar, surgindo então, a tecnologia cibernética, uma verdadeira "Revolução Informática", criada para beneficiar a população, que necessitava cada vez mais de rapidez na troca de informações e que trouxe inúmeros benefícios economicamente, politicamente, culturalmente e socialmente.

O avanço tecnológico revolucionou a sociedade e o campo do Direito, exigindo assim, que a área jurídica, que rasteja para acompanhar e solucionar os litígios advindos desse avanço, resultados do mau uso da internet, possa se adequar significativamente a essas mudanças, mesmo não alcançando a velocidade desejada, ao mesmo tempo, se beneficia de tais avanços, solucionando os conflitos através das tecnologias oriundas do mesmo.

Os crimes cibernéticos ganharam, com o passar dos anos, uma nova roupagem: fotos íntimas publicadas na rede, invasão de privacidade através da web, invasão de contas bancárias, enfim, uma infinidade de mudanças. Todo tipo de transformação traz consequências, questionamentos e abre caminhos para novas decisões e mudanças de paradigma, fazendo com que a sociedade cobre do Poder Judiciário e do Estado, um estudo detalhado, ações e leis capazes de defender os direitos daqueles que são vítimas de crimes dessa natureza.

O foco deste estudo volta-se para o caso da atriz Carolina Dieckman, que foi vitimada em maio de 2011, quando teve seu computador invadido por hackers que roubaram suas fotos íntimas e publicaram na internet. O caso teve grande repercussão na mídia nacional que motivou a aprovação da Lei 12.737 de 30 de novembro de 2012,

conhecida também como “Lei Carolina Dieckman”, que veio alterar os artigos 154, incluindo os artigos 154A e 154B, como também 266 e 298, todos do Código Penal.

CRIMES CIBERNÉTICOS

Com o aperfeiçoamento dos computadores e a evolução da internet e dos meios digitais de acesso a ela, a atuação dos criminosos foi modificando-se ao longo dos anos e os crimes virtuais ganharam uma nova roupagem, não apenas para prática de espionagem e sabotagem das máquinas, mas em manipulações bancárias, pirataria em programas de computador, pornografia infantil, racismo, abuso sexual, dentre outros.

No Brasil, a internet chegou somente na década de 1990, mas o cibercrime já era um problema posto em cogitação desde a criação dos computadores, surgindo as primeiras preocupações sobre o tema na década de 1960, tendo como características a sabotagem, espionagem, uso abusivo de computadores e sistemas, denunciados em matérias jornalíticas. (SILVA, 2000).

É inegável que a prática de crimes como a pornografia infantil, o racismo, o abuso sexual, entre outros, já eram bem praticados em nosso País e já existiam bem antes do surgimento do computador. Com efeito, o surgimento da internet veio incrementar essa prática que cresceu com o advento e a evolução virtual, onde este tipo de delito necessita do uso de tecnologias digitais para alcançar seu objetivo final, que é a consumação.

O cibercrime começou com uma brincadeira de criança. Em 1982, um estudante do ensino médio, querendo pregar uma peça em seus colegas, escreveu o vírus Elk Cloner para computadores Apple2. Esse pequeno pedaço brincalhão de código gerava um poema (bem ruim, diga-se) na tela de quem reiniciasse 50 vezes o computador com um disquete infectado. E assim foi criado o primeiro vírus, que também trouxe uma inovação importante: um sistema de autopropagação.

Como pode ser constatado acima, os crimes virtuais tiveram início mais cedo em outros países, porém, no Brasil, tiveram destaque nas principais colunas jornalísticas apenas no ano de 1997, não deixando de lado sempre a conscientização que a população tinha desde que a internet começou a ser comercializada no Brasil, sobre a ameaça e consumação desses mesmo crimes que já eram praticados presencialmente, passaram a ser praticados virtualmente, tais como clonagem de cartões, pedofilia, racismo, assedio sexual, dentre outros.

Dessa forma, os principais crimes virtuais mais comuns no Brasil. Dentre eles estão: calúnia, insultos, difamação, revelar segredos de terceiros, divulgação de material íntimo, como fotos e documentos, atos obscenos, apologia ao crime, preconceitos/racismo e pedofilia (POZZEBOM, 2015, p. 03).

Os crimes contra a honra (calúnia, injúria e difamação) e a incitação aos crimes contra a vida são tratados, geralmente, pela Polícia Civil. Quando se trata de tráfico de drogas, quando extrapole ou não os limites ncionais e atribuição de investigar é da polícia Federal, cabendo a atribuição suplementar às Polícias civis, ou seja, das duas polícias judiciárias têm atribuição para tratar do assunto dentro do País e extrapolando os limites a função privativa é da PF. (WENDT, 2011, p. 83-84).

A LEI 12.737/2012- CAROLINA DIECKMANN

A Lei 12.737/2012 surgiu a partir do projeto de Lei nº 2.793/2011, que foi aprovado após o caso da atriz Carolina Dieckman, que teve seus dados acessados por crackers que, através de um e-mail infectado que atriz teria dado um click, acessaram seu computador pessoal, obtendo fotos íntimas da atriz, inclusive nua, e fotos familiares com o filho de apenas quatro anos de idade. Inicialmente cogitou-se a hipótese de a invasão ter sido feita na loja em que Carolina teria consertado o computador meses antes.

Logo depois, ficou comprovado que, de fato, foram hackers do interior de minas Gerais e de São Paulo que praticaram o delito. A atriz foi chantageada pelos criminosos que exigiram o pagamento de R$ 10 mil para que as fotos não fossem divulgadas nas mídias sociais (MENDES, 2012).

Carolina registrou o boletim de ocorrência, quando foram iniciadas as investigações sobre o caso, três dias após a publicação das imagens a fim de evitar mais exposições. Como o Brasil não tinha uma lei específica para crimes de informática, os envolvidos foram indiciados por furto, extorsão qualificada e difamação, todos do Código Penal Brasileiro.

Antes do caso da atriz, muitas vítimas já eram registradas, no entanto, o caso ganhou destaque por se tratar de uma figura pública.

Este é um caso clássico do chamado phishing (envio de mensagens de spam contendo links para sites falsos), geralmente oferecendo algum benefício, mas que no fim baixam um programa malicioso no computador (MACHADO, 2012).

Geralmente ocorre com computadores desatualizados, sem qualquer tipo de proteção como antivírus, onde a máquina pode ser contaminada com apenas um click em e-mails contaminados ou até mesmo nas redes sociais como Facebook e Twitter, podendo os hackers através desses dispositivos acessarem qualquer tipo de dados pessoais das vítimas que estejam armazenados (MACHADO, 2012).

Segundo dados do FBI, só nos EUA acontecem 31 mil ataques de phishing por mês, ou seja, mais de mil por dia, e 11 milhões de pessoas tiveram suas identidades digitais roubadas em 2011. No mundo, 187 milhões dessas identidades foram roubadas em 2011, segundo a Symantec, e um entre cada 239 e-mails continha malware (MACHADO, 2012, p.02).

O primeiro suspeito encontrado foi Diego Fernando Cruz, de 25 anos, que teria sido o primeiro a divulgar as fotos na internet. Com um mandado de busca e apreensão, os policias entraram no quarto dele, em Macatuba, no interior de São Paulo. No local, foram encontrados CDs, softwares e cinco computadores. Um laptop estava aberto em uma página só com fotos da atriz. Uma das pastas de arquivo estava nomeada como "Carola", mas a maioria dos arquivos tinha sido completamente apagada. “Formatei ontem”, disse Diego.

O principal suspeito de ter invadido o computador e furtado as fotos da atriz é Leonan Santos, de 20 anos que vive numa casa simples em Córrego Dantas, em Minas Gerais. Ele já é investigado em outra ação de hackers, que teriam desviado dinheiro de um banco pela internet, mas se disse inocente. Pedro Henrique Mathias seria o dono do site que publicou as fotos. O quarto integrante não teve a identidade revelada pela polícia.

Os investigadores interceptaram uma troca de mensagens pela internet entre o grupo, em que Diego admite a divulgação das fotos: “Eu passei ‘pro’ cara na quinta (3) à noite. Ele pôs no site dele na sexta (4) de tarde. Na mesma hora estava em todos os jornais”. ‘Ela tinha que ter cuidado de apagar, né’?"

Com a repercussão do caso da atriz, foi sancionada a Lei 12.737 de 2012, que entrou em virgor dia 02 de abril de 2013, a chamada Lei “Carolina Dieckcmanm”, que torna crime a invasão de aparelhos eletrônicos para obtenção de dados particulares. Esta lei alterou o Código Penal Brasileiro acrescentando os artigos 154-A a 154-B, que estão dentre os crimes contra a liberdade individual, na seção que diz respeito aos crimes contra a inviolabilidade dos segredos profissionais.

Art 154-A. Invadir dispositivo informático alheio, conectado ou nõ à rede de computadores, mediante violação indevida de mecanismo de segurança e com 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. § 1º Na mesma pena incorre quem produz, ofefece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput [...] Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal e Municípios ou contra empresas concessionárias de serviços públicos.

Diante do exposto, percebe-se que antes do advento da Lei 12.737/2012, não havia um dispositivo específico para enquadrar quem cometia crime de invasão de dispositivos informáticos. Com o advento da Lei Carolina Dieckmann, quem comete esse tipo de invasão, agora será indiciado, baseado nesta lei. Antes do caso da atriz, muitas vítimas já eram registradas pelo Brasil.

Muito se tem discutido, recentemente, acerca de algumas particularidades acerca da Lei 12.737/2012, que não dispõe de meios processuais que possam garantir sua efetiva eficácia. Sabemos que as investigações de delitos informáticos se tornam dificéis por conta da morosidade, e em muitos casos, quando é solicitado algum IP (Internet Protocol) aos provedores de internet, não há a preservação desses registros como deveriam ser feitos e a enorme burocracia na hora fornecer os registros de conexão.

Nesse contexto, vimos anteriormente o caso do Juíz Luís Moura Correia, da Central de Inquéritos da Comarca de Teresina, no Piauí, que em 11 de fevereiro de 2015, determinou que uma empresa de acesso à internet suspendesse o funcionamento do aplicativo de mensagens Whatsapp no Brasil, por conta do não fornecimento de informações a justiça pela empresa responsável pelo aplicativo (HIGA, 2015).

O projeto de lei 21.626/11, conhecido popularmente como o Marco Civil da Internet, é uma espécie de "constituição" que vai reger o uso da rede no Brasil definindo direitos e deveres de usuários e provedores da web no país. No dia 25 de março de 2014, após quase três anos de tramitação na Câmara, o plenário da Casa aprovou o projeto (Portal EBC, 2014).

O Marco Civil da Internet, Lei 12.965/2014, foi aprovado pelo Senado no dia 23 de abril de 2014, e veio preencher as lacunas deixadas pela Lei Carolina Dieckmann e também é fruto de questionamentos advindos após os escândalos de espionagem protagonizados pelos Estados Unidos.

O art. 154-A do Código Penal Brasileiro, que foi incluído pela Lei 12.727/2012, traz, em sua redação, que a simples invasão de dispositivo móvel alheio não configura tipo penal incriminador, somente se houver uma violação, adulteração de mecanismo de segurança, ai sim, se configura o tipo penal, ou seja, se alguém invadir o computador de outrem não configura crime, mas se o dipositivo invadido contiver senhas, antivírus ou outros meios de segurança, haverá a conduita delitiva:

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.** § 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.

§ 2o Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 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: **Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.**

§ 4o Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Muito se tem discutido também a respeito das penas impostas pela Lei Carolina Dieckamann, que nada inibem seus invasores. São penas bastante brandas que dão entendimento que o crime relamente ficará impune. Se o objetivo da criação da Lei era inibir os hackers na prática de seus delitos, infelizmente com a aplicação das penas impostas pela mesma não se obterá resultado meramente satisfatório como almejado.

A Lei também inclui em seu art. 3º a interrupção ou perturbação de serviços telegráficos, informáticos ou de informação de utilidade pública, deixando sem amparo legal os sites de particulares que ficaram de fora da norma.

Outro ponto importante também, é que a Lei deveria ter criado a responsabilidade criminal dos administradores dos sites de redes sociais por injúrias, difamações, calúnias e demais crimes praticados contra terceiros, por falta de controle de acesso, embora faturem bilhões de dólares, utilizando, por exemplo, a tão comentada teoria do conhecimento do fato, responsabilidade objetiva (CASTRO, 2013, p.02).

Pode-se mencionar outra dificuldade que as autoridades têm na hora de aplicar o tipo penal é a identificação dos criminosos. De acordo com o Marco civil da internet, Lei 12.965/14, os provedores são obrigados a manter as informações de acesso armazenadas por um período de 6 meses, podendo o Judiciário solicitar aos provedores que seja armazenado por um período superior, caso seja relevante. Contudo, quando solicitados os dados aos provedores há uma burocracia muito grande na liberação das informações, que na maioria dos casos, geram brigas judiciais infrutíferas, como já citados anteriomente. Neste sentido, preceitua a referida Lei 12.965/2014:

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos, deverá manter os respectivos registros de acesso a aplicções de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de (6) meses, nos termos do regulamento §1º Ordem judicial poderá obrigar, por tempo certo, os provedores de

aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado. § 2º A autoridade policial ou administrativa ou Ministério Público poderão requerer cautelarmente a qualquer provedor de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§3º e 4º do art. 13.

Portanto, levando-se em consideração esses aspectos e lacunas encontradas nesta Lei, podemos concluir que o Brasil não necessita de leis novas para que a justiça se efetive, basta que as leis já existentes sejam cumpridas e aplicadas integralmente. É inegável, porém, que apesar de encontrar amparo legal antes da promulgação da lei de crimes virtuais nossa Constituição, Código Penal, Estatuto da Criança e do Adolescente e outras leis, já desempenhavam importante papel no controle das ilegalidades cometidas no campo virtual, uma vez que o homem tornou-se vulnerável em meio às ameaças que essa evolução oferece e que foram se aprimorando ao longo dos anos.

Contudo, apesar de a nossa Carta Maior assegurar a inviolabilidade, intimidade, honra e vida privada, ainda há uma insegurança muito grande nas relações provindas da internet, visto que a incidência de crimes e abusos tem sido cada vez maior foi necessitando de uma mudança urgente em nosso ordenamento jurídico.

CONCLUSÃO

O mundo virtual é imensurável e além das decobertas que beneficiam as investigações e elucidações de casos no campo do Direito, a tecnologia trouxe o aperfeiçoamento das relações humanas na arte da comunicação. As pessoas foram cada vez menos se utilizando de meios manuais como: cartas, telegramas, uso da escrita em papel, para utilizar meios eletrônicos, entrando em desuso a antiga carta que demorava chegar ao seu destino, por e-mails e outras técnicas de comunicação que foram surgindo nas últimas décadas.

Atualmente, o cliente pode acessar sua própria conta através do celular, a qualquer tempo, em qualquer lugar através da internet, sem precisar se deslocar à agência bancária tornando o atendimento mais célere. Com isso, a tecnologia ultrapassa classes sociais beneficiando ricos e pobres e com a mais alta velocidade que os outros meios de comunicação como jornais, rádio, televisão, não oferecem.

As pessoas foram cada vez mais se interessando e utilizando essa poderosa ferramenta, e usufruindo de tantos benefícios, utilizando meios eletrônicos como forma de comunicação e transações comerciais nas diversas áreas do Direito, bem como as do Consumidor e Civil como: compras, vendas, trocas, redes sociais possibilitando romper barreiras com a interação entre diversas raças e culturas.

Dessa forma, trouxe também desvantagens e malefícios provindos de sua má utilização por pessoas de má-fé que se escondem por trás das telas, e que, muitas vezes, acabamos por nos relacionar sem saber a conduta e a índole de quem trocamos informações. Sabendo de toda a carência e morosidade ao combate a este tipo de delito, os "criminosos informáticos" acabam agindo com certa segurança por tantas vantagens que lhes beneficiam, como a velocidade na hora de cometer tais condutas, o "anonimato" e a carente fiscalização na área.

Podemos concluir, assim, que ninguém está isento de ser vitimado de um delito dessa natureza, como vimos o caso da famosa Daniella Cicareli, que teve seu vídeo íntimo publicado nas redes sociais, e o caso da famosa Carolina Dieckmann que após ter seu dispositivo informático invadido, o projeto de Lei nº 2.793/2011 que já estava em tramitação foi aprovado, resultando na Lei nº 12.737/2012.

Pela observação dos aspectos analisados no que se refere à pornografia da vingança, podemos concluir que a maioria das vítimas são mulheres e existe um fio condutor que liga todos os casos: a continuidade. Esse tipo de crime se diferencia dos outros crimes cometidos pelo quesito da continuidade. Não há como se retirar o material publicado por completo da rede. Ele ficará lá para sempre podendo ser utilizado por uma pessoa de má índole a qualquer momento ou até mesmo com fins comerciais.

Por todos os aspectos analisados, deve-se reconhecer que o Brasil já deu um grande passo na tentativa de punir os criminosos virtuais com o advento da Lei Carolina Dieckmann e o Marco Civil da internet. Esperamos, contudo, que o Direito consiga acompanhar essas significativas mudanças que ocorrem no mundo virtual a cada instante, e alcance o objetivo almejado que é o combate à prática delitiva virtual.

Que mais Delegacias de crimes cibernéticos sejam instaladas pelo Brasil afora com o objetivo de facilitar o amparo às vítimas. Que a tecnologia seja utilizada de forma objetiva e positiva para somar o ordenamento jurídico já existente a essa nova ferramenta importante e eficiente.

REFERÊNCIAS

ALCÂNTARA, Lucas; CASTRO, Raphaella. **Cibercrimes e a tardia Legislação Brasileira**, 9 de janeiro de 2014. Disponível em: <https://www.profissionaisti.com.br/2014/01/cibercrimes-e-a-tardia-legislacao-brasileira/>. Acesso em: 17 de fev. 2017.

ANDRADE, Douglas Santos. **O Direito à privacidade e os valores da personalidade**. Disponível em: < https://www.maxwell.vrac.puc-rio.br/21185/21185.PDF>. Acesso em: 15 maio 2017.

ARAÚJO, Thiago. **Caso Fran-Jovem acusado de divulgar vídeo íntimo é julgado em Goiânia**. Disponível em: http://www.jornalopcao.com.br/ultimas-noticias/jovem-acusado-de-divulgar-video-intimo-e-julgado-em-goiania-17480/>. Acesso em: 07 de maio de 2017.

BARROS, Thiago. **Pornografia e racismo são os crimes mais denunciados na web**. Disponível em: <http: //http://www.techtudo.com.br/noticias/noticia/2014/02/pornografia-infantil-e-racimo-são-os-crimes-mais-denunciados-na-web.html>. Acesso em: 07 de maio de 2017.

BERETTA, Pedro. **Sem meios eficazes, Lei Carolina Dieckmann até atrapalha.** Disponível em: http://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha>. Acesso em: 17 de maio de 2017.

BRASIL, Portal. **Mulheres são o principal alvo da pornografia de vingança**.Disponível em: <http://www.brasil.gov.br/cidadania-e-justica/2016/11/mulheres-sao-principal-alvo-da-pornografia-de-vinganca>. Acesso em: 06 de maio de 2017.

BRASIL, Lei 9.296, de 24 de julho de1996. **Lei das interceptações telefônicas.** Disponível em: <http://www.planalto.gov.br>ccivil_03>leis>. Acesso em: 17 de fev. de 2017.

BRASIL, Lei 9.609 de 19 de fevereiro de 1998. **Lei que dispõe sobre a proteção da propriedade intelectual de programas de computador**. Disponível em: <http://www.planalto.gov.br>ccivil_03>leis>. Acesso em: 17 de fev. de 2017.

BRASIL, Scientific American. **A origem da computação**. Disponível em: http://www2.uol.com.br/sciam/reportagens/a_origem_da_computacao.html Acessado em: 26 de abril de 2017.

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

CANDIDO, Fabiano.**Em 2006, Justiça dá razão ao YouTube no caso Cicarelli**. Disponível em: http://exame.abril.com.br/tecnologia/justica-da-razao-ao-youtube-no-caso-cicarelli/>. Acesso em: 07 de maio 2017.

CASTRO, Luiz Augusto. **Texto ruim inviabiliza Lei Carolina Dieckmann, afirmam advogados**. Disponível em: <m.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=mobile&infoid=33404&sid=4>. Acesso em: 21 de maio de 2017.

CERQUEIRA, Tamiris. **Reflexão sobre o vídeo que viralizou na internet, onde a mulher é filmada entrando no motel com o melhor amigo do marido.** Disponível em: https://tamiriscerqueira.jusbrasil.com.br/artigos/268526022/analise-juridica-do-caso-fabiola>. Acesso em: 07 de maio de 2017.

COHEN, Marina. **Jornalista que teve fotos íntimas vazadas na web cria ONG para apoiar vítimas do problema**. Disponível em: https://oglobo.globo.com/sociedade/jornalista-que-teve-fotos-intimas-vazadas-na-web-cria-ong-para-apoiar-vitimas-do-problema-14722916>. Acesso em: 07 de maio de 2017.

CRESPO, Marcelo. **Revenge porn: a pornografia da vingança.** Disponível em: <https://marcelocrespo1.jusbrasil.com.br/artigos/153948423/revenge-porn-a-pornografia-da-vinganca>. Acesso em: 06 de maio de 2017.

GOMES, Fernanda Cunha. **A nova interpretação constitucional e o juízo de ponderação**. Revista Âmbito Jurídico Constitucional, Rio Grande. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=8783> Acesso em: 21 de março de 2017.

GRECO, Rogério. **Código Penal Comentado**. 6. ed. Rio de Janeiro: Impetus, 2012.

HIGA, Paulo. Tecnoblog. **Juiz manda tirar watsap do ar no Brasil**. Disponível em: https: //tecnoblog.net/174326/juiz-bloqueio-whatsapp-brasil/. Acesso em: 20 maio 2017.

LEONARDI, Marcel. **Tutela e Privacidade na Internet**. Saraiva, São Paulo; 2012.

MACHADO, ANDRÉ. **Especialistas explicam como computador de Carolina Dieckmann foi hackeado.** Disponível em: https://oglobo.globo.com/rio/especialistas-explicam-como-computador-de-carolina-dieckmann-foi-hackeado-4895771>. Acesso em: 09 de maio de 2017.

MAGESK, Laila; SOARES, Leonardo. **Pornografia de vingança: um crime que não para de crescer.** Disponível em: Acesso em: 06 de maio de 2017.

MASCARENHAS, Fabiana. Uol.**Racismo é o segundo crime mais denunciado na internet**. Disponível em: <http: //atarde.uol.com.br/bahia/noticias/racismo-e-o-segundo-crime-mais-denunciado-na-internet-161880>. Acesso em: 05 de maio de 2017.

MENDES(2012), Priscilla. G1 em Brasília. **Dieckmann foi chantageada em R$ 10 mil por fotos, diz advogado.** Disponível em: http://g1.globo.com/tecnologia/noticia/2012/05/dieckmann-foi-chantageada-em-r10-mil-devido-fotos-diz-advogado.html>.Acesso em: 09 de maio de 2017.

MIDIAMAX. **Jovem se suicida no interior do Piauí após vídeo íntimo vazar no WhatsApp.** Disponível em: http://www.midiamax.com.br/noticias/881838-jovem-se-suicida-no-interior-do-piaui-apos-video-intimo-vazar-no-whatsapp.html>. Acesso em: 07 de maio de 2017.

MULLER NICOLAS. **O começo da Internet no Brasil.** Oficina da Net. Disponível em: https://www.oficinadanet.com.br/artigo/904/o_comeco_da_internet_no_brasil> Acesso em: 26 de abril de 2017.

PAULO Vicente. ALEXANDRINO Marcelo. **Direito Constitucional Descomplicado,** 5 ed. Rio de Janeiro: Forense; São Paulo: Método 2010.

PERRIN Stephanie, **O cibercrime**. <http://vecam.org/archives/article660.html> Acesso em: 29 de março de 2017.

POZZEBOM, Rafaela. Oficinad a net.**Quais são os crimes virtuais mais comuns?** Disponível em: http://www.oficinadanet.com.br/post/14450-quais-os-crimes-virtuais-mais-comuns. Acesso em 05 de maio 2017.

Significado de AIDS. **O que é AIDS**, conceito, definição Disponível em: <https: //http://www.significados.com.br/aids/>. Acesso em: 03 de maio 2017.

SILVA, Leonardo Werner. Folha de São Paulo. **Internet foi criada em 1969 com o nome de "Arpanet" nos EUA. <** http://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml> Acesso em: 25 de abril de 2017.

SILVA, Remy Gama. **Crimes de Informática**. Disponível em: https://www.passeidireto.com/arquivo/22916425/crimes-da-informatica---remy-gama-silva. Acesso em: 1º de jun 2017.

Superior Tribunal de Justiça. **Justiça usa Código Penal para combater crime virtual**. Disponível em: https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual>. Acesso em: 17 de fev de 2017.

VARELLA, Gabriella e SOPRANA, Paula. Época. **Pornografia da vingança: crime rápido, trauma permanente**. Disponível em: <http://epoca.globo.com/vida/experiencias-digitais/noticia/2016/02/pornografia-de-vinganca-crime-rapido-trauma-permanentee.html>. Acesso em: 06 de maio de 2017.

VILAR Dalliana. MACÊDO Gills Lopes. **A Convenção de Budapeste e as Leis Brasileiras**. Disponível em: <http://www.charlieoscartango,com.br> Acesso em: 26 de abril de 2017.

WARREN, Samuel; BRANDEIS, Louis. **The right to privacy (O Direito à Privacidade) 1890.** Disponível em:http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em 07

(Fonte: https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann, https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann/2, data de acesso: 15/09/2020)

6A. CONCEITOS

A - Sigilo profissional
B – Ética
C- Liberdade de Expressão
D – Desinformação
E – Espionagem Industrial

1 A- Significado de Sigilo

O que é Sigilo:

Sigilo é a **condição de algo que é mantido como oculto e secreto**, fazendo com que poucas pessoas saibam da sua existência.

Quando uma pessoa pede sigilo sobre determinado assunto, está implícito que a informação não deve ser reproduzida para outras pessoas, mas sim reservada exclusivamente para aquela que a está recebendo.

Exemplo: "*Vou ser promovido, mas ainda é sigil*o".

Um **conteúdo sigiloso** é aquele que está sob regime de sigilo, devendo ser mantido em privacidade. Todas as pessoas têm direito ao sigilo pessoal, ou seja, de não cederem informações indesejadas sobre as suas vidas privadas.

Alguns dos principais **sinônimos de sigilo** são: segredo, silêncio, privacidade, discrição e confidência.

Sigilo profissional

Este é um comportamento previsto no **Código de Ética** de todas as profissões. Consiste na condição de manter o sigilo das informações cedidas pelo usuário / cliente ao profissional que o recepciou / atendeu.

Por exemplo, o sigilo profissional dos psicólogos garante que estes profissionais não forneçam dados pessoais ou fatos inerentes às vidas dos seus pacientes para terceiros.

O sigilo profissional também diz respeito ao comprometimento que o profissional deve ter para com a empresa que trabalha, evitando a divulgação de informações para companhias rivais que possam, de alguma forma, prejudicar a sua empresa.

Quando o profissional não segue estas regras, ocorre a chamada "quebra do sigilo profissional".

Saiba mais sobre o significado do Código de Ética e da Ética Profissional.

Sigilo bancário

O sigilo bancário garante que as instituições financeiras não divulguem os dados e informações de seus clientes.

No Brasil, a **Lei Complementar nº 105**, de 10 de janeiro de 2001, prevê a pena de até quatro anos para o infrator, caso haja a quebra do sigilo bancário sem autorização prévia das autoridades competentes (Ministério Público e Polícia Federal, por exemplo).

O pedido de **quebra do sigilo bancário** só pode ocorrer caso o indivíduo seja alvo de investigação criminal para a apuração de ocorrência de atos ilícitos, como contrabando, lavagem de dinheiro, terrorismo e etc.

(Fonte: https://www.significados.com.br/sigilo/, data de acesso: 15/09/2020)

6B. Ética

Significado de Ética Profissional

O que é Ética Profissional:

Ética profissional é o **conjunto de normas éticas que formam a consciência do profissional** e representam imperativos de sua conduta.

Ética é uma palavra de origem grega (*éthos*), que significa "propriedade do caráter".

Ser ético é agir dentro dos padrões convencionais, é proceder bem, é não prejudicar o próximo. Ser ético é cumprir os valores estabelecidos pela sociedade em que se vive.

O indivíduo que tem ética profissional cumpre com todas as atividades de sua profissão, seguindo os princípios determinados pela sociedade e pelo seu grupo de trabalho.

Cada profissão tem o seu próprio código de ética, que pode variar ligeiramente, graças a diferentes áreas de atuação.

No entanto, há elementos da ética profissional que são universais e por isso aplicáveis a qualquer atividade profissional, como a honestidade, responsabilidade, competência e etc.

Saiba mais sobre o significado de Ética.

Código de Ética Profissional

O Código de Ética Profissional é o conjunto de normas éticas, que **devem ser seguidas pelos profissionais no exercício de seu trabalho**.

Este código é elaborado pelos Conselhos, que representam e fiscalizam o exercício da profissão.

O código de ética médica, por exemplo, em seu texto descreve:

> **"*O presente código contém as normas éticas que devem ser seguidas pelos médicos no exercício da profissão, independentemente da função ou cargo que ocupem.***
>
> ***A fiscalização do cumprimento das normas estabelecidas neste código é atribuição dos Conselhos de Medicina, das Comissões de Ética, das autoridades de saúde e dos médicos em geral.***
>
> ***Os infratores do presente Código, sujeitar-se-ão às penas disciplinares previstas em lei*".**

(Fonte: https://www.significados.com.br/etica-profissional/#:~:text=%C3%89tica%20profissional%20%C3%A9%20o%20conjunto,%C3%A9%20n%C3%A3o%20prejudicar%20o%20pr%C3%B3ximo, data de acesso: 15/09/2020)

6C. LIBERDADE DE EXPRESSÃO

O QUE É LIBERDADE DE EXPRESSÃO:

Liberdade de expressão é um direito fundamental do homem que garante a **manifestação de opiniões, ideias e pensamentos** sem retaliação ou censura por parte de governos, orgãos privados ou públicos, ou outros indivíduos.

No Brasil, a liberdade de expressão é garantida pelo **artigo quinto da Constituição Federal.** Também é um direito estabelecido mundialmente pela Declaração Universal dos Direitos Humanos da ONU.

A doutrina jurídica entende a liberdade de expressão enquanto um direito que não pode ser vendido, renunciado, transmitido ou revogado.

O **limite da liberdade de expressão** está em ultrapassar os demais direitos fundamentais de outros indivíduos. Ao cometer preconceito ou proferir palavras racistas, por exemplo, não é liberdade de expressão, e sim um crime contra outra pessoa que tem os mesmos direitos assegurados e é considerada igual a todos aos demais perante a lei. Se a liberdade de expressão de um fere a liberdade do outro, então torna-se opressão.

A relação entre a **liberdade de expressão e a mídia** é marcada principalmente pela questão da censura. Entre os preceitos de um país democrático estão justamente a liberdade de expressão de seus cidadãos e a liberdade de imprensa. Se não há liberdade para opinar na mídia, seja por repressão de governos ou de grupos econômicos, não há um estado democrático de direito.

A **liberdade de expressão na internet** segue as mesmas regras da liberdade de expressão em qualquer veículo de comunicação, e o mesmo se aplica quando estamos

falando fora da mídia: seja em casa ou na rua. E deve manter as mesmas garantias e limites. Assim como não se fala palavras racistas por ser um crime, também não se usa a internet para promover o racismo ou a xenofobia.

A contribuição da internet para a liberdade de expressão é fundamental, pois democratiza a informação e abre novos canais de divulgação. Ela dá voz a inúmeras pessoas e grupos cujas posições ficariam de fora dos círculos de divulgação tradicionais, como a grande mídia e a publicidade.

Mas também a internet abre espaço para a disseminação de pensamentos opressores e antidemocráticos, sob o pretexto do anonimato e da proteção de se estar atrás da tela do computador, e não em um confronto real. Embora já existam leis contra isto, estão sendo desenvolvidas normas para regulamentar os crimes cometidos no ambiente virtual, como o cyberbullying.

(Fonte: https://www.significados.com.br/liberdade-de-expressao/, data de acesso: 15/09/2020)

6D. DESINFORMAÇÃO

Significado de Desinformação

Ação ou efeito de desinformar. Informação inverídica ou errada que é divulgada com o objetivo de induzir em erro. Falta de conhecimento; ignorância: a desinformação sobre métodos contraceptivos é perigosa. Etimologia (origem da palavra ***desinformação***).

Desinformar + ção.

Sinônimos de Desinformação

Desinformação é sinônimo de: desconhecimento, ignorância

https://www.dicio.com.br/desinformacao/

DESINFORMAÇÃO

Origem: Wikipédia, a enciclopédia livre.
Saltar para a navegaçãoSaltar para a pesquisa

Desinformação é a utilização das técnicas de comunicação e informação para induzir a erro ou dar uma falsa imagem da realidade, mediante a supressão ou ocultação de informações, minimização da sua importância ou modificação do seu sentido.[1] Tem como objetivo influenciar a opinião pública de maneira a proteger interesses privados.

Algumas vezes, a palavra é empregada no contexto de relações públicas ou da propaganda.

A desinformação pode operar através da publicidade pública de um regime político, geralmente organizada por um *spin doctor* por meio de mecanismos da engenharia social, ou da publicidade privada ou, ainda, por meio de boatos, "sondagens", estatísticas, filtragem de informações ou estudos supostamente científicos e imparciais, mas pagos por empresas ou instituições económicas interessadas, por afirmações não autorizadas para inspecionar os argumentos adversos que possam suscitar uma medida e antecipar respostas e uso de meios não independentes ou financiados em parte por quem divulga a notícia ou com jornalistas sem contrato fixo.

A desinformação serve-se de diversos procedimentos retóricos como a demonização, o esoterismo, a pressuposição, o uso de falácias, mentiras, omissão, sobreinformação, descontextualização, negativismo, generalização, especificação, analogia, metáfora, eufemismo, desorganização do conteúdo, uso de adjetivo dissuasivo, reserva da última palavra ou ordenação da informação preconizada sobre a oposta (ordem nestoriana).

A demonização ou satanização consiste em identificar a opinião contrária com o mal, de forma a que a própria opinião fique enobrecida ou glorificada. Falar do vizinho como de um demónio converte-nos em anjos e as "guerras santas" sempre serão menos injustas que as outras guerras. Trata-se antes de mais de convencer as pessoas com sentimentos e não com razões objectivas. Habitualmente emprega-se em defesa de interesses económicos, ou, por exemplo, quando se demoniza a Internet chamando-lhe refúgio de pederastas e piratas, encobrindo a intenção económica a que obedece esse ponto de vista aparentemente bem-intencionado de a regular.

Algumas palavras e expressões não admitem réplica nem razoabilidade lógica: são os chamados **adjetivos dissuasivos,** contundentes e negativistas que obrigam a submeter-se a essas palavras e excluem o teor e qualquer forma de trâmite inteligente. A sua contundência emocional, o pathos emotivo da mensagem, eclipsa toda qualquer possível dúvida ou ignorância, os princípios de qualquer forma razoável de pensamento: a constituição ou a integração europeia é *irreversível*.

A mesma aplicação têm os adjetivos *inquestionável, inquebrável, inexequível, insuspeitável, indeclinável* e *substancial.* O seu maximalismo serve para rebaixar qualquer discurso no sentido oposto e criar uma atmosfera irrespirável de monologia. Segundo Noam Chomsky, muitas destas palavras costuma atrair outros elementos em cadeia formando lexias: *adesão inquebrável*, *dever incontornável*, *legítimas aspirações*, *absolutamente imprescindível*. Ou com lexias redundantes como *totalmente cheio* ou *absolutamente indiscutível, inaceitável* ou *inadmissível.*

Retórica da desinformação

- **Apelo ao medo** - Um público que tenha medo está em situação de receptividade passiva e admite mais facilmente qualquer tipo de indoutrinação ou a ideia que se lhe

quer incutir; recorre-se a sentimentos instalados na psicologia do cidadão por preconceitos escolares e de educação, mas sem razões nem provas.

- **Apelo à autoridade** - Citar personalidades importantes para sustentar uma ideia, um argumento ou uma linha de conduta e negligenciar outras opiniões.
- **Testemunho** - Mencionar dentro ou fora de contexto casos particulares em vez de situações gerais para sustentar uma opção política.
- **Efeito acumulativo** - Persuasão do auditório para adoptar uma ideia insinuando que um movimento de massas irresistível e implacável está já comprometido no seu apoio, embora tal seja falso.
- **Redefinição e revisionismo** - Consiste em redefinir as palavras ou falsificar a história de forma parcial para criar uma ilusão de coerência.
- **Procura de desaprovação** ou **pôr palavras na boca de alguém** - Relacionada com o anterior, consiste em sugerir ou apresentar uma ideia ou acção que seja adoptada por um grupo adverso sem a estudar verdadeiramente. Afirmar que um grupo tem uma opinião e que os indivíduos indesejáveis, subversivos ou reprováveis a têm também. Isto predispõe os demais a mudar a sua opinião.
- **Uso de generalidades e palavras virtuosas** - As generalidades podem provocar emoção intensa no auditório. O amor à pátria e o desejo de paz, de liberdade, de glória, de justiça, de honra e de pureza permitem assassinar o espírito crítico do auditório, pois o significado destas palavras varia segundo a interpretação de cada indivíduo, mas o seu significado conotativo general é positivo e por associação os conceitos e os programas do propagandista serão percebidos como grandiosos, bons, desejáveis e virtuosos.
- **Imprecisão intencional** - Referir factos deformando-os ou citar estatísticas sem indicar as fontes ou todos os dados. A intenção é dar ao discurso um conteúdo de aparência científica sem permitir analisar a sua validade ou a sua aplicabilidade.
- **Transferência** - Esta técnica serve para projectar qualidades positivas ou negativas de uma pessoa, entidade, objecto ou valor (indivíduo, grupo, organização, nação, raça, etc.) sobre algo para fazer isto mais (ou menos) aceitável mediante cargas emotivas.
- **Simplificação exagerada** - Generalidades usadas para contextualizar problemas sociais, políticos, económicos ou militares complexos.
- **Quidam** - Para ganhar a confiança do auditório, o propagandista emprega o nível de linguagem e as maneiras e aparências de uma pessoa comum. Pelo mecanismo psicológico de projecção, o auditório encontra-se mais inclinado a aceitar as ideias que se apresentam deste modo, já que quem as presenta parece-lhe semelhante.
- **Estereotipagem** ou **etiquetagem** Esta técnica utiliza os preconceitos e os estereótipos do auditório para conseguir a adesão a algo.
- **Bode expiatório** - Lançando anátemas de demonização sobre um indivíduo ou um grupo de indivíduos, acusado de ser responsável por um problema real ou suposto, o propagandista pode evitar falar dos verdadeiros responsáveis e aprofundar o problema.

- **Uso de chavões (slogans)** - Frases breves e curtas, fáceis de memorizar e reconhecer e que permitem deixar um traço em todos os espíritos, de forma positiva, ou de forma irónica: "*Bruto é um homem honrado*", por exemplo.
- **Eufemismo** ou **deslize semântico** - Substituição de uma expressão por outra retirando-lhe todo o conteúdo emocional e esvaziá-la do seu sentido: "*interrupção voluntária da gravidez*" em vez de aborto induzido, "*solução habitacional*" em vez de habitação, "*limpeza étnica*" por matança racista. Outros exemplos, "*danos colaterais*" em vez de vítimas civis, "*liberalismo*" em vez de capitalismo, "*lei da selva*" em vez de liberalismo, "*reajuste laboral*" em vez de despedimento, "*solidaridade*" em vez de imposto, "*pessoas com preferências sexuais diferentes*" em lugar de homossexuais, "*pessoas com capacidades diferentes*" em lugar de deficientes e "*relações impróprias*" em vez de adultério.
- **Adulação** - Uso de qualificativos agradáveis, por vezes sem moderação, com a intenção de convencer o receptor: "Você é muito inteligente, deveria estar de acordo com o que lhe digo".

(Fonte: https://pt.wikipedia.org/wiki/Desinforma%C3%A7%C3%A3o, data de acesso: 15/09/2020)