

# **Direito Digital: o que é, oportunidades e como ser um advogado especialista em Direito e Tecnologia? (2021)**

Atualmente, a sociedade está inserida em um contexto cada vez mais digital, sendo notório o impacto da tecnologia em todas as áreas. O Direito tem passado por inúmeras transformações nos últimos tempos, sendo que o Direito Digital é um desdobramento desse novo cenário.

Assim, o Direito Digital é uma releitura dos demais ramos do Direito e visa tutelar as relações que ocorrem no ambiente virtual. Cumpre ressaltar que há um verdadeiro diálogo de fontes com os outros ramos do Direito, principalmente o Civil e o Penal.

Diversas situações contribuem para o desenvolvimento do Direito Digital. Até 2022, haverá 18 milhões de dispositivos IoT (*Internet of Things*), o que representa um aumento massivo de situações, seja para regularizar, proteger ou reduzir os riscos existentes (MARKETSANDMARKETS). Também, o emprego de algoritmos e o uso da Inteligência Artificial (IA) impulsionam cada vez mais a sociedade. Recentemente, uma pesquisa do MIT *Technology Review Insights* (2020) com 301 líderes de negócios e tecnologia, verificou que 38% relataram que seus planos de investimento em IA permaneceram inalterados como resultado da pandemia do Covid-19 e 32% indicaram que a crise acelerou seus planos.

Essas situações representam um crescimento exponencial do volume de dados no mundo, o que influencia na maneira como os dados podem ser usados, isto é, na criação de padrões comportamentais, auxílio na tomada de decisões, identificação

de riscos, entre outras formas.

Por isso, o advogado especialista em direito digital nunca foi tão essencial atuando não só no contencioso em questões envolvendo direito civil, contratos, tributário, consumidor, mas, também, no consultivo e *compliance* em apoio e negócios digitais e startups.

Vale destacar que o Direito Digital não envolve somente os crimes cibernéticos, mas se relaciona com todas as demais áreas do direito, a medida em que a sociedade está cada vez mais informacional. Além disso, a sua atuação envolve a conscientização para os riscos existentes no ambiente virtual, contribuindo para a construção de uma sociedade mais segura e na preservação dos direitos fundamentais.

## **PRINCIPAIS NORMAS APLICADAS AO DIREITO DIGITAL**

Dentre as inúmeras leis existentes no Brasil, há algumas que estão relacionadas à tecnologia, sendo que o advogado especialista em Direito Digital deve conhecê-las profundamente. São elas:

- a Lei de Acesso à Informação (Lei nº 12.527/2011),
- a Lei Carolina Dieckmann ou de crimes informáticos (Lei nº 12.737/2012),
- o Marco Civil da Internet (Lei nº 12.965/2014),
- o Decreto nº 8.771/16, que regulamentou alguns aspectos do Marco Civil,
- a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), e
- o Decreto nº 9.854/2019, que institui o Plano Nacional de Internet das Coisas.

Além disso, os advogados especialistas em Direito Digital

precisam conhecer as demais normas que estão relacionadas ao caso concreto, como o Código Civil, Código Penal, Código Tributário, além dos conhecimentos gerais, visto que o Direito Digital estabelece conexões com outros ramos do Direito.

## **ÁREAS DE ATUAÇÃO PROMISSORAS NO DIREITO DIGITAL**

O Advogado especialista em Direito Digital poderá atuar na área consultiva e contenciosa. Em inúmeros casos trabalhará com aportes de outros ramos do Direito, com o viés tecnológico, em outros, no entanto, trabalhará com fontes próprias do Direito Digital. Apesar de haver diversas áreas de atuação, serão mencionadas, a seguir, as principais áreas promissoras.

### **Crimes digitais ou Crimes Cibernéticos**

A prática de crimes no ambiente virtual foi um dos principais motivos que impulsionou o Direito Digital, em razão da necessidade de produzir provas válidas e penalizar condutas praticadas nesse contexto.

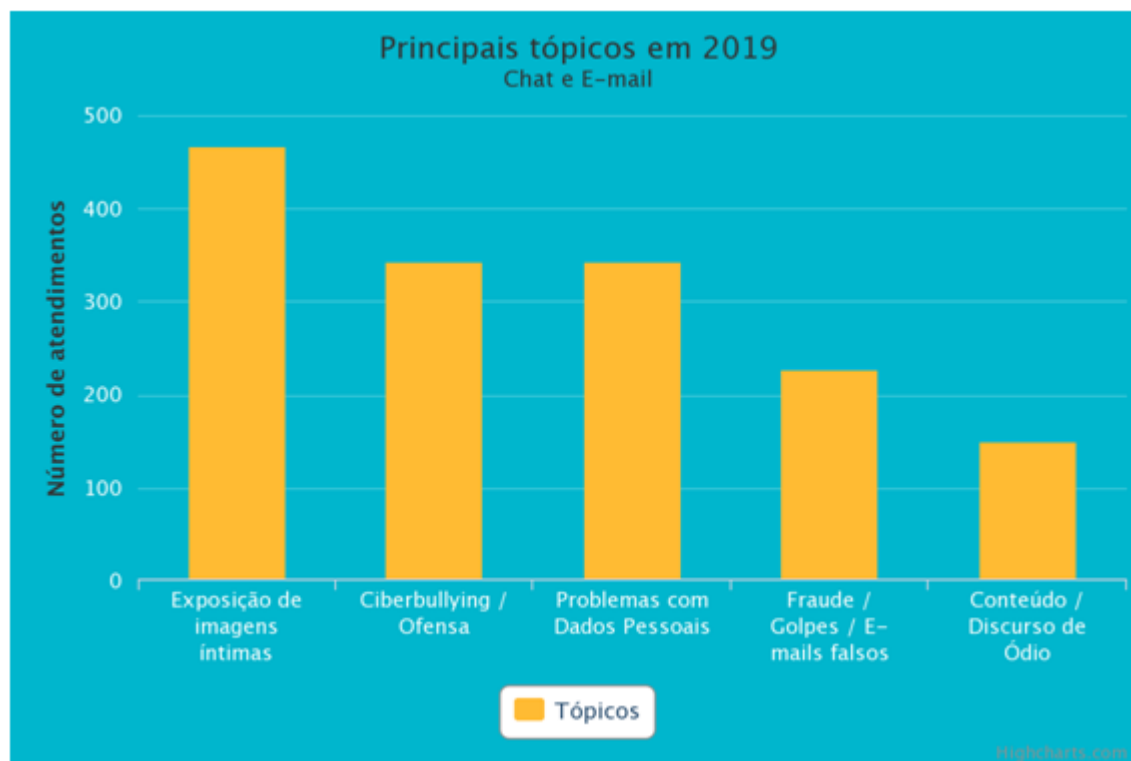
O Brasil é um dos principais países no mundo em número de crimes cibernéticos, sendo as perdas de 10 bilhões de dólares por ano, segundo McAfee, sendo que a maioria (54%) dos ataques tem origem no próprio país (MACHADO, 2018).

Em relação às leis aplicadas, a Lei Carolina Dieckmann ou de crimes informáticos (Lei nº 12.737/2012) representa uma importante lei para os crimes digitais, pois tornou crime a prática de invadir dispositivos eletrônicos a fim de obter, adulterar ou destruir dados de terceiros.

O Marco Civil da Internet (Lei nº 12.965/2014), no contexto dos crimes digitais, auxilia na identificação dos autores dos crimes, visto que regulamenta o dever de guardar e fornecer os registros de conexão e de acesso, além de disciplinar a responsabilidade civil dos provedores de acesso e aplicações.

O Estatuto da Criança do Adolescente – ECA (Lei nº 8.069/90) é uma norma que protege as vítimas com maior vulnerabilidade e prevê diversos crimes envolvendo o uso da tecnologia, como os artigos 240, 241, 241-A e 241-B.

A prática de crimes na Internet vem sendo cada vez mais comum. Os principais crimes em 2019, conforme o Datasaber (2019), são:



Verifica-se que continuam em alta os crimes contra honra, quais sejam, a calúnia, a injúria e a difamação, bem como os relacionados à intimidade sexual. Além disso, são comuns os crimes como *revenge porn*, que visam divulgar matérias íntimas com o fim de vingança, previsto no artigo 218-C, § 1º, e o compartilhamento não consentido previsto no art. 218, *caput*, ambos do Código Penal.

Igualmente, ameaças e extorsões são cada vez mais comuns, sobretudo com a onda *ransomware*, ataques que criptografam os discos e exigem resgates, muitas vezes em moeda digital (criptomoedas). Também, golpes por meio de técnica conhecida como SIM SWAP, que consiste no repasse pela operadora do

número de telefone do usuário para um novo chip, que está em posse de criminosos, possibilitando a invasão de aplicativos de trocas de mensagens, *internet banking* e o acesso a informações privadas.

Cumpramos ressaltar a importância do advogado especialista em Direito Digital ter conhecimento dos aspectos informáticos e de perícia forense, a fim de compreender a cadeia de custódia e a formação da prova informática, bem como conhecimentos relativos à remoção do conteúdo ilícito que se encontra em determinado site ou rede social.

Neste contexto, é quase consenso para os advogados especialistas em Direito Digital que as leis atuais são, em parte, suficientes para tutelar vítimas dos mais variados crimes cometidos através do computador ou outro dispositivo informático. Os maiores problemas são, muitas vezes, as investigações e a falta da cooperação dos provedores de aplicação, principalmente os estrangeiros, necessários à apuração da autoria.

O advogado especialista em Direito Digital deverá conhecer sobre Processo Penal e as condutas tipificadas como crimes no Código Penal e nas demais leis, além de conhecimentos técnicos sobre perícia digital, para obter êxito na sua atuação, seja na defesa das vítimas, ou daquelas que praticaram as condutas criminosas.

### **Proteção de dados pessoais**

Em razão da vigência da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a preocupação com a proteção de dados pessoais foi potencializada e a adequação à lei deixou de ser opcional e tornou-se prioridade.

Sabemos que o dado pessoal é considerado um bem importante, pois permite identificar diversas informações sobre os indivíduos, como comportamentos e desejos, e auxiliar na tomada de decisões.

A sociedade enfrenta vários desafios: aumento constante do volume de dados, a diversidade de formatos e fontes de dados, e a velocidade em que são produzidos e identificados. Por isso, a preocupação com a proteção de dados torna-se cada vez mais necessária e exige um olhar especial por parte dos advogados especialistas em Direito Digital que atuem com Privacidade de Proteção de Dados, sendo que essa atuação pode ocorrer tanto no setor privado, como no setor público.

Dentro do cenário da implementação da LGPD, o advogado especialista em Direito Digital pode realizar consultorias voltada à implementação da lei, auxiliando diretamente no processo de adequação, ou apenas na identificação das bases legais que permitem o tratamento dos dados em determinada situação.

Além disso, poderá atuar na redação e revisão de documentos essenciais ao processo de adequação, como Políticas de Privacidades e Termos de Uso, Relatório de Impacto à Proteção de Dados (RIPD), Processo de Respostas à Incidentes, bem como na revisão de contratos e acordos de processamento de dados elaborados entre as empresas.

Vale ressaltar, também, a possibilidade de atuar em favor dos titulares dos dados pessoais, representando-os, seja perante os agentes de tratamento, a ANPD ou Poder Judiciário.

Dessa forma, poderão solicitar informações aos agentes de tratamento sobre como é realizado o tratamento de dados; requer a correção de dados incompletos, inexatos ou desatualizados; a eliminação dos dados, dentre outras ações voltadas à observância dos seus direitos.

Em relação à representação perante a ANPD, o advogado especialista em Direito Digital pode formular petições para os titulares, após comprovada a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação, além de realizar reclamações sobre o

tratamento de dados pessoais em desconformidade com a LGPD.

Em situações graves, como nos vazamentos de dados, poderá buscar o Poder Judiciário para buscar a reparação pelos danos causados, que inclusive pode ser exercido coletivamente em juízo, nos termos do art. 42, § 3º, da LGPD.

Assim, como todas as áreas necessitam adequar-se à LGPD, o advogado especialista em Direito Digital deve estar preparado para atender às demandas, realizando consultorias e auxiliando nos processos de implementação, bem como atuando no assessoramento de empresas e agentes de tratamento no relacionamento com titulares de dados e Autoridade Nacional de Proteção de Dados (ANPD).

## **Inteligência Artificial**

Uma das principais transformações em razão do avanço tecnológico é o desenvolvimento da Inteligência Artificial, que pode ser verificada em todas as áreas da sociedade.

A Inteligência Artificial insere-se dentro de um conjunto de tecnologias que integram a chamada Quarta Revolução Industrial, expressão trazida por Klaus Schwab no seu livro “A Quarta Revolução Industrial”, publicado em 2016.

O conceito de Inteligência Artificial é: a capacidade de um software se aprimorarem sem precisar ser explicitamente programado para isso. Isso ocorre através da aplicação de modelos de aprendizado de máquina, por meio de uma nuvem, que envolve: análise de imagens, vídeos e textos, reconhecimento da fala e tradução para outros idiomas, conforme o Guia sobre análise de dados e aprendizado de máquina para CIO (2017).

Em parceria com a empresa de pesquisa M-Brain, o Google Cloud entrevistou, em 2017, 20 líderes empresariais e de TI que implementaram projetos de aprendizado de máquina sobre as principais vantagens provenientes dos projetos. Os principais benefícios são: economia de tempo, redução dos custos, melhor

gerenciamento de risco, melhor qualidade das análises, aumento de receita (M-BRAIN, 2017).

Nesse cenário, já existem carros que dirigem sozinhos (*self driving car*), como o da Tesla (2019). Apesar de terem potencial para melhorar a segurança pública, diversas questões éticas, jurídicas e técnicas precisam ser debatidas, considerando os pedestres e situações de tráfego, tais como: se um carro autônomo sofrer um acidente, quem será responsável: o fabricante do carro, o designer do *software* ou o motorista?

Além disso, há a situação que a I.A. pode criar música (GONZAGA; FERNANDES, 2019). Em relação ao direito à propriedade intelectual sobre essa obra criada, surgem indagações como: o dono da produção artística seria o *software*, seu desenvolvedor ou quem o possui?

Existem, também, os robôs relacionados às profissões como os cuidadores que envolvem uma tecnologia de assistência e reabilitação para idosos, tendo em vista o envelhecimento populacional (ALLISON, 2019).

Na área jurídica, em especial na advocacia, temos o primeiro robô-advogado, Ross, criado em 2016, que foi desenvolvido pela startup canadense, Ross Intelligence, que utiliza a plataforma Watson, da IBM. É capaz de ouvir a linguagem humana, rastrear mais de 10 mil páginas por segundo e formular respostas muito mais rápido do que qualquer profissional. Também, tem a capacidade de rastrear em tempo real os resultados de julgamentos para alertar os advogados sobre qualquer novidade que possa representar um risco ou uma ameaça aos clientes, bem como realizar a interpretação da jurisprudência a partir de casos armazenados em seu banco de dados (ÉPOCA, 2019).

No Poder Judiciário brasileiro, já existem diversos robôs sendo utilizados. Um deles é o Victor, que teve seu projeto



iniciado em dezembro de 2017 e é fruto da parceria do Supremo Tribunal Federal (STF) com a Universidade de Brasília (UnB). Em suma, as funções do robô Victor são: auxiliar na separação e na classificação das peças do processo judicial e identificar os principais temas de repercussão geral (STF, 2018).

Essas ferramentas deixam a seguinte dúvida: até que ponto algumas profissões serão necessárias?

Também existem ferramentas de Inteligência Artificial que são usados no Sistema Norte Americano, como o Compas (Propriedade intelectual NorthPoint inc.) que calculam os riscos que aquele indivíduo traz para a sociedade, com base no grau de periculosidade, podendo causar discriminação.

Além disso, o Google, em 2015, anunciou um novo sistema de armazenamento e organização de fotografias que prometia não limitar o espaço na nuvem para os consumidores. Contudo, um usuário percebeu que o programa etiquetava pessoas negras como gorilas, o que resultou numa grande polêmica (HARADA, 2015).

Aliás, a discriminação por parte de algoritmos é um dos desafios do Direito Digital. Como dar respostas à uma sociedade discriminada por códigos que a rotulam, classificam ou humilham?

Igualmente, existem diversas situações que o uso da Inteligência Artificial causou danos ou obtiveram resultados equivocados.

Nos casos envolvendo o reconhecimento facial através da Inteligência Artificial, apesar de terem como fundamento a segurança pública, gera insegurança jurídica, visto que muitos casos o reconhecimento é errôneo. Em 2018, uma pesquisa da ACLU demonstrou que o software de identificação facial Rekognition, da Amazon, identificou 28 membros do Congresso dos Estados Unidos que eram negros como suspeitos da polícia (FUSSEL, 2018).

Há o caso do chat criado pela Microsoft e liberado no Twitter, chamada Tay, que foi feita para conversar com as pessoas de forma divertida, descontraída e natural, mas, em menos de 24 horas, começou a proferir mensagens de cunho racista e ofensivos, devido ao contato com os demais internautas (TECHMUNDO, 2019).

Além disso, existem as *deepfakes*, isto é, o emprego de Inteligência Artificial para fazer vídeos e imagens, criando pessoas que não existem ou alterando os conteúdos de vídeos, a fim de espalhar notícias falsas, causar fraudes ou prejudicar a honra de alguém. Nesse contexto, a poetisa Helen Mortd descobriu que suas imagens tinham sido enviadas para um site de pornô, sendo que as originais foram copiadas de suas redes sociais e foram mescladas com imagens sexuais explícitas e violentas (ROYLE, 2021).

Dessa forma, o uso da Inteligência Artificial provoca diversos questionamentos aos operadores do Direito, visto que a maioria dos sistemas que utilizam a Inteligência Artificial são “treinados” por seres humanos a partir de uma base de dados.

Ao mesmo tempo em que o emprego de algoritmos para a tomada de decisões traz diversos benefícios, também apresenta riscos que, muitas vezes, não são evidentes e podem causar diversos problemas, como discriminação e insegurança jurídica.

Em relação à regularização do uso Inteligência Artificial, em 2017, a União Europeia elaborou a Disposições de Direito Civil sobre Robótica, que contém princípios, responsabilidades e outras regulamentações.

No Brasil, há o Projeto de Lei nº 21/20 que cria o marco legal do desenvolvimento e uso da Inteligência Artificial (IA) pelo poder público, por empresas, entidades diversas e pessoas físicas, além do Projeto de Lei nº 5.051/2019, que estabelece os princípios para o uso da Inteligência Artificial no Brasil. Todas estas questões farão parte do diaadia do Advogado

especialista em Direito Digital.

Portanto, os advogados especialistas em Direito Digital são essenciais e devem auxiliar no desenvolvimento de programas que utilizam a Inteligência Artificial, bem como na construção de parâmetros para o uso responsável e adequado da tecnologia, visto que diversos questionamentos e debates vêm surgindo com o seu uso, além de inúmeras situações com repercussão jurídica.

### **IoT (Internet of things)**

O termo *Internet of Things* (IoT), também conhecido como Internet das coisas, significa o estabelecimento de uma conexão entre as pessoas, as máquinas, os objetos e outros aspectos da vida, em que tudo está ligado à Internet.

Na vida cotidiana, a IoT permite que os celulares, relógios, aparelhos eletrônicos, carros, eletrodomésticos e outros equipamentos estejam conectados entre si, aumentando a agilidade nas tarefas diárias e no monitoramento de questões pessoais, como saúde e segurança.

Dentro de um setor empresarial, a IoT estabelece redes inteligentes que auxiliam na prevenção e resolução de problemas, bem como impulsiona a eficácia dos processos já existentes.

No Brasil, foi publicado o Decreto nº 9.854/19 e institui o Plano Nacional de Internet das Coisas no Brasil, estabelecendo conceitos, diretrizes sobre a Internet das Coisas. O Decreto define IoT como “a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade”.

A IoT também está relacionada ao fenômeno conhecido como *Big Data*, em que muitos dados são detectados, coletados e

processados pelos objetos e computadores, numa velocidade rápida, o que deve preocupar o advogado especialista em Direito Digital, visto que isso pode gerar muitos riscos, como a coleta indevida de dados.

Nos Estados Unidos, um cassino instalou um aquário de peixes utilizando IoT em seu salão, que possuía um cronograma de alimentação dos peixes, assim como os níveis de sal e temperatura eram automaticamente regulados, o termostato podia enviar uma mensagem para o dono caso a água ficasse muito quente ou fria. Um hacker usou o aquário inteligente como ponto de entrada na rede, aproveitou-se da falha de segurança para se mover dentro do sistema informático (GRUSTNIY, 2018).

Apesar de existirem muitas vantagens, é preciso que o advogado especialista em Direito Digital esteja atento aos riscos em razão do uso de dispositivos envolvendo IoT.

Para analisar os riscos quando da utilização da IoT, é preciso considerar os princípios da proteção de dados, como os princípios da *privacy by design* (desde a concepção) e *privacy by default* (por padrão).

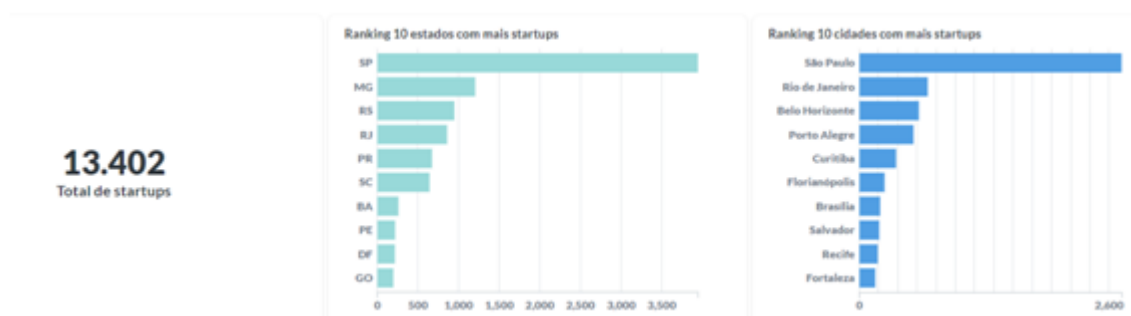
Portanto, a atuação do advogado especialista em Direito Digital pode ser voltada para a regulamentação e a adequação dos dispositivos, a identificação de riscos e alternativas para mitigá-los, bem como na defesa dos criadores do dispositivo ou dos consumidores quando da ocorrência de um dano.

## **Startups e Inovação**

A definição de uma startup é: empresas que estão em uma fase de desenvolvimento e pesquisa de mercado e podem vir em todas as formas, incluindo aquelas associadas a empresas orientadas para a tecnologia de alto crescimento. As Startups têm modelos de negócio repetíveis, temporários e escaláveis. Os investidores geralmente são mais atraídos pelas novas empresas que se distinguem por seu perfil de risco/recompensa e

escalabilidade. Isto é, eles têm custos de inicialização mais baixos, maior risco e maior potencial de retorno sobre o investimento. As startups bem-sucedidas são normalmente mais escaláveis do que uma empresa estabelecida, no sentido de que podem crescer rapidamente com investimento limitado de capital, trabalho ou terra (USLEGAL).

Atualmente, no Brasil há mais de 13.400 startups, sendo o estado de São Paulo o estado que mais possui. Em relação ao público alvo, 47,88% está direcionada ao B2B (STARTUPBASE).



Acesso em: 26/01/2021

Dentro do cenário jurídico brasileiro, há diversas startups voltadas ao Direito, denominadas legaltechs e lawtechs. Segundo a AB2L (Associação Brasileira de Lawtechs e Legaltechs), existem as seguintes categorias:

- Analytics e Jurimetria – Plataformas de análise e compilação de dados e jurimetria.
- Automação e Gestão de Documentos – Softwares de automação de documentos jurídicos e gestão do ciclo de vida de contratos e processos.
- Compliance – Empresas que oferecem o conjunto de disciplinas para fazer cumprir as normas legais e políticas estabelecidas para as atividades da instituição.
- Conteúdo Jurídico, Educação e Consultoria – Portais de informação, legislação, notícias e demais empresas de consultoria com serviços desde segurança de informação a

assessoria tributária.

– Extração e monitoramento de dados públicos – Monitoramento e gestão de informações públicas como publicações, andamentos processuais, legislação e documentos cartorários.

– Gestão – Escritórios e Departamentos Jurídicos – Soluções de gestão de informações para escritórios e departamentos jurídicos.

– IA – Setor Público – Soluções de Inteligência Artificial para tribunais e poder público.

– Redes de Profissionais – Redes de conexão entre profissionais do direito, que permitem a pessoas e empresas encontrarem advogados em todo o Brasil.

– Regtech – Soluções tecnológicas para resolver problemas gerados pelas exigências de regulamentação.

– Resolução de conflitos online – Empresas dedicadas à resolução online de conflitos por formas alternativas ao processo judicial como mediação, arbitragem e negociação de acordos.

– Taxtech – Plataformas que oferecem tecnologias e soluções para todos os seus desafios tributários.

– Civic Tech – Tecnologia para melhorar o relacionamento entre pessoas e instituições, dando mais voz para participar das decisões ou melhorar a prestação de serviços.

– Real Estate Tech – Aplicação da tecnologia da informação através de plataformas voltadas ao mercado imobiliário e cartorário.

Como as startups estão cada vez mais ligadas à tecnologia, seja durante o desenvolvimento do negócio ou na criação das soluções, é necessário que um advogado especialista em Direito Digital acompanhe a empresa e dê respostas jurídicas aos

desafios impostos por negócios disruptivos e que geram reação de competidores, governos e da sociedade.

A exemplo, temos inúmeros processos que tratam de questões jurídicas relativas ao UBER e aplicativos de transporte privados de passageiros, incluindo processos no Superior Tribunal de Justiça (STJ) que buscam vínculo trabalhista entre motoristas, conforme a decisão a seguir:

CONFLITO NEGATIVO DE COMPETÊNCIA. INCIDENTE MANEJADO SOB A ÉGIDE DO NCP. AÇÃO DE OBRIGAÇÃO DE FAZER C.C. REPARAÇÃO DE DANOS MATERIAIS E MORAIS AJUIZADA POR MOTORISTA DE APLICATIVO UBER. RELAÇÃO DE TRABALHO NÃO CARACTERIZADA. SHARING ECONOMY. NATUREZA CÍVEL. COMPETÊNCIA DO JUÍZO ESTADUAL. 1. A competência *ratione materiae*, via de regra, é questão anterior a qualquer juízo sobre outras espécies de competência e, sendo determinada em função da natureza jurídica da pretensão, decorre diretamente do pedido e da causa de pedir deduzidos em juízo. 2. Os fundamentos de fato e de direito da causa não dizem respeito a eventual relação de emprego havida entre as partes, tampouco veiculam a pretensão de recebimento de verbas de natureza trabalhista. A pretensão decorre do contrato firmado com empresa detentora de aplicativo de celular, de cunho eminentemente civil. 3. **As ferramentas tecnológicas disponíveis atualmente permitiram criar uma nova modalidade de interação econômica, fazendo surgir a economia compartilhada (sharing economy), em que a prestação de serviços por detentores de veículos particulares é intermediada por aplicativos geridos por empresas de tecnologia. Nesse processo, os motoristas, executores da atividade, atuam como empreendedores individuais, sem vínculo de emprego com a empresa proprietária da plataforma.[...].** (STJ, Conflito de

Competência 164544/MG, Rel. Min. Moura Ribeiro, DJE 04/09/2019).

Outro conflito judicial é o Recurso Especial (STJ) nº 1.819.075/RS que está relacionado à possibilidade dos condomínios residenciais, por meio de suas convenções, proibirem moradores de oferecerem a unidade imobiliária ou parte delas para locação, inclusive por meio de plataformas digitais, como o Airbnb, que é uma startup.

Portanto, a atuação do especialista em Direito Digital pode ser voltada para o auxílio na regularização do negócio, na elaboração de termos de uso e políticas de privacidade para sites e aplicativos, bem como na adequação à Lei Geral de Proteção de Dados. Além disso, poderá atuar de forma multidisciplinar, dando suporte e orientação para investimentos relacionados à tecnologia e nas questões cíveis, societárias, consumeristas e financeiras ligadas ao negócio.

### **Contratos eletrônicos, e-commerce e marketplaces**

Como muitas relações são estabelecidas no ambiente virtual, uma área que vem ganhando destaque é o Direito Contratual. Desde a compra de um produto e até a contratação de um serviço digital, é preciso realizar um contrato para estabelecer as obrigações de cada parte, bem como identificá-las.

Além disso, cumpre destacar o desenvolvimento do e-commerce, fator que também reforça o aumento de contratos celebrados no ambiente virtual.

O conceito de contrato eletrônico é: contrato em que sua celebração depende da existência de um sistema informático, ou da intercomunicação entre sistemas informáticos. As categorias de contratos eletrônicos são: 1) interpessoal: a comunicação ocorre entre as partes; 2) intersistêmico: os sistemas informáticos se intercomunicam-se por meio de comandos automáticos; e 3) interativo: é o resultado de uma relação de comunicação estabelecida entre uma pessoa e um servidor de



aplicação (BRANCHER, 2018).

Uma opção para garantir a autenticidade, validade jurídica e integridade dos documentos celebrados no ambiente digital, é a utilização de assinatura eletrônica (ICP- Brasil ou Assinatura Digital biométrica), o que representa uma forma de proporcionar segurança jurídica.

No Brasil, já existem decisões reconhecendo a validade jurídica de contratos eletrônicos, incluindo os não efetivados por meio de assinatura digital, como nas as denominadas “telas sistêmicas” ou contratos interativos. Além disso, já se reconhece até mesmo a possibilidade de execução de contratos digitais.

Nesse sentido, cumpre colacionar as seguintes decisões:

Processual civil. Agravo de instrumento. Execução de título extrajudicial. Exceção de pré-executividade. Contrato eletrônico. Assinatura digital. Validade. Inclusão do fiador após a citação do executado. Possibilidade. Art. 264 do CPC (LGL\2015\1656)

**APELAÇÃO – AÇÃO DE EXIBIÇÃO DE DOCUMENTOS – CONTRATAÇÃO REALIZADA POR MEIO ELETRÔNICO – DOCUMENTOS APRESENTADOS PELA PARTE REQUERIDA – ESGOTAMENTO DA OBRIGAÇÃO – PRESENÇA DE PEDIDO ADMINISTRATIVO – RESISTÊNCIA AO PEDIDO INICIAL – HONORÁRIOS DE SUCUMBÊNCIA DEVIDOS – MAJORAÇÃO – POSSIBILIDADE. A parte requerida trouxe aos autos todos os documentos inerentes à relação jurídica firmada entre as partes, possibilitando a verificação de todos os encargos que recaem sobre o contrato, razão pela qual esgotada está a sua obrigação. Nos casos em que a celebração do contrato se dá por meio eletrônico, não há falar em exibição do instrumento de contrato impresso e**

**devidamente assinado pelas partes, uma vez tal documento não existe.** A parte que recusa apresentar documentos dá causa ao ajuizamento da ação exorbitária e, por conseguinte, deve arcar com os ônus de sucumbência. (TJMG – Apelação Cível 1.0290.14.009126-2/001, Relator: Des. Alberto Henrique, 13ª CÂMARA CÍVEL, julgamento em 01/10/2015)

MONITÓRIA. EMPRÉSTIMO. DEMONSTRAÇÃO DA RELAÇÃO JURÍDICA. **1. O contrato eletrônico, autenticado digitalmente, é documento hábil a demonstrar existência de relação jurídica entre as partes.** 2. Nada nos autos infirma a existência da dívida, ao contrário. Há elementos suficientes a corroborar existência e valor do débito perseguido. 3. Observando-se que a sentença não deve ser reformada, porquanto irretocável sua análise dos fatos e fundamentação, possível a confirmação do resultado, ratificando aqueles fundamentos, nos termos do art. 252 do Regimento Interno desta Corte. 4. Recurso não provido. (TJSP; Apelação Cível 1026263-69.2017.8.26.0224; Relator: Melo Colombi; Órgão Julgador: 14ª Câmara de Direito Privado; Data do Julgamento: 16/12/2020)

Portanto, o advogado especialista em Direito Digital deve ser criativo para prever situações que podem trazer consequências negativas para o seu cliente, bem como poderá auxiliar as partes durante a celebração do contrato, bem como realizá-los, através de plataformas online de assinatura de contratos, *blockchain* ou *smart contracts*, que serão analisados posteriormente.

## **PERSPECTIVAS E DESAFIOS NO DIREITO DIGITAL**

E os ânimos neste ponto são bem acirrados. O Brasil já possui diversas ações judiciais importantes no âmbito do Direito

Digital, tais como:

– Supremo Tribunal Federal – Recurso Extraordinário nº 1.057.258: apesar de ainda não ter sido julgado, discute o dever de empresa hospedeira de sítio na internet fiscalizar o conteúdo publicado e de retirá-lo do ar quando considerado ofensivo, sem intervenção do Judiciário.

– Supremo Tribunal Federal – Ação Direta de Constitucionalidade (ADC) nº 51: o compartilhamento de dados controlados por provedores de acesso à internet sediados no exterior, em razão do crescimento e dependência da obtenção desses dados como elemento de evidência na persecução criminal.

– Supremo Tribunal Federal – Ação Direta de Inconstitucionalidade (ADI) nº 5.527 e Ação de Descumprimento de Preceito Fundamental (ADPF) nº 403: possibilidade de decisões judiciais autorizarem o bloqueio de serviços de mensagens pela internet, como WhatsApp.

– Supremo Tribunal Federal – Ação Direta de Constitucionalidade (ADC) nº 6.387: decisão que reconheceu o direito fundamental autônomo à proteção de dados pessoais e o direito à autodeterminação informativa.

Além disso, o volume de reclamações em delegacias cresce e, por outro lado, não existe especialização e pessoas suficientes para atender todos os casos, pois faltam profissionais na área.

Todos estes fatores somados ao crescimento de novos meios de comunicação e a onda de negócios digitais influenciados pela mentalidade das startups faz com que este universo da advocacia no Direito Digital tenda a crescer cada vez mais e se consolidar como uma das áreas mais promissoras do direito. Cresceu a demanda e procura por escritórios especializados em tecnologia e digital, por agências de marketing digital por exemplo, buscando respaldo em suas ações variadas e de “*inbound marketing*”, bem como por startups, afiliados em

negócios digitais, influenciadores digitais preocupados com licenciamento de imagem e conteúdo (direitos autorais) e fábricas de aplicativos.

Em relação às regulamentações, a União Europeia elaborou o *"The Digital Services Act package"*, que abrange um conjunto de regras que regem os serviços digitais e possui os escopos: 1) criar um espaço digital mais seguro no qual os direitos fundamentais de todos os usuários de serviços digitais sejam protegidos; 2) estabelecer condições de concorrência equitativas para promover a inovação, o crescimento e a competitividade.

No Brasil, podemos mencionar o Projeto de Lei nº 2.630/2020, também denominada Lei das Fake News, que estabelece normas relativas à transparência de redes sociais e de serviços de mensagens privadas, sobretudo no tocante à responsabilidade dos provedores pelo combate à desinformação e pelo aumento da transparência na internet, à transparência em relação a conteúdos patrocinados e à atuação do poder público, bem como estabelece sanções para o descumprimento da lei.

Também há o Decreto nº 9.283/2018 que regulamenta a Lei de Inovação (Lei nº 10.973/2004, modificada pela Lei nº 13.243/2016), a Lei das Licitações (art. 24, § 3º, e o art. 32, § 7º, da Lei nº 8.666/1993), o art. 1º da Lei nº 8.010/1990 (Lei de Importações de bens destinados à pesquisa científica e tecnológica) e o art. 2º, caput, inciso I, alínea g, da Lei nº 8.032/1990 (Lei de Isenção de Impostos de Importação – Empresas), e estabelece medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação tecnológica, ao alcance da autonomia tecnológica e ao desenvolvimento do sistema produtivo nacional e regional.

Assim, os principais desafios do advogado especialista em Direito Digital é acompanhar as mudanças tecnológicas e as alterações legislativas, para atender de forma cada vez mais

eficiente e atualizada.

## **TENDÊNCIAS NO DIREITO DIGITAL**

As tendências no Direito Digital, como IoT, Inteligência Artificial, *blockchain*, bitcoin, demandarão mais ainda o profissional do Direito Digital, que deve ser capaz de “pensar fora da caixa” e de dar soluções ágeis para manutenção da segurança jurídica das operações, no dinamismo que elas acontecem, equacionando a balança entre “inovar” e “estar em conformidade”. Isso não é fácil. Dentre as novas tendências, podemos citar:

### **▪ Métodos On-line de Resolução de Disputas (ODRs)**

O aumento da quantidade das disputas e dos litígios é um efeito colateral da inovação, visto que as interações acontecem cada vez mais no espaço digital.

Por sua vez, fatores como a evolução tecnológica e a globalização permitem que se estabeleça formas de usar a tecnologia também para resolver os conflitos.

Nesse cenário, surge o *Online Dispute Resolution Systems* (ODR) ou mecanismos online de resolução de conflitos, que é uma forma mais célere e econômica de resolver conflitos, além de evitar desgastes emocionais com o encontro presencial.

No Brasil, temos uma plataforma de solução de disputas desenvolvida pelo Ministério da Justiça do Governo Federal, que se chama **consumidor.gov.br**.

Portanto, o advogado especialista em Direito Digital deve atentar-se a essas novas formas de solucionar os conflitos, buscando simplificar e agilizar a resolução do conflito do cliente, sem deixar de lado a segurança jurídica.

### **▪ *Smart contract* e *blockchain***

O *smart contract* são contratos digitais autoexecutáveis (*self-*

*enforcement*), que usam determinada tecnologia, como *ablockchain*, para garantir a execução dos acordos estipulados, independente da intervenção humana. Para tanto, através de um programa de computador, são elaborados os termos contratuais, sendo que o contrato será cumprido até o final, não permitindo alterações entre as partes.

A *blockchain* é uma tecnologia descentralizada de dados onde se tornam possíveis as transações digitais com as criptomoedas. O conceito *blockchain* surgiu em 2008 no artigo acadêmico "Bitcoin: Um sistema financeiro eletrônico peer-to-peer", elaborado por Satoshi Nakamoto (2008).

Apesar de não haver regulamentação legal no direito brasileiro, é preciso verificar se a situação que está sendo celebrado o *smart contract* está em consonância com os princípios norteadores dos contratos, como o da autonomia da vontade.

Alguns projetos de Lei que tratam de *blockchain* e Criptomoedas no Brasil são:

- Projeto de Lei nº 2.060/2019 que dispõe sobre o regime jurídico de Criptoativos;
- Projeto de Lei nº 3.443/2019 que dispõe sobre a Prestação Digital dos Serviços Públicos na Administração Pública – Governo Digital e prevê o uso da *blockchain*;
- Projeto de Lei nº 3.949/ 2019 que regulamenta a utilização de moedas virtuais e o funcionamento de empresas intermediadoras dessas operações;
- Projeto de Lei nº 4.207/2020 que dispõe sobre os ativos virtuais e sobre as pessoas jurídicas que exerçam as atividades de intermediação, custódia, distribuição, liquidação, transação, emissão ou gestão desses ativos virtuais.

Como visto, dentro do Direito Digital, a especialização em negócios com base na *blockchain* ou de criptoativos demonstra-se promissora, considerando que a tecnologia se consolida e impõe desafios para os negócios que estão surgindo, demandando profissionais especializados no ambiente regulatório.

Do mesmo modo, como o *smart contract* está revolucionando os negócios jurídicos, o advogado especialista em Direito Digital deve auxiliar as partes quando da elaboração do contrato, bem como utilizá-lo para facilitar o dia a dia, a fim de agilizar e conferir segurança nas relações acordadas. Em breve, estes especialistas programarão contratos autoexecutáveis.

#### ▪ **LGPD: eficácia da lei e a atuação da ANPD**

Com a entrada em vigor da LGPD em setembro de 2020, haverá uma crescente procura por advogados especialistas em Direito Digital e Proteção de Dados para regularização dos negócios ou atuação em casos pontuais envolvendo questionamentos e tratamentos irregulares de dados, sobretudo, diante das multas previstas na LGPD que poderão ser aplicadas a partir de agosto de 2021.

Assim, muitas empresas vão entrar numa corrida contra o tempo para se adequarem, o que representa uma oportunidade para os advogados do Direito Digital. Sobre o tema, veja o artigo sobre as 10 oportunidades rentáveis para advogados com o advento da LGPD (<https://josemilagre.jusbrasil.com.br/artigos/698996875/lei-geral-de-protecao-de-dados-10-oportunidades-rentaveis-de-atuacao-para-advogados>).

Em relação à ANPD, espera-se que após o início de suas atividades, muitas questões sejam devidamente regulamentadas e esclarecidas, bem como realize suas atribuições previstas na LGPD com êxito.

Dessa forma, no ano de 2021 haverá muitas oportunidades para os advogados especialistas em Direito Digital, visto que as

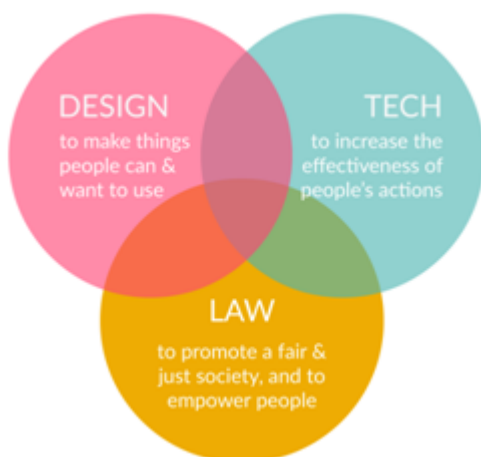
empresas estão cada vez mais buscando a adequação à LGPD.

### ▪ *Legal design*

Em uma realidade em que muitos serviços legais são realizados por meio de plataformas, como ODR e startups, os advogados especialistas em Direito Digital precisam estar atentos às formas de entregar os seus serviços e realizar a comunicação.

Margaret Hagan, em seu livro “Law by design”, afirma que o *legal design* é uma forma de avaliar e criar serviços jurídicos, com foco em quão utilizáveis, úteis e envolventes são esses serviços. É uma abordagem com três conjuntos principais de recursos – processo, mentalidade e mecânica – para os profissionais jurídicos usarem. Esses três recursos podem ajudar a conceber, construir e testar melhores maneiras de fazer as coisas na lei, que irão envolver e capacitar leigos e profissionais do direito.

Nesse contexto, o *legal design*, inspirado no *Design Thinking*, tem o escopo encontrar soluções estratégicas e inovadoras no mundo jurídico, a partir da intersecção do Design, Tecnologia e Direito.



Assim, o advogado especialista em Direito Digital, através do *legal design*, estabelecerá uma comunicação legal inteligente, tornando os documentos jurídicos mais acessíveis e compreensíveis, principalmente com os seus clientes. Além



disso, auxiliará na desburocratização do acesso à justiça, facilitando a interpretação.

## **COMPETÊNCIAS DESEJÁVEIS DO ADVOGADO ESPECIALISTA EM DIREITO DIGITAL**

Não existe uma “formação obrigatória” para atuar com Direito Digital. No entanto, é lógico que é desejável, além do conhecimento jurídico, profundo conhecimento de tecnologia da informação.

Com a multiplicação de cursos e pós-graduações em Direito Digital e da tecnologia da informação, a concorrência também ficou maior do que há quinze ou dez anos atrás, razão pela qual espera-se deste profissional mais do que breves noções ou “paixão” em tecnologia, redes, protocolos, mas, de fato, que entenda como as principais tecnologias funcionam, sobretudo em procedimentos de quebras de sigilo informático, em que um erro de interpretação ou cálculo de fuso-horários por exemplo, pode ser fatal e indicar pessoas sem qualquer relação com um incidente informático ou crime digital.

Como se pode ver, atualização é palavra constante para o profissional que deseje atuar com direito, tecnologia e inovação. Mais que isso, espera-se que o advogado especialista em Direito Digital conheça técnicas de coleta de provas eletrônica, mas, principalmente, que tenha em mente que advogar em Direito Digital exige um dinamismo fora do comum em comparação com outras áreas do Direito, o que demandará dos profissionais atualização constante e muitas horas dedicadas ao estudo de tecnologias incluindo, mas não se limitando a redes, segurança da informação, programação, perícia forense digital e outras habilidades.

Portanto, para que o advogado especialista em Direito Digital domine sua área de atuação, é importante o comprometimento com o estudo e a frequente busca pelo conhecimento profissional, a fim de atuar com segurança e acompanhar a evolução

tecnológica.

## **CONCLUSÃO**

Como visto, foi possível compreender o que é o Direito Digital, quais as oportunidades na área, as competências necessárias, qual o foco de atuação deste profissional, e, inclusive apresentar as tendências que prometem movimentar o mercado.

O advogado especialista em Direito Digital vai necessitar de uma visão cada vez mais multidisciplinar para ser capaz de “pensar fora da caixa” e de dar soluções ágeis para manutenção da segurança jurídica das operações, no dinamismo que elas acontecem na sociedade da informação.

Hoje, todos os advogados devem entender de tecnologia, razão pela qual é comum que muitos se enveredam para as causas do Direito Digital e não somente usem a informática jurídicas, para terem escritórios mais eficientes e atrativos.

Para crescerem, empresas e pessoas precisam estar juridicamente preparadas para o mundo digital, razão pela qual precisam do profissional do Direito Digital, que poderá atuar de forma preventiva ou contenciosa nas inúmeras questões que podem surgir quando da utilização da tecnologia.

Em uma sociedade digital, sobretudo pósCOVID-19, os ataques e golpes cibernéticos aumentaram e a defesa dos direitos de vítimas precisa ser exercida por profissionais preparados.

A medida em que a tecnologia evolui impõe-se novos desafios jurídicos. O advogado em Direito Digital tem este relevante papel, servido como o elo entre as pessoas e seus direitos, a partir de violações e problemas trazidos pela tecnologia, cada vez mais comuns e que se renovam a cada dia.

Portanto, o advogado especialista em Direito Digital deve estar preparado para atender as demandas que ocorrem no

ambiente virtual, capacitando-se, a fim de proporcionar segurança jurídica e proteção aos usuários. Além disso, esse profissional nunca foi tão essencial. Não só para defender vítimas de crimes digitais, apurar autoria de crimes e buscar justiça diante de fatos danosos ou desavenças cometidas ou originadas no ciberespaço, mas tem grande propósito: **Por meio de sua atuação, sempre diligente e atenta aos rumos das tecnologias e suas consequências, conscientizar e educar a sociedade para riscos do mundo digital, contribuindo para uma sociedade mais evoluída e segura. Acredito que com isso respondo à pergunta do título deste artigo.**

## **COMO COMEÇAR?**

Pela CyberExperts oferecermos cursos de absoluta relevância para o profissional que pretenda atuar no direito digital, sendo o **CURSO ADVOCACIA PRÁTICA DE DIREITO DIGITAL e FERRAMENTAS TECNOLÓGICAS PARA ADVOCACIA**Os treinamentos práticos de extensão que prepara o profissional para o mercado de trabalho. Para conhecer as próximas turmas conecte-se comigo ou acesse [www.cyberexperts.com.br](http://www.cyberexperts.com.br)

Também se inscreva no meu canal no Youtube ([youtube.com/josemilagre](https://youtube.com/josemilagre)) onde disponibilizo conteúdo semanal e gratuito para profissionais na área. Para contatos sobre mentoria para escritórios fale comigo: [consultor@josemilagre.com.br](mailto:consultor@josemilagre.com.br)

**José Antonio Milagre**  
(<https://app.exeed.pro/holder/badge/55319>) Data Protection Officer (DPO) EXIN. Pesquisador em direito e dados do Núcleo de Estudos em Web Semântica e Análise de Dados da USP (Universidade de São Paulo). Mestre e Doutorando em Ciência da Informação pela UNESP. Pós Graduado em Gestão de Tecnologia da Informação. Advogado com atuação em Direito Digital. Perito

Judicial em Informática e Proteção de Dados. Presidente da Comissão de Direito Digital da Regional da Vila Prudente da OAB/SP. Autor de dois livros pela Editora Saraiva (Marco Civil da Internet: Comentários a Lei 12.975/2014 e Manual de Crimes Informáticos).

**Laura Secfém Rodrigues.** Pós-graduanda em Direito, Tecnologia e Inovação com ênfase em proteção de dados, no Instituto New Law. Graduada em Direito pelo Centro Universitário de Bauru/SP, mantido pela Instituição Toledo de Ensino (ITE).

© 2021. Proibida cópia ou reprodução sem autorização prévia e expressa do autor: [consultor@josemilagre.com.br](mailto:consultor@josemilagre.com.br)

## REFERÊNCIAS

**AB2L.** Disponível em: <https://ab2l.org.br/radar-lawtechs/>. Acesso em 26/01/2021.

ALLISON, Peter Ray. A revolução dos robôs cuidadores está por vir? **BBC**, 05 de junho de 2019. Disponível em: <https://www.bbc.com/portuguese/vert-fut-48290191>. Acesso em 25/01/2021.

A new horizon: Expanding the AI landscape. **Mit Technology Review**, 30 de novembro de 2020. Disponível em: [A new horizon: Expanding the AI landscape. https://www.technologyreview.com/2020/11/30/1012528/a-new-horizon-expanding-the-ai-landscape/](https://www.technologyreview.com/2020/11/30/1012528/a-new-horizon-expanding-the-ai-landscape/). Acesso em 25/01/2021.

BRANCHER, Paulo Marcos Rodrigues. Contrato eletrônico. **Enciclopédia jurídica da PUC-SP**. Celso Fernandes Campilongo, Alvaro de Azevedo Gonzaga e André Luiz Freire (coords.). Tomo: Direito Comercial. Fábio Ulhoa Coelho, Marcus Elidius Michelli de Almeida (coord. de tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em:

<https://enciclopediajuridica.pucsp.br/verbete/259/edicao-1/contrato-eletronico>. Acesso em 25/01/2021.

**Datasafer**. 2019. Disponível em: <https://helpline.org.br/indicadores>. Acesso em 25/01/2021.

Digital Forensics Market by Component (Hardware, Software, and Services), Type (Computer Forensics, Network Forensics, Mobile Device Forensics, and Cloud Forensics), Tool, Vertical, and Region – Global Forecast to 2022. **Markets and markets**. Disponível em: <https://www.marketsandmarkets.com/Market-Reports/digital-forensics-market-230663168.html>. Acesso em 25/01/2021.

Disposições de Direito Civil sobre Robótica. Disponível em: [https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051\\_PT.html#title1](https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html#title1). Acesso em 25/01/2021.

FUSSEL, Sidney. Amazon sem querer mostrou por que não deveria oferecer seu reconhecimento facial para a polícia. **GIZMODO**, 30 de julho de 2018. Disponível em: <https://gizmodo.uol.com.br/amazon-reconhecimento-facial-policia/>. Acesso em 25/01/2021.

GRUSTNIY, Leonid. O aquário que quebrou um cassino. **KASPERSKY**, 16 de maio de 2018. Disponível em: <https://www.kaspersky.com.br/blog/leaking-fish-tank/10280/>. Acesso em 25/01/2021.

GONZAGA, Francisco; FERNANDES, Matheus. Com a inteligência artificial, criar música é uma questão de segundos. **Estadão**, 16 de julho de 2019. Disponível em: <https://arte.estadao.com.br/focas/estadaoqr/materia/inteligencia-artificial-musica-startup-amper>. Acesso em 25/01/2021.

GOOGLE. **Guia sobre análise de dados e aprendizado de máquina para CIO**. 2017. Disponível em: [https://lp.google-mkto.com/rs/248-TPC-286/images/Guide\\_to\\_Data\\_Analytics\\_%26\\_Machine\\_Learning\\_portuguese.pdf](https://lp.google-mkto.com/rs/248-TPC-286/images/Guide_to_Data_Analytics_%26_Machine_Learning_portuguese.pdf). Acesso em

25/01/2021.

HAGAN, Margaret. **Law by design**. <https://www.lawbydesign.co/legal-design/>. Disponível em: Acesso em 25/01/2021.

HARADA, Eduardo. Fail épico: sistema do Google Fotos identifica pessoas negras como gorilas. **TECHMUNDO**, 01 de julho de 2015. Disponível em: <https://www.tecmundo.com.br/google-fotos/82458-polemica-sistema-google-fotos-identifica-pessoas-negras-gorilas.htm>. Acesso em 25/01/2021.

Introducing a More Seamless Navigate on Autopilot. **Tesla**, 03 de abril de 2019. Disponível em: <https://www.tesla.com/blog/introducing-more-seamless-navigate-autopilot>. Acesso em 25/01/2021.

Machine Learning Initiatives Across Industries: Practical Lessons from IT Executives. **M-Brain**, 14 de junho de 2017. Disponível em: <https://www.m-brain.com/white-papers/machine-learning-initiatives-across-industries-practical-lessons-executives/>. Acesso em 25/01/2021.

MACHADO, Felipe. Brasil perde US\$ 10 bilhões por ano com cibercrime, diz McAfee. **Veja**, 21 de fevereiro de 2018. Disponível em: <https://veja.abril.com.br/economia/brasil-perde-us-10-bilhoes-por-ano-com-cibercrime-diz-mcafee/>. Acesso em: 26/01/2021.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em 25/01/2021.

Projeto VICTOR do STF é apresentado em congresso internacional sobre tecnologia. **STF**, 26 de setembro de 2018. Disponível em: <http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=390818>. Acesso em 25/01/2021.

ROYLE, Sara. Pornô deepfake: 'As imagens falsas com a minha cara ainda me dão pesadelos'. **BBC**, 14 de janeiro de 2021. Disponível em: <https://www.bbc.com/portuguese/geral-55630077>. Acesso em: 26/01/2021.

Startup canadense desenvolve robô-advogado que interpreta leis. **Época**, 13 de fevereiro de 2019. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2019/02/startup-canadense-desenvolve-robo-advogado-que-interpreta-leis.html>. Acesso em 25/01/2021.

**STARTSE**. Disponível em: <https://startupbase.com.br/home/stats>. Acesso em 26/01/2021.

Tay: Twitter conseguiu corromper a IA da Microsoft em menos de 24 horas. **TECHMUNDO**, 24 de março de 2016. Disponível em: <https://www.tecmundo.com.br/inteligencia-artificial/102782-tay-twitter-conseguiu-corromper-ia-microsoft-24-horas.htm>. Acesso em 25/01/2021.

The Digital Services Act package. Disponível em: <https://ec.europa.eu/digital-single-market/en/digital-services-act-package>. Acesso em 25/01/2021.

**USLEGAL. Startup Companies Law and Legal Definition.** Disponível em: <https://definitions.uslegal.com/s/startup-companies>. Acesso em 25/01/2021.

---

# **Criminosos aplicam golpe do falso agendamento de vacina**

# contra Covid-19

Saiba como se proteger assistindo ao vídeo.

Você também encontra outras orientações sobre como agir, caso seja vítima de crimes digitais, no canal do YouTube, acesse: <https://www.youtube.com/user/josemilagre>

---

## **FAKE NEWS! Vulnerabilidades do armazenamento da cadeia de contatos dos serviços de mensageria (PL 2630)**

O Especialista e Perito em crimes cibernéticos, José Milagre, fala à Folha SP sobre os malefícios da medida e a importância dos provedores na contribuição para identificar os criminosos.

Acompanhe

em:

<https://www1.folha.uol.com.br/poder/2020/07/regra-para-armazenar-cadeia-de-mensagens-do-whatsapp-pode-ser-ineficaz-em-projeto-de-fake-news-no-congresso.shtml?fbclid=IwAR3KjFnigHxi3nmZPjVDwgAiKYfFTj5QpaQdRNQdUqRILfcCR58TJ80TPMY>

---



# **Vendas pela internet podem facilitar fraudes na Black Friday; veja como evitar**

Você costuma fazer compras pela internet? Sabe como conferir a autenticidade dos sites? Como se proteger para não cair em golpes? O Especialista em Direito Digital e Crimes cibernéticos, José Antonio Milagre, fala sobre os cuidados que devem ser adotados durante as compras e o cenário atrativo para os criminosos durante o período de grandes descontos, como a Black Fryday.

Saiba mais em:  
<https://jovempan.com.br/noticias/brasil/vendas-pela-internet-podem-facilitar-fraudes-na-black-friday-veja-como-evitar.html>

---

**O novo sistema de transferência bancária está dando o que falar! Já cadastrou a sua chave Pix? O Especialista, José Milagre dá dicas para fazê-lo com**

# tranquilidade

O Especialista em Crimes Digitais e Perito em Informática falou ao Gazeta do Povo sobre o novo sistema de transferência bancário, o Pix, você já está por dentro desta nova tecnologia? O Especialista fala sobre a segurança da ferramenta e como se proteger dos golpes que podem surgir.

Para saber mais detalhes acesse:  
<https://www.gazetadopovo.com.br/economia/chave-pix-armadilhas-no-uso-de-dados/>

---

## **Black Friday 2020: Especialista em crimes digitais, José Antonio Milagre, orienta como evitar golpes virtuais e como agir caso tenha sido vítima.**

Mais uma BlackFriday se aproxima e com ela o oportunismo de criminosos cibernéticos, que usam de técnicas variadas para aplicação de golpes, explorando muitas vulnerabilidades dos consumidores virtuais, que desatentos, acabam fornecendo dados pessoais ou comprando em páginas falsas, que são criadas apenas pelo período necessário para tirar o dinheiro do consumidor. Esta edição, porém, promete ser maior por conta do isolamento social diante da COVID-19. Segundo a Ebit Nielsen, as vendas devem crescer 27% em comparação com a edição de

2019.

Os criminosos digitais têm criado “lojas iscas”, normalmente hospedadas em servidores no exterior. Do mesmo modo, ocultam os dados do registrante, por meio de registros “*domain by proxy*”, tudo para dificultar a investigação de quem está por trás do e-commerce “simulado”.

Rapidamente investem em anúncios nos buscadores e outros métodos de impulsionamento, incluindo redes sociais e rapidamente ficam bem ranqueados na rede. A vítima então se depara com o anúncio, normalmente com preço fora do comum. Se não se atentar para elementos visuais da página ou dados de contato da loja, acaba acreditando que está fazendo um bom negócio, e nunca mais verá seu dinheiro.

As lojas falsas, normalmente se valem de depósito bancário ou boletos, que dificultam o cancelamento das compras ou o rastreamento do dinheiro. Assim, todo o cuidado é pouco no período de promoções, já que o crime digital brasileiro explora momentos de grande mobilização digital para auferir lucro, lesando pessoas.

O advogado e perito especialista em crimes cibernéticos, José Antonio Milagre, CEO da CyberExperts e Diretor do Instituto de Defesa do Cidadão na Internet (IDCI) apresenta estratégias para se proteger de golpes digitais e dá dicas sobre como agir, caso tenha sido vítima de fraudes e crimes cibernéticos na BlackFriday.

Dez estratégias para que não que seja vítima de golpes digitais na BlackFriday:

**1) Cuidado com descontos absurdos.** Embora seja BlackFriday, 90% de desconto é algo estranho de se ver. Cuidado, confira a média de preço dos produtos. O criminoso vai usar este gatilho para chamar sua atenção;

**2) Avalie a reputação da Loja.** Em um universo de

aproximadamente 1 milhão de lojas virtuais, muitas delas podem ser “lojas iscas”, criadas para ficar no ar por pouco tempo, fazer centenas de vítimas e desaparecer. Portanto, pesquise se a loja tem “histórico”, comentários, outras compras, etc. O Google está aí para isso;

**3) Avalie as formas de pagamento.** Desconfie de lojas que só oferecem depósito bancário, boleto ou criptomoedas. Estas modalidades podem dificultar o cancelamento da compra ou a investigação dos destinatários. Opte sempre por meios de pagamento seguros, onde o dinheiro é liberado quando o consumidor declara que recebeu a mercadoria;

**4) Busque contatos da loja.** Faça contatos prévios com a loja, mas não só por e-mail, busque um contato telefônico, verifique onde está a sede e desconfie de lojas onde o único contato é um telefone celular;

**5) Cuidado com ofertas em comunicadores, e-mails e redes sociais.** Jamais clique ou acesse lojas virtuais a partir de links, ou ofertas que receber em comunicadores, WhatsApp e redes sociais;

**6) Não acesse lojas pelo buscador.** Acesse diretamente o site da loja evitando também pesquisar pela loja no buscador. Cuidado com pequenas mudanças no nome do site e avalie se possui certificado digital expedido para o próprio site. Os criminosos digitais podem falsear um link direcionando a vítima para o site errado. Ataques de phishing são muito comuns, com a falsificação de marcas e identidade visual de sites com ofertas de descontos, dentre outras chamadas para pescar consumidores desatentos;

**7) Cuidado com códigos enviados para o celular para supostos descontos.** Imagine que você recebe uma mensagem que conseguiu um cupom especial para o BlackFriday, mas para que você receba, você precisará informar um código que chegará pelo celular via SMS. Neste exato momento a vítima não ganhou o

desconto, mas pode ter permitido a clonagem do WhatsApp ou até mesmo ter o reset de senhas de app's financeiros realizados com sucesso, dando acesso ao criminoso. Não confie jamais nesta abordagem. Não informe a ninguém códigos que receber pelo celular;

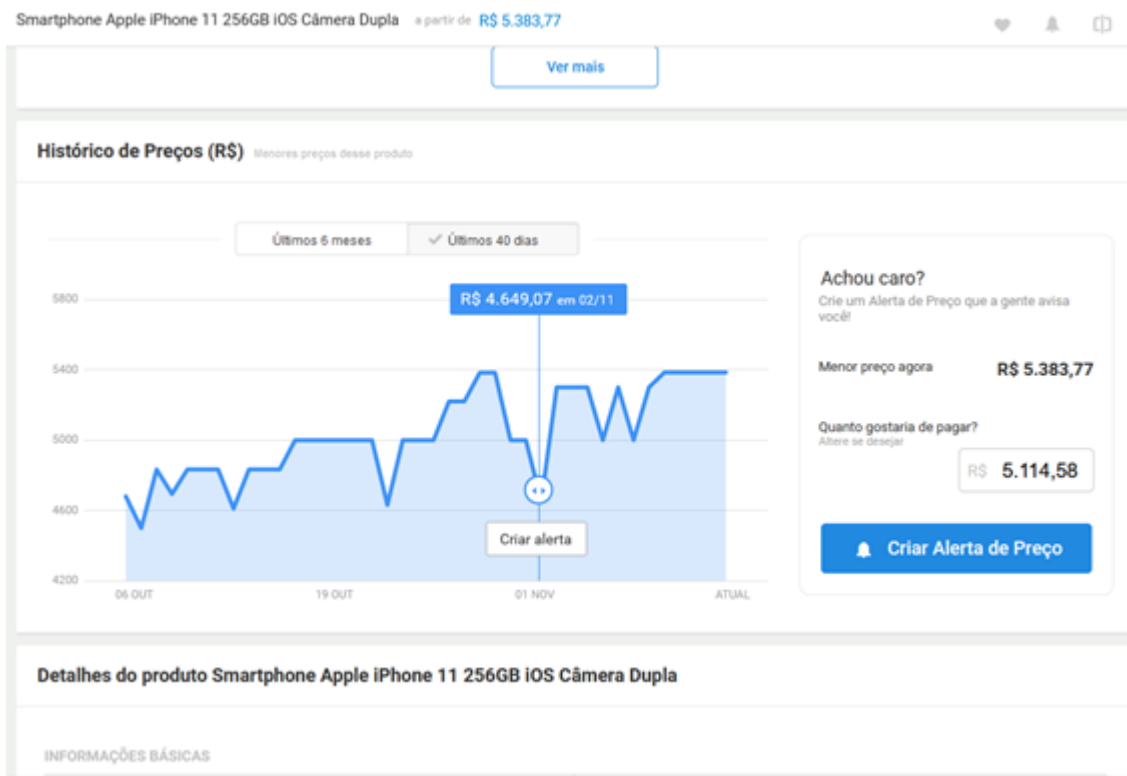
**8) Golpes com PIX.** Muitos criminosos também poderão explorar este momento envolvendo a novidade, falsear identidade visual de lojas e oferecer produtos com “desconto” para compras com o pix, oferecendo códigos errados ou chaves que direcionarão o pagamento para o fraudador. Muita cautela no uso da nova tecnologia;

**9) Desconfie de dados excessivos.** Cheque a política de privacidade do site, se conecte a partir de uma conexão segura, avaliando se o site também tem SSL (https) assegurando proteção contra interceptação de dados e jamais forneça dados mais que necessários para a compra, como “senha do cartão” e outros dados. Mantenha sempre seu sistema operacional atualizado, com firewall e anti-malware ativados;

**10) Faça provas de tudo.** Guarde provas de toda a compra, salve os códigos, registre prints, e-mails recebidos, se necessário registre em vídeo do processo de compra. Todos estes dados podem ser uteis diante de uma fraude ou golpe, onde a perícia digital poderá identificar a autoria dos criminosos.

Avaliar aspectos de legalidade de um site nem sempre é uma tarefa fácil para o consumidor. Embora a Lei Geral de Proteção de Dados já esteja em vigor (LGPD), já esteja em vigor, muitas lojas ainda não estão em conformidade e não são totalmente transparentes em seus processos.

Outra proteção importante, mas não realizada a golpes digitais, é avaliar as chamadas “fraudes” de lojas que sobem o preço para depois baixarem. Para isso sites como buscapé, zoom e baixou agora podem auxiliar, pois, apresentam um histórico do preço.



**Buscapé mostra preço do Iphone 11 em 02/11 e 14/11 de R\$ 4649,07 por R\$ 5383,00**

Caso tenha sido vítima de um golpe digital, o especialista, José Antonio Milagre, recomenda: “Imediatamente *resgate todos os dados da compra, registre um boletim de ocorrência online e procure um especialista em direito digital e crimes cibernéticos para que se incie um processo de apuração da autoria e responsabilização dos criminosos. Em casos de clonagem do chip, pode-se buscar a reparação em face da operadora de telefonia móvel.*”

Do mesmo modo é muito importante contactar o banco com informações sobre a fraude e notificar a loja que eventualmente teve a marca usada para a fraude, para se buscar uma resolução amigável. As lojas podem ser responsáveis, se não adotavam medidas de segurança da informação ou não monitoravam o uso indevido de suas marcas, permitindo que fossem usadas para fraudes e golpes.

Porém, é importante advertir, se a loja comprovar que não deu causa ou que a despeito de todas as ostensivas demonstrações de segurança, a culpa foi exclusiva do consumidor, esta pode

não se obrigada a reparar. Cada caso é um caso, e muitos deles serão apreciados pela Justiça. Por isso, prevenção é a melhor opção, sempre.

O IDCI (Instituto de Defesa do Cidadão e Consumidor na Internet) presta atendimento e apoio a vítimas de golpes e crimes cibernéticos, por seus canais, Siga @idcibrasil no Facebook e Instagram.

Prof. MSc. **José Antonio Milagre**, é Advogado e perito especializado em Direito Digital e Crimes Cibernéticos, Mestre e Doutorando Ciência da Informação pela UNESP, Presidente da Comissão de Direito Digital da OAB/SP Regional da Vila Prudente, Autor pela Editora Saraiva em co-autoria com o Professor Damásio de Jesus, dos livros “Marco Civil da Internet: Comentários à Lei 12.965/2014” e “Manual de Crimes Informáticos”. Fundador do Instituto de Defesa do Cidadão na Internet – IDCI.

***Canais:***

<http://www.instagram.com/drjosemilagre>

<http://www.facebook.com/drjosemilagre>

<http://www.youtube.com/josemilagre>

---

## **Nova modalidade de transferência “PIX” já é alvo de bandidos.**

Você já conhece o PIX? A nova modalidade de transferência foi criada pelo Banco Central e já é sucesso entre os consumidores pelas diversas vantagens que oferece em relação as outras modalidades de transferência, no entanto, os criminosos já

desenvolveram diversas formas de contornar o sistema e de se favorecerem com o novo serviço. Para saber como identificar os golpes e se proteger acompanhe as orientações do Especialista em Crimes Digitais Dr. José Milagre através do link abaixo.

<https://einvestidor.estadao.com.br/educacao-financeira/pix-fraude-protecao/>