CLAUDIO JOEL BRITO LÓSSIO

MANUAL *DESCOMPLICADO* DE DIREITO DIGITAL

Guia para Profissionais do Direito e da Tecnologia

3ª edição
revista, atualizada
e ampliada

2022

EDITORA JusPODIVM
www.editorajuspodivm.com.br

4. OS PROTAGONISTAS DA SOCIEDADE DIGITAL

Neste tópico serão apresentados os protagonistas presentes diante da relação do Direito e da Tecnologia da Informação, seja o causador, a pessoa que sofre, o profissional que poderá proteger preventivamente ou de forma repressiva. O primeiro a ser apresentado, será o protagonista mais fraco de todo o meio, pois, normalmente, não está pronto quando se fala em proteção no ambiente cibernético.

4.1. USUÁRIO/UTILIZADORES

O termo usuário é denominado como a pessoa que opera o computador ou *smartphone* com conexão com a *internet* ou não. O usuário é, normalmente, o elo mais fraco diante dos que causam e os que protegem o ambiente digital. Eis a necessidade de esse usuário se capacitar cada vez mais para minimizar o risco para si e para a organização que trabalha.

A imprudência e a imperícia deste usuário fazem com que crimes ocorram no ambiente digital frequentemente, tendo seus direitos violados como, por exemplo, ao ter o seu computador invadido, visto que há tipificação penal para tal

fato, previsto no Código Penal Brasileiro, em seu Artigo 154-A[1]. Ou esse mesmo usuário violando direitos de outra pessoa, quando, por exemplo, abrir e ler o *e-mail* indevidamente, sem autorização de seu proprietário titular, caindo assim no tipo penal de violação de correspondência, previsto no Artigo 151 do Código Penal Brasileiro[2].

1. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940.** Código Penal Brasileiro. Artigo 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". Disponível em: <http://www2. camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro- 1940-412868-normaatualizada-pe.doc>. Acesso em: 27 dez. 2017.
2. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940**. Código Penal Brasileiro. Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem: Pena - detenção, de um a seis meses, ou multa. Ibidem.

Para o Direito, o usuário é uma pessoa com personalidade jurídica, mas nem sempre com capacidade plena, visto que crianças e adolescentes têm acesso a computadores e *smartphones*, sendo que, normalmente, esse acesso é permitido de forma negligente pelos seus responsáveis. Muitos desses responsáveis, ou melhor, irresponsáveis, na maioria das vezes, não estão preparados, ou melhor, habilitados, para usufruírem do ambiente digital da *internet*, pois acreditam que não precisam de medida de segurança alguma, acreditando que podem falar o que querem, por exemplo, achando que o ambiente digital é local sem lei.[3]

No Brasil, esse descuido em relação a prevenção no ciberespaço é praticamente cultural, fazendo com que o usuário só venha buscar a correção quando algum delito no meio digital acontece com ele.

Cabe perceber que inclusive quando o fato é a falta de cuidado com as crianças e os adolescentes no ambiente digital, assim também como idosos, ou qualquer outra pessoa que necessite de auxílio, pode ocorrer o abandono digital.

No meio cibernético dá para perceber que o elo mais fraco entre os protagonistas apresentados é um: "o Usuário". E esse usuário deverá buscar meios de se habilitar para o ambiente cibernético, fazendo cursos de educação digital, obedecendo a faixa etária imposta pelos contratos eletrônicos como, por exemplo, os das redes sociais, e buscando ter a certeza de que a *internet* não é um ambiente sem lei, mas sim um local onde a prova de uma atitude é muito forte, então só escreva algo que realmente tenha orgulho de difundir.

3. PINHEIRO, Patricia. **Direito Digital.** Op. Cit. 67.

Desde o início da popularização do computador e, principalmente, a partir da união deste com a *internet*, as infrações e fraudes jurídicas no ambiente digital crescem a cada segundo diante da facilidade que os cibercriminosos têm, como também pelo descuido dos usuários que não buscam nenhuma medida de proteção ao se conectar à grande rede.

Esse fato ascende no mundo a luta pela privacidade e à proteção de dados pessoais.

4.2. O *HACKER* VS. O CIBERCRIMINOSO

São dois os elementos essenciais para que a tecnologia se desenvolva: *hacker* e o cibercriminoso. Se existissem exclusivamente os *hackers*, que são os "mocinhos" não ocorreriam os crimes digitais próprios/puros causados pelos cibercriminosos, logo, os primeiros citados acabariam por se acomodar.

Hacker e cibercriminosos são elementos essenciais a serem apresentados quando se fala em *Cybersecurity*, Cibersegurança ou Cibercrime, visto que, em ambos os casos, é comum a presença deles, diretamente ou indiretamente. Diretamente quando, por exemplo, um cibercriminoso está fazendo um acesso ilegal a um computador, ou indiretamente quando um sistema está protegido devido a um *hacker* que estudou e corrigiu as vulnerabilidades do sistema.

São termos comuns, principalmente o termo *hacker*, visto que a maioria das pessoas o relacionam com invasão de computadores ou quando se imagina que algo de ruim ou ilícito acontece no ambiente digital.

Os *hackers,* também conhecidos como *White Hats,* são pessoas que têm uma inteligência acima da média e têm uma facilidade enorme de escrever códigos que funcionam e,

geralmente, são contratadas por empresas para descobrirem falhas de segurança, ou seja, são pessoas que trabalham com a informática, usando a sua inteligência e suas habilidades com esse universo[4].

O cibercriminoso, também conhecido como *cracker*, recebe essa nomenclatura por ser *Crime Hacker*, ou simplesmente por serem quebradores, traduzindo diretamente o termo do inglês. Quando se fala quebrador, é porque o *cracker* visa quebrar a segurança de algo. Os cibercriminosos, também conhecidos como *Black Hats*, são aqueles que também têm um conhecimento acima da média, mas o utilizam para se beneficiar de maneira ilícita, gerando delitos, que nem sempre estão relacionado com conhecimentos técnicos informáticos, podendo ter o poder da oratória para o convencimento de pessoas em ceder os dados pessoais. Em um exemplo bem corriqueiro de nossa realidade é quando milhões são roubados de contas bancárias, mas apenas um centavo por conta. Assim, o cibercriminoso tenta invadir o banco, e o *hacker* estuda e corrige possíveis pontos de vulnerabilidade para tentar impedir esta invasão[5].

Tanto os *hackers* quanto os cibercriminosos são pessoas consideradas com inteligência acima da média e com grande conhecimento na área das ciências da computação, sendo o que os diferencia exclusivamente a finalidade com que cada um usará sua principal ferramenta, o cérebro, pois o *hacker* busca o lado ético, a segurança, já o cibercriminoso busca o ilícito e/ou o crime no ambiente cibernético.

---

4. VANCIM, Adriano Roberto; MATIOLI, Jefferson Luiz. **Direito & Internet:** Contrato Eletrônico e Responsabilidade Civil na Web. 2. ed. Franca - SP: Lemos & Cruz, 2014, p. 167.
5. Idem. Ibidem.

O *hacker* de hoje é o profissional de segurança da informação, assim também denominado como *Hacker* Ético ou Engenheiro de Segurança da Informação/Informática, que no próximo subtópico receberão conceituação acerca da função exercida.

Percebam que cibercriminosos são especialistas em engenharia social, sendo que alguns não possuem o conhecimento em quebra de sistemas digitais, mas possuem uma grande habilidade de fala e criatividade em criar cenários que possibilite enganar pessoas para conseguir o que desejam, como por exemplo, os dados, eis o fato que justifica a evolução do tipo penal estelionato diante das fraudes eletrônicas, acrescido pela Lei 14.155 de 2021.

4.3. ENGENHEIRO DE SEGURANÇA INFORMÁTICA

O *hacker* de antigamente, hoje está mais bem denominado: *Hacker* Ético, *Ethical Hacker* ou profissional de segurança da informação, atualmente habilitado diante de uma formação em engenharia de segurança informática, certificações ou trabalho prático na área.

Segundo Vallim[6], na palestra "Hacker vs Cyber Crime", *Ethical Hacker* é o nome adotado para o *Hacker* ético e, conforme subtópico anterior, é a denominação das pessoas consideradas com inteligência acima da média e com grande conhecimento na área digital, sendo que o que os diferencia é

6. VALLIM, Adriano Penedo de Attheyde. **Hackers vs Cyber Crime**. *In* Universidade Nove de Julho, São Paulo, 2017. Disponível em: <https://www.youtube.com/watch?v=Ez0q1Oa_Y34&feature=youtu.be>. Acesso em: 19 abr. 2017.

exclusivamente a finalidade com que cada um usará sua principal ferramenta, o cérebro, pois o *hacker* busca o lado ético, a segurança digital. Quando esses atuam profissionalmente ou possuem título acadêmico específico, são denominados engenheiros de segurança informática.

O Engenheiro de Segurança Informática pode ser conhecido pelo termo *Ethical Hacker*. Normalmente adquire esse título por meio da aquisição de certificações através das quais se inserirá na área de segurança da informação em que irá atuar. O profissional de segurança da informação, normalmente, é uma pessoa que concluiu cursos de graduação na seara da tecnologia ou terminou outros cursos, mas acabou se especializando através de uma pós-graduação buscando o viés da tecnologia, assim como sua segurança.

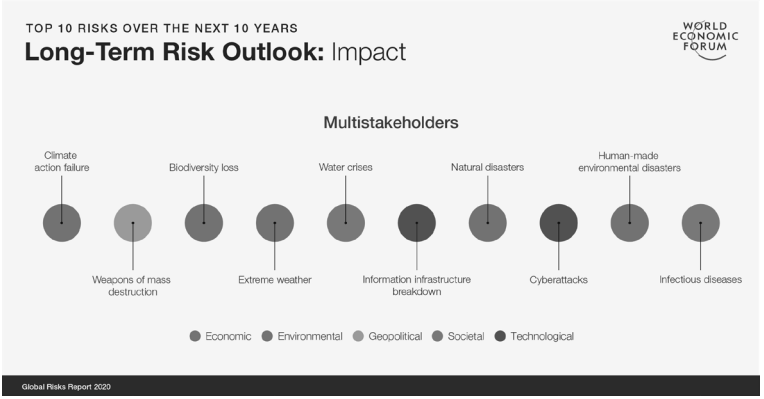
A prevenção é o principal remédio diante das violações causadas pelos ciberataques, visto que assim se promoverá a maior proteção possível em busca da manutenção da inviolabilidade dos arquivos particulares seja de uma pessoa ou de uma empresa. E, assim como o profissional da segurança da informação, poderá promover o máximo de proteção. É comum este possuir em sua equipe um advogado para promover auxílio jurídico diante da melhor instrumentalização contratual em âmbito legal.

Segundo o Fórum Global Risk 2020[7], os riscos de ciberataques, quebras de infraestrutura de informação ou fraudes envolvendo dinheiro e dados estão presentes nas probabilidades e nos impactos. Ainda existem atentados terroristas voltados

7. WELIVESECURITY. **World Economist Forum. The Global Risks Perception Survey 2020**. Disponível em: <http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf. Acesso em: 22 jan. 2021.

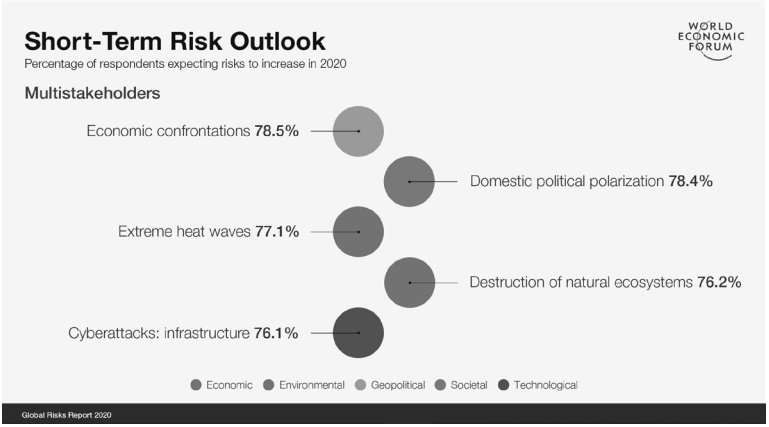
para a seara dos ataques cibernéticos, que podem provocar por meio digital a parada de estruturas físicas como hospitais, instituições financeiras, impactando a ordem e a paz pública. Pode ser conferido na imagem a seguir:

Figura 1.1 - The Global Risks Perception Survey 2020. Impacto a Longo Prazo



Fonte: <http://www3.weforum.org/docs/. WEF_Global_Risk_Report_2020.pdf>. Acesso em: 12 jan. 2021.

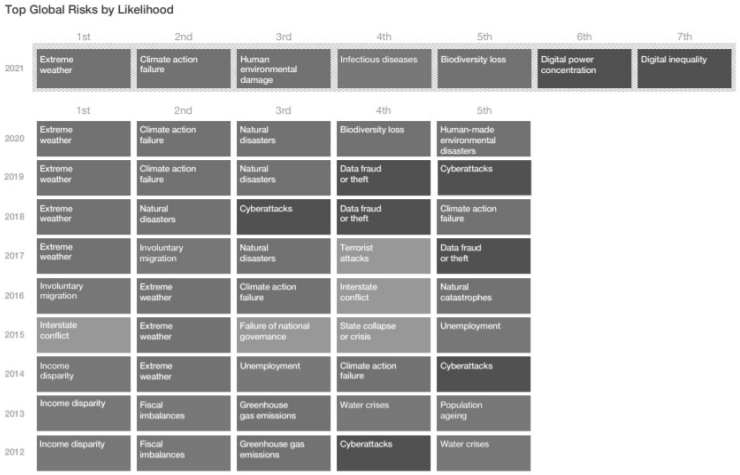
Figura 1.2 - The Global Risks Perception Survey 2020. Risco a Curto Prazo



Fonte: <http://www3.weforum.org/docs/. WEF_Global_Risk_Report_2020.pdf>. Acesso em: 12 jan. 2021.

Já ao visualizar o comparativo dos últimos anos, incluindo o ano de 2021, pode ser observado uma evolução na quantidade de institutos que estão direcionados às tecnologias da informação e comunicação e, ainda assim, também se observam outras que estão relacionadas com o novo modelo social, o digital.

Figura 2 - The Global Risks Perception Survey 2021.[8] Probabilidade[9]



Fonte: <http://www3.weforum.org/docs/. WEF_Global_Risk_Report_2020.pdf>. Acesso em: 12 jan. 2021.

É percebida a evolução iniciando pela evidência dos ciberataques em 2012, fraudes envolvendo dados como a coleta indevida e, em 2021, a grande preocupação envolve o poder digital da concentração de dados e a desigualdade digital.

O poder digital da concentração de dados deve ser a nova preocupação das pessoas e organizações públicas ou privadas, pois dado é poder, e, concentrado, o poder é imensurável. Um governo que coleta de maneira desenfreada todos os tipos de

8. WELIVESECURITY. **World Economist Forum. The Global Risks Perception Survey 2020**. Ibidem.
9. WELIVESECURITY. **World Economist Forum. The Global Risks Perception Survey 2020**. Disponível em: <http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf>. Acesso em: 22 mar. 2021.

dados de seu povo está minimizando cada vez mais os direitos, garantias e liberdades individuais.

A vigilância digital massiva e permanente pode estar não só nas mãos de governos que concentram dados, mas nas *big-techs* que tratam dados de seus usuários, assim os conhecendo melhor que eles próprios.

Uma pergunta: você já pensou em algo e de repente apareceu uma oferta exatamente com o que você imaginou em pesquisar? Esses algoritmos de sentimentos podem ajudar pessoas, mas também podem ser uma ferramenta de discriminação e segregação.

Já ao falar de desigualdade digital, não pode deixar evidente o que o processo de transformação digital causa, principalmente pela necessidade do trabalho em *home office*, educação a distância e socialização, por exemplo.

Veja a seguinte situação: uma empresa que só contrata novos colaboradores que possuam computador, *smartphone* e *internet* pessoal para serem utilizados no trabalho em *home office*. Nem todos possuem tais recursos. Assim, já são automaticamente desclassificados.

Na educação a distância ficou clara a desigualdade provocada pela necessidade de distanciamento social, fazendo com que pessoas devessem estar em casa. Nem todas as pessoas têm recursos tecnológicos disponíveis para assistir às aulas, por várias vezes sequer tinham a alimentação que presencialmente era ofertada na escola.

O que poderia ter sido feito em busca de minimizar esse processo de desigualdade digital na educação seria a distribuição massiva de dispositivo, *internet* e alimentação para essas

pessoas que estudam em instituições públicas ou que possuem financiamento estudantil ou bolsa.

Então, nesse caso, seria necessário não só o engenheiro de segurança informática, mas uma equipe multidisciplinar para compreender esse processo de implementação digital na sociedade, pois, é claro, não há desenvolvimento sem segurança, principalmente informática.

O engenheiro de segurança informática é o profissional com formação acadêmica ou com trabalho prático na área de segurança que trabalhará para que a segurança seja promovida em um ambiente de trabalho.

É comum que esse tipo de engenheiro conheça as amplitudes da segurança ofensiva, forense digital, entre outras práticas que promovam a segurança preventiva e repressiva diante de possíveis ataques informáticos, não podendo limitar-se à tecnologia da informação, assim possuindo o dever de conhecer o Direito, para não provocar acessos ilegítimos ou invalidação na preservação de provas, por exemplo. Já assistiu *Mr. Robot*? Perceberam quem são os engenheiros de segurança informática e a importância deles em uma gestão de crise?

4.4. ADVOGADO ESPECIALISTA EM DIREITO DIGITAL

O advogado é um operador do direito que, para se tornar tal profissional, necessita, primeiramente, concluir um curso de graduação em Direito e, logo após a conclusão, se submeter ao Exame da Ordem dos Advogados do Brasil – OAB para, assim, ter o seu conhecimento avaliado. Após aprovado na OAB, esse bacharel em Direito poderá efetuar o seu pedido de inscrição e, em seguida, receberá o seu número de inscrição na OAB, especificando o estado que assim fez o procedimento.

Além dos pré-requisitos acima citados, existem alguns que são de supra necessidade, pois estão elencados no Artigo 8º[10] disposto no Estatuto da Advocacia e da Ordem dos Advogados do Brasil como de imperiosa importância para se conseguir a inscrição, visto que, sem tal número, continuará sendo um bacharel em Direito e não um advogado.

Certo, apresentamos como se tornar um advogado, agora cabe demonstrar como se tornar um especialista em Direito Digital. Para fazer qualquer tipo de pós-graduação é necessário ter concluído o curso de graduação. Assim, a pós-graduação em Direito Digital que gera o título de especialista é *lato sensu.*

Para se tornar um advogado especialista em Direito Digital é necessário ter concluído o curso graduação em Direito, concluir uma pós-graduação em Direito Digital e, ainda, possuir o número de sua inscrição na OAB.

10. **Lei 8.906, de 4 de julho de 1994**. Artigo 8º "Para inscrição como advogado é necessário: I - capacidade civil; II - diploma ou certidão de graduação em direito, obtido em instituição de ensino oficialmente autorizada e credenciada; III - título de eleitor e quitação do serviço militar, se brasileiro; IV - aprovação em Exame de Ordem; V - não exercer atividade incompatível com a advocacia; VI - idoneidade moral; VII - prestar compromisso perante o conselho. § 1º O Exame da Ordem é regulamentado em provimento do Conselho Federal da OAB. § 2º O estrangeiro ou brasileiro, quando não graduado em direito no Brasil, deve fazer prova do título de graduação, obtido em instituição estrangeira, devidamente revalidado, além de atender aos demais requisitos previstos neste artigo. § 3º A inidoneidade moral, suscitada por qualquer pessoa, deve ser declarada mediante decisão que obtenha no mínimo dois terços dos votos de todos os membros do conselho competente, em procedimento que observe os termos do processo disciplinar. § 4º Não atende ao requisito de idoneidade moral aquele que tiver sido condenado por crime infamante, salvo reabilitação judicial". Estatuto da Advocacia e da Ordem dos Advogados do Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8906.htm>. Acesso em: 30 mar. 2018.

Mas o que significa ser um advogado com especialização em Direito Digital? Esse é o profissional que tratará do Direito diante das relações computacionais e/ou tecnológicas, tendo uma visão social da sociedade no ambiente digital, independentemente da seara, seja no âmbito penal, cível, tributário, consumidor ou trabalhista, por exemplo. Ele deve estar analisando sempre as inovações e os problemas cernes que estas novas tecnologias causarão diante das novas relações proporcionadas entre o direito e a informática.[11]

Cabe perceber que o advogado, para entrar nessa área Digital, não basta querer, mas também deverá possuir amor à tecnologia, ser inicialmente um entusiasta da informática, e buscar mergulhar dentro deste ambiente tecnológico de forma crescente e tão profunda que não se consiga mais perceber se é um advogado ou um profissional da informática e, em consequência dessa união, promoverá uma maior segurança jurídica voltada ao âmbito da segurança da informação.

Deve ser lembrado que a privacidade e a proteção de dados são algo cada vez mais necessário, seja em organizações públicas ou privadas, para efetuar a análise legal das documentações, como para os titulares de dados pessoais, como os clientes e colaboradores, em demandas judiciais para reparação em face de alguma pessoa física ou jurídica que esteja em desconformidade com o tratamento de dados pessoais.

11. PINHEIRO, Patrícia Peck. **Em vídeo, Patrícia Peck Pinheiro fala sobre os 10 anos do escritório**. São Paulo, 2017. Disponível em: <http://pppadvogados.com.br/profissionais/patricia-peck-pinheiro/em-video-patricia-peck-pinheiro-fala-sobre-10-anos-do-escritorio>. Acesso em: 30 mar. 2018.