CÂMARA DOS DEPUTADOS
Gabinete do Deputado Federal **HUGO LEAL –** PSD/RJ

PROJETO DE LEI Nº , de 2020.

(Do Senhor Hugo Leal).

Dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências.

O Congresso Nacional decreta**:**

CAPÍTULO I
Das Disposições Gerais.

Art. 1º Esta Lei estabelece princípios e diretrizes na aplicabilidade do Direito da Tecnologia da Informação, bem como normas de obtenção e admissibilidade de provas digitais na investigação e no processo, definindo crimes e penas.

Parágrafo único: As normas contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Art. 2º - Esta Lei será pautada pelos seguintes fundamentos:

I - Direito fundamental à proteção de dados, assegurando-se o seu uso de forma adequada, necessária e proporcional;

II - A garantia de acesso dos legítimos interessados à prova digital sob controle ou disponibilidade de terceiros;

III - Respeito à soberania nacional;

IV - A cooperação jurídica internacional;

V - Garantia de autenticidade e da integridade da informação;

VI - A Preservação da Empresa e sua função social;

VII - Transparência dos meios de tratamento da informação.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 3º Para feitos desta Lei considera-se:

I - Dispositivo eletrônico: Qualquer equipamento, instrumento ou componente que dependa para seu funcionamento dos princípios da eletrônica e use a manipulação do fluxo de elétrons para seu funcionamento.

II - Sistema Informático: Conjunto de dispositivos eletrônicos inter-relacionados que coletam, processam, armazenam e distribuem informações.

III - Protocolos de rede: Regras sobre como ocorrerá a comunicação entre dispositivos eletrônicos segundo padrões pré-determinados.

IV - Redes de Dados: Conjunto de dois ou mais dispositivos eletrônicos interligados por um sistema informático e guiados por protocolos de rede para compartilhar entre si informação e serviços.

V - Pacotes de dados: Estrutura unitária de transmissão de informação em uma rede de dados.

VI - Dados em transmissão: dados encapsulados em pacotes trafegando por redes segundo protocolos determinados.

VII - Dados em repouso: dados que se encontram armazenados em um dispositivo eletrônico ou sistema informático.

VIII - Prova nato-digital: informação gerada originariamente em meio eletrônico.

IX - Prova digitalizada: informação originariamente suportada por meio físico e posteriormente migrada para armazenamento em meio eletrônico, na forma da Lei.

X - Integridade da prova: certeza de que a informação que a constitui se mantém inalterada após o seu tratamento.

XI - Autenticidade da prova: certeza da sua origem, contexto ou autoria.

XII - Interceptação: coleta de dados em transmissão através de dispositivos eletromagnéticos, acústicos, mecânicos ou outros.

XIII - Metadados: qualquer informação sobre outra informação armazenada em meio eletrônico que identifique ou revele a origem, datas e horários relevantes e qualquer outra circunstância relativa ao contexto da evidência digital.

Art. 4º Considera-se prova digital toda informação armazenada ou transmitida em meio eletrônico que tenha valor probatório.

Parágrafo Único - À prova digital aplicam-se subsidiariamente as disposições relativas às provas em geral.

Art. 5º A admissibilidade da prova nato-digital ou digitalizada na investigação e no processo exigirá a disponibilidade dos metadados e a descrição dos procedimentos de custódia e tratamento suficientes para a verificação da sua autenticidade e integridade.

Parágrafo Único: Caso a prova digital seja produto de tratamento de dados por aplicação de operação matemática ou estatística, de modo automatizado ou não, devem estar transparentes os parâmetros e métodos empregados, de modo a ser possível a sua repetição e reprodutibilidade.

Art. 6º Poderão os legítimos interessados, para o fim da investigação ou instrução processual, requerer ordem judicial para guarda e acesso a prova digital sob controle de terceiros, observados os requisitos de necessidade, adequação e proporcionalidade.

§ 1º O requerimento deve individualizar usuários, provedores, dispositivos eletrônicos ou sistemas informáticos, temporalidades,

redes de dados e protocolos de rede próprios ao contexto do legítimo interesse manifestado, não podendo ter caráter genérico.

§ 2º Os dados encaminhados, transmitidos ou em suporte físico, pelos controladores ou provedores em cumprimento de ordem judicial ou requisição da autoridade policial e do Ministério Público devem estar em formato interoperável e com garantia de autenticidade e integridade.

Art. 7º Os provedores de infraestrutura, conexão e aplicação deverão manter, além das informações de guarda legal previstas em lei, os registros de dados necessários e suficientes para a individualização inequívoca dos usuários de seus serviços pelo prazo de 1 (um) ano.

Art. 8º Se houver receio de que a prova digital possa perder-se, alterar-se ou deixar de estar disponível, poderá o juiz, a requerimento do legítimo interessado, ordenar a quem tenha disponibilidade, controle ou opere os dados, que os guarde pelo prazo de até 1 (um) ano, podendo este prazo ser renovado, observadas a necessidade, adequação e proporcionalidade.

CAPÍTULO II
DA PROVA DIGITAL NA INVESTIGAÇÃO E NO PROCESSO PENAL
Seção I
Dos Meios de obtenção.

Art. 9º Constituem meios de obtenção da prova digital, na forma da Lei:

I – a busca e apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, e o tratamento de seu conteúdo.

II – a coleta remota, oculta ou não, de dados em repouso acessados à distância.

III – a interceptação telemática de dados em transmissão.

IV – a coleta por acesso forçado de sistema informático ou de redes de dados.

V – o tratamento de dados disponibilizados em fontes abertas, independentemente de autorização judicial.

Seção II
Interceptação Telemática

Art. 10 A interceptação telemática poderá ser destinada aos provedores ou serviços de infraestrutura, de conexão ou aplicação, bem como aos dispositivos eletrônicos ou sistemas informáticos particulares, devendo ser individualizadas as redes de dados e os protocolos de internet envolvidos.

Parágrafo Único. A interceptação telemática seguirá subsidiariamente o procedimento estabelecido para a interceptação telefônica.

Seção III
Requisição itinerante

Art. 11 O provedor de infraestrutura, de conexão ou de aplicação em face da qual tenha sido expedida a diligência, constatando que a medida deve ser cumprida por outro provedor, remeterá a requisição a este em caráter itinerante, a fim de se praticar o ato, independentemente de nova ordem, comunicando-se à autoridade judicial ou ao órgão de investigação em 24 (vinte e quatro) horas.

Parágrafo Único. Os provedores em face da qual tenha sido ordenada a diligência indicará à autoridade judiciária e ao órgão de investigação em 24 (vinte e quatro) horas os outros provedores através das quais tenha tido conhecimento da ocorrência de tráfego de dados pertinentes ao alvo da interceptação, com o fim de identificar todas os provedores envolvidos.

Seção IV
Coleta por Acesso Forçado

Art. 12 A coleta por acesso forçado a dispositivo eletrônico, sistema informático ou redes de dados, ocorrerá somente após prévia desobediência de ordem judicial determinando a entrega da prova pretendida ou quando impossível identificar o controlador ou provedor em território nacional, e compreenderá os métodos de

segurança ofensiva ou qualquer outra forma que possibilite a exploração, isolamento e tomada de controle.

Seção V
Decisão judicial e prazo

Art. 13 A ordem judicial para obtenção da prova digital para fins de investigação e processo penal descreverá os fatos investigados com a indicação da materialidade e possível autoria delitiva, indicando ainda os motivos, a necessidade e os fins da diligência, estabelecendo os limites da atividade a ser empreendida e o prazo para seu cumprimento.

§ 1º Em caso de monitoramento do fluxo de dados, o prazo da medida não poderá exceder a 60 (sessenta) dias, permitidas prorrogações por igual período, desde que continuem presentes os pressupostos autorizadores da diligência, até o máximo de 360 (trezentos e sessenta) dias, salvo quando se tratar de crime permanente, enquanto não cessar a permanência.

§ 2º A obtenção da prova digital pode se dirigir a uma terceira pessoa, desde que haja indícios de que o investigado utilize o dispositivo eletrônico, ou quaisquer outros meios de armazenamento de informação eletrônica, com ou sem o conhecimento do proprietário.

§ 3º O órgão de investigação ou o Ministério Público poderá requisitar a guarda da prova digital sem acesso ao conteúdo pelo prazo de 1 (um) ano, independentemente de autorização judicial, quando houver perigo na demora, devendo comunicar a medida ao juiz competente em até 24 (vinte e quatro) horas, para validação da medida.

Seção VI
Mandado judicial

Art. 14 A decisão judicial será instrumentalizada por mandado judicial, dirigido aos seus executores e às pessoas físicas ou jurídicas que irão sofrê-la, suficientemente instruído com informações sobre os fatos sob investigação, a pessoa física ou jurídica alvo da diligência, se possível, os dispositivos eletrônicos,

sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica, se for o caso, os provedores ou serviços de infraestrutura, de conexão ou de aplicação, potencialmente atingidos, o objeto da medida, os procedimentos autorizados a serem efetuados, os limites da apreensão e o prazo para cumprimento.

Parágrafo Único Será expedido mandado de intimação aos interessados, nos termos do caput, logo após o fim do cumprimento da medida, desde que não prejudique a operação.

Seção VII
Termo Circunstanciado

Art. 15 Ao fim da diligência para obtenção da prova digital, o órgão de investigação lavrará auto circunstanciado, com declaração do lugar, dia e hora em que se realizou, com menção das pessoas que a sofreram e das que nela tomaram parte ou a tenham assistido, com as respectivas identidades, bem como de todos os incidentes ocorridos durante a sua execução, especificando-se os procedimentos adotados e equipamentos utilizados.

Art. 16 Caso a diligência para obtenção da prova digital seja positiva, constará do auto circunstanciado a relação e descrição das coisas e dos dados apreendidos, bem como dos métodos de preservação de sua autenticidade e integridade.

Art. 17 O cumprimento da diligência será comunicado à autoridade judicial competente, no prazo de 72 (setenta e duas) horas, informando-se do seu resultado e do encaminhamento conferido aos objetos coletados e apresentando-se cópia do auto circunstanciado.

Seção VIII
Cadeia de Custódia Específica

Art. 18 Além do auto circunstanciado, será elaborado o registro da custódia do que foi apreendido na diligência, indicando os custodiantes e as transferências havidas, bem como as demais operações realizadas em cada momento da cadeia.

Art. 19 Os meios de obtenção da prova digital serão implementados por perito oficial ou assistente técnico da área de informática, que deverão proceder conforme as boas práticas aplicáveis aos procedimentos a serem desenvolvidos, cuidando para que se preserve a integridade, a completude, a autenticidade, a auditabilidade e a reprodutibilidade dos métodos de análise.

§ 1º A realização da obtenção garantirá, independentemente de norma técnica:

I - ambiente controlado com redução de contaminação;

II - espelhamento técnico em duas cópias, com o máximo de metadados e a descrição completa de procedimentos, datas, horários ou outras circunstâncias de contexto aplicáveis;

III - preservação imediata após o ato de espelhamento com emprego de recurso confiável que garanta a integridade da prova.

§ 2º A autoridade judicial, mediante requerimento do órgão de investigação ou do interessado, requisitará aos controladores o encaminhamento de dados pessoais associados à prova digital obtida e que sejam complementares e suficientes para a sua análise contextual.

Art. 2O Uma cópia dos dados resultantes da diligência, feita por espelhamento, será encaminhada e armazenada pela autoridade judicial competente, para eventual confronto. As análises, as pesquisas e os exames periciais devem ser realizados sobre cópia de trabalho.

Art. 21 Salvo expressa determinação judicial em contrário ou impossibilidade de cumprimento da medida desta forma, a apreensão da prova digital ocorrerá por espelhamento, não se fazendo a apreensão de dispositivos eletrônicos, sistemas informáticos ou quaisquer outros meios de armazenamento de informação eletrônica.

Seção IX
Restituição de dispositivos eletrônicos ou sistemas informáticos

Art. 22 Em caso de impossibilidade de apreensão por espelhamento, será garantida aos titulares ou agentes de tratamento atingidos pela apreensão dos dispositivos eletrônicos, sistemas informáticos ou outros meios de armazenamento de informação eletrônica cópia dos dados coletados. A apreensão não poderá superar 60 (sessenta) dias, salvo por motivo relevante.

Seção X
Sigilo profissional e religioso

Art. 23 Os meios de obtenção da prova digital observarão o sigilo em razão de função, ministério, ofício ou profissão, incluindo, mas não se limitando, o sigilo médico, religioso e o sigilo da relação advogado e cliente, ressalvados os casos em que o exercício da atividade represente ou preste-se a encobrir a atuação delitiva.

Seção XI
Dados íntimos e restrições de acesso à informação

Art. 24 Os dados pessoais sensíveis, íntimos ou sigilosos do investigado, acusado ou pessoas a ele relacionadas, que sejam relevantes ao caso, mas que não digam respeito aos demais sujeitos processuais, serão apartados em autos próprios, mantendo-se acessíveis apenas aos interessados, vedada a alteração do espelhamento.

§ 1º Decorridos 05 (cinco) anos do cumprimento integral da sentença condenatória ou em caso de absolvição ou de decretação de extinção de punibilidade, os dados mencionados no caput serão indisponibilizados, desde que não haja interesse público na preservação ou que não tenham relevância ou pertinência processual, devendo ser intimados os interessados e atualizada a garantia de integridade e anterioridade dos dados remanescentes.

§ 2º Os dados que se enquadrem nas restrições de acesso à informação, nos termos da Lei, serão apartados em autos próprios e encaminhados em 24 (vinte e quatro) horas à autoridade competente, vedada a alteração do espelhamento.

Seção XII
Encontro fortuito e serendipidade

Art. 25 Se, na coleta da prova digital judicialmente autorizada, houver o encontro fortuito de dados relacionados a fatos diversos, estes deverão ser remetidos como notícia crime ao órgão de investigação.

Seção XIII
Infiltração virtual

Art. 26 A infiltração de agentes de investigação em redes de dados, conectadas entre si ou não, com o fim de investigar crimes punidos com pena privativa de liberdade máxima igual ou superior a 4 (quatro) anos, obedecerá às seguintes regras:

I – será precedida de autorização judicial, mediante requerimento do Ministério Público, órgão de investigação ou representação de delegado de polícia, que conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a individualização dessas pessoas;

II – não poderá exceder o prazo de 60 (sessenta) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 360 (trezentos e sessenta) dias e seja demonstrada sua efetiva necessidade, salvo quando se tratar de crime permanente, enquanto não cessar a permanência.

§ 1º A autoridade judicial, o órgão de investigação e o Ministério Público poderão requisitar relatórios parciais da operação de infiltração a qualquer tempo.

§ 2º A tramitação da medida será em autos apartados, cujo acesso somente será dado ao juiz, ao membro do Ministério Público, ao órgão de investigação e à autoridade policial, que podem indicar formalmente no máximo dois auxiliares para colaborarem.

Art. 27 É atípica a conduta do agente que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes investigados.

Parágrafo Único. Não é punível, no âmbito da infiltração, a prática de crime pelo agente infiltrado no curso da investigação, quando inexigível conduta diversa.

Art. 28 Os órgãos de registro e cadastro público e privado poderão incluir nos bancos de dados próprios, mediante procedimento sigiloso e requisição da autoridade judicial, as informações necessárias à efetividade da identidade fictícia criada.

Art. 29 Concluída a investigação, todos os atos eletrônicos praticados durante a operação deverão ser registrados e armazenado, devendo ser encaminhados ao juiz e ao Ministério Público, juntamente com relatório circunstanciado.

Parágrafo Único. Os atos eletrônicos registrados citados no caput deste artigo serão reunidos nos autos apartados e vinculados ao processo judicial juntamente com a investigação criminal, assegurando-se a preservação da identidade do agente infiltrado e, se necessário, das pessoas envolvidas.

Seção XIV
Ação disfarçada

Art. 30 É admissível a medida de ação disfarçada de agentes de investigação ou, excepcionalmente, de particular no curso da investigação relativa aos crimes cometidos por meio eletrônico, ainda que parcialmente, quando presentes elementos probatórios razoáveis de conduta criminal preexistente e em andamento, independentemente de autorização judicial.

Parágrafo Único. À ação disfarçada aplicam-se as disposições relativas à infiltração policial, no que for cabível.

CAPÍTULO III
DOS CRIMES E DAS PENAS
Seção I
Falsidade informática

Art. 31 Falsificar, omitir, introduzir, modificar ou suprimir dados informáticos ou por qualquer outra forma interferir em um tratamento de dados, produzindo informação ou seu registro

documental ilícito, no todo ou em parte, para que seja considerado ou utilizado para finalidade juridicamente relevante.

Pena - reclusão, de três a oito anos, e multa.

§ 1º Se a informação é gerada originalmente por pessoa jurídica de direito público interno ou estrangeiro.

Pena - reclusão, de quatro a doze anos, e multa.

§ 2º Se o intuito for a obtenção de vantagem econômica indevida:

Pena - reclusão, de quatro a dez anos, e multa.

§ 3º Elaborar, produzir, importar, distribuir, vender ou possuir para fins comerciais qualquer dispositivo eletrônico, sistema informático ou código malicioso que permita o acesso a meio de pagamento.

Pena - reclusão, de quatro a doze anos, e multa.

§ 4º Se o agente é funcionário público e comete o crime prevalecendo-se do cargo.

Pena - reclusão, de quatro a doze anos, e multa.

Seção II
Dano informático

Art. 32 Indisponibilizar, alterar, destruir, danificar, suprimir ou tornar não acessíveis permanentemente sistemas informáticos, programas de computador, rede de dados ou dados armazenados em meio eletrônico sob controle ou operação de terceiros, no todo ou em parte, ou por qualquer forma lhes afetar disponibilidade, sem permissão legal ou para tanto estar autorizado.

Pena - reclusão, de dois a seis anos, e multa.

§ 1º Incorre na mesma pena quem indevidamente elaborar, produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir em redes de dados, dispositivos eletrônicos ou sistemas informáticos, programas de computador ou código malicioso destinado a produzir as condutas não autorizadas no caput.

§ 2º Se o dano atingir de forma grave ou por tempo relevante um dispositivo eletrônico, rede de dados ou sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas, especialmente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Pena – 3 a 6 anos.

§ 3º Se o agente é funcionário público e comete o crime prevalecendo-se do cargo.

Pena - reclusão, de quatro a doze anos, e multa.

Seção III
Sabotagem informática

Art. 33 Entravar, impedir, interromper ou perturbar o funcionamento de um dispositivo eletrônico, sistema informático ou rede de dados, através da introdução de código malicioso, programa de computador ou qualquer outra forma de interferência, capaz de causar deterioração, danificação, alteração, indisponibilização ou impedimento do acesso, sem permissão legal ou sem para tanto estar autorizado.

Pena - reclusão, de um a cinco anos, e multa.

§ 1º Incorre na mesma pena quem ilicitamente elaborar, produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir em dispositivo eletrônico, sistemas informáticos ou rede de dados, programa de computador ou código malicioso destinado a produzir as condutas não autorizadas no caput.

2º Se a sabotagem atingir de forma grave ou por tempo relevante um dispositivo eletrônico, rede de dados ou sistema informático que apoie uma atividade destinada a assegurar funções sociais críticas, especialmente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Pena - reclusão, de dois a seis anos, e multa.

Seção IV
Acesso ilícito

Art. 34 Aceder de qualquer modo a um dispositivo, sistema informático ou redes de dados sem permissão legal ou sem para tanto estar autorizado.

Pena - detenção, de seis meses a dois anos, e multa.

§ 1º Se o agente é funcionário público e comete o crime prevalecendo-se do cargo.

Pena - 1 a 3 anos

§ 2º. 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.

§ 3º Incorre na mesma pena quem elaborar, produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir ilicitamente programa de computador ou código malicioso em sistemas informáticos, dispositivos eletrônicos ou redes de dados, a fim de produzir as condutas não autorizadas descritas no caput.

§ 4º Se, através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei.

Pena - reclusão, de dois a seis anos, e multa.

Seção V
Interceptação ilícita

Art. 35. Coletar, interceptar, capturar ou obter, através de meios técnicos, dados em transmissão sem permissão legal ou sem para tanto estar autorizado.

Pena - reclusão, de dois a quatro anos, e multa.

§ 1º Incorre na mesma pena quem ilicitamente elaborar, produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir em dispositivo eletrônico, sistemas informáticos ou rede de dados, programas de computador ou código malicioso destinado a produzir as condutas não autorizadas no caput.

CAPÍTULO III
DISPOSIÇÕES FINAIS

Art. 36. O Decreto-Lei 2.848/40 (Código Penal) passa a vigorar com as seguintes alterações.

"Art.
325.....
.....

.....
.....

I - permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas banco de dados da Administração Pública." (NR)

Art. 37. Revogam-se os artigos 154-A e 313-A do Decreto-Lei 2.848/40.

Art. 38. Esta Lei entra em vigor 60 dias após a data de sua publicação.

JUSTIFICAÇÃO

A forte influência que a tecnologia vem exercendo sobre o modo de viver do ser humano tem provocado, também, intensa alteração na constituição e regulação dos fatos jurídicos contemporâneos.

Contratos eletrônicos, moedas virtuais e relações sociais digitais se tornaram de tal forma presentes e relevantes na sociedade a ponto de fazer anacrônica a legislação disponível. Tal circunstância tem gerado grandes dúvidas sobre o correto entendimento e tratamento destas realidades modernas e cambiantes, trazendo insegurança jurídica e angústias.

Em paralelo, instituiu-se ao longo dos últimos 20 anos uma diversidade de normas visando, de algum modo, adaptar o regramento diante das novas possibilidades, o que ocorreu na medida em que vieram surgindo.

Nesta leva, veio a digitalização dos registros públicos, a partir das disposições da Lei 11.977/2009 (que em seu artigo 37 e seguintes criou o registro imobiliário eletrônico) tendo o tema evoluído a ponto de alcançar hoje os registros notariais de toda ordem, como se observa da edição do provimento 100/2020 do Conselho Nacional de Justiça.

Ademais, tanto o processo judicial quanto o administrativo migram rapidamente para um processamento integralmente eletrônico, fatores autorizados e fomentados pela Lei 11.409/2006, pelo CPC de 2015 e demais diplomas autorizativos da ação de sistemas eletrônicos de informação (SEI), o que vem ocorrendo em todos os entes federativos e demais pessoas jurídicas de direito público interno.

As regras sobre a digitalização documental foram amplamente introduzidas em nosso ordenamento através da Lei 12.682/12 e suas regulamentações, tornando algo autônomo da mera fotocopia o processo de desmaterialização de um documento público ou particular.

No plano penal, temos gerado paulatinamente no ordenamento diversos tipos penais cuja matriz factual é de ordem tecnológica, tais como as alterações provocadas pela Lei 12.737/12, a par de outras advindas de outras legislações.

Em 2018, a Internet era utilizada em 79,1% dos domicílios brasileiros (https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html acessado em 05/10/2020). Consequentemente, a migração massiva das relações sociais para o meio

eletrônico tem o substancial efeito de digitalizar os conflitos, matéria-prima do Direito.

De fato, a forma dos negócios jurídicos, e mesmo da prática de ilícitos civis e penais, sofreu grande transformação em um curto período, a fazer desafiar a adaptabilidade do Direito que, agora, precisa ainda reconhecer a existência e necessidade de proteção maior de direitos fundamentais que decorrem da própria existência de um mundo cibernético.

Esta realidade, inexorável e galopante, torna fundamental prover uma resposta aos anseios sociais quanto a uma norma capaz de regular as novas peculiaridades e bens jurídicos advindos da evolução tecnológica de um modo mais uniforme.

Neste cenário, as legislações vigentes, a exemplo do Marco Civil da Internet (Lei n. 12.965/14), da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/18) e do Projeto do Senado de Combate a Notícias Falsas (Projeto de Lei n. 2.630/20), objetivaram conceituar e regular este novo ambiente de fatos jurídicos, mas não trouxeram em seu bojo a definição suficiente de conceitos e protocolos probatórios. A evidência digital tem natureza e comportamento distinto das conhecidas evidências físicas, confortavelmente assentadas em classificações documentais, testemunhais e periciais. Sua natureza eletrônica, consubstanciada hodiernamente em um padrão binário, mas já caminhando para novas codificações quânticas, revela a premente necessidade de complementar as normas vigentes que trouxeram a regulação do uso de dados pessoais, relações sociais por meio da Internet, transparência da informação, processamento eletrônico e armazenamento massivo de documentos em formato nato-digital. As velhas práticas probatórias solidificadas no ambiente físico, uma vez transportadas para os meios eletrônicos, ganham alcance ampliado, o que necessita ser harmonizado, também, com os impactos da cibernética nos direitos fundamentais.

Destarte, os conflitos surgidos na colidência de diversos direitos e garantias (proteção à intimidade, à vida privada, à honra e à imagem das pessoas, além da liberdade de expressão, de opinião e o direito de ser informado), todos de sede constitucional, encontram um concreto caminho de pacificação na ampliação da compreensão e da regulação dos meios de prova eletrônicos - atendendo-se aos princípios da proporcionalidade e da

adequação -, bem como na definição de tipicidades e protocolos processuais cíveis e penais aderentes não só ao microssistema de Direito Digital mas, principalmente, à ontologia da existência humana no ciberespaço.

Existem diversas legislações vigentes internacionais e brasileiras sobre dados e provas digitais, além de várias normas técnicas. As mais importantes são:

- Convenção de Budapeste de 2001;

- Carta Europeia de Ética sobre o Uso da Inteligência Artificial (na Justiça Preditiva) de 2018;

- Lei n. 109/2009 (Portugal);

- Art. 588 da Ley de Enjuiciamiento Criminal (Espanha);

- Art. 242 do Código de Procedimiento Penal (Colômbia);

- Lei n. 12.965/14 (Marco Civil da Internet – LMCI);

- Lei 13.709/18 (Lei Geral de Proteção de Dados Pessoais – LGPD);

- Lei 13.874/19 (Lei da Liberdade Econômica);

- Provimento n. 100/2020 do CNJ (atos notariais eletrônicos);

- Diretrizes para evidências digitais n. 27.037 da ABNT de 2013 e RFC 3227/2002;

- Procedimento Operacional Padrão (POP) da Perícia de Informática Forense do MJ de 2013;

- Protocolo da Internet Engineering Task Force (IETF);

- Protoloco do National Institute of Standards and Technology (NIST);

- Artigos 439 a 441 do Código de Processo Civil Brasileiro de 2015;

- Lei 11.419/2006 – Lei do Processo Eletrônico;

- Lei 12.682/12 e seu Decreto regulador 10.278/20.

Referido projeto, desenvolvido por meio da coordenação dos Promotores de Justiça do Ministério Público do Estado do Rio de Janeiro e Professores SAUVEI LAI e PEDRO BORGES MOURÃO, perfaz a necessária simbiose entre Tecnologia e Direito, compatibilizando instrumentos jurídicos e harmonizando a nomenclatura técnica dessas legislações, com o necessário tratamento legislativo no uso da evidência digital diante do decidido pelo E. Supremo Tribunal Federal nas ADIs 6.387, 6.388, 6.389, 6.390 e 6.393.

De fato, uma vez reconhecida a existência de um direito autônomo à proteção de dados pessoais, que se diferencia da proteção da intimidade e da vida privada, resta declarada nova cláusula de validade da ação estatal e dos particulares no manejo da evidência e dos dados em geral.

Ademais, o presente projeto foi elaborado depois de reuniões com advogados e membros da academia (Professores Geraldo Prado, Flaviane Barros, Fauzi Hassan, Victoria de Sulock e Manuel Valente, entre outros), além de integrantes do Ministério Público do Estado do Rio de Janeiro (MPRJ) e de peritos da comunidade eletrônica (do MPRJ, da Polícia Civil do Estado do Rio de Janeiro e daqueles que prestam consultoria à investigação defensiva).

Durante a reunião com os advogados, estes manifestaram preocupação com a guarda e preservação de urgência de dados (art. 3º do anteprojeto), mediante requisição direta do órgão de investigação e do MP, independente de autorização judicial – por dotar de poderes extraordinários os órgãos de persecução criminal –, algo que já existe no art. 13, § 2º e art. 15, § 2º da Lei n. 12965/14, bem como na legislação internacional (Lei n. 109/2009 de Portugal).

Também houve questionamento acerca da requisição itinerante (art. 6º) que permite um provedor encaminhar a ordem judicial ou do órgão de investigação diretamente a outro provedor, quando perceber que houve a portabilidade de serviço por parte do usuário para provedor diverso, dispensando a devolução ao juiz para emissão de nova ordem – mas com comunicação imediata –, como ocorre na carta precatória itinerante do art. 262 do Código de Processo Civil.

Em suma, o projeto buscou equilibrar os seguintes objetivos:

- Direito fundamental à proteção de dados, assegurando-se o seu uso de forma proporcional, adequada e necessária (art. 2º.);

- A garantia de acesso dos legítimos interessados à prova digital sob controle ou disponibilidade de terceiro (art. 6º.);

- O respeito à soberania nacional e o estímulo à ampliação da cooperação jurídica internacional no tema (art. 2º.);

- A preservação da Empresa e da sua função social (art. 2º.);

- A transparência e a garantia de integridade e autenticidade dos meios de tratamento da informação – transparência algorítmica (art. 5º.);

- A eficiência da persecução criminal com as garantias individuais, sobretudo a paridade de armas;

- A legalização de instrumentos investigatórios modernos e atuais, a exemplo da coleta remota, oculta e forçada (art. 2º), além da infiltração policial (art. 20) e ação disfarçada (art. 24);

- O uso de expressões genéricas (art. 1º), mantendo-se a essência da segurança jurídica (art. 13), porém sem o risco de tornar a legislação obsoleta;

- A exigência da boa prática forense (art. 13), aliada à realidade pericial;

- A harmonização de termos jurídicos e técnicos, à luz das legislações nacional e estrangeira, destacando-se: 9.10.1. A coleta remota e oculta (art. 2º);

- A coleta em fontes abertas (art. 2º);

- O Legal hold, ou seja, guarda e preservação de dados (art. 3º);

- A requisição itinerante, isto é, redirecionamento de ordem (art. 6º);

- O acesso forçado de sistema informático (art. 5º) do art. 19.1 da Convenção de Budapeste;

- A especificação da cadeia de custódia da prova digital (art. 13);

- O respeito ao sigilo profissional (art. 17) e de dados íntimos (art. 18);

- O encontro fortuito (art. 19);

- A infiltração virtual do art. 20, inspirado no instituto do art. 190-A da Lei n. 8.069/90 (Lei n. 13.441/17) c/c art. 13 da Lei n. 12.850/13;

- A ação disfarçada do art. 24, semelhante à ação de agente policial disfarçado do art. 33, § 1º, IV da Lei n. 11.343/06, do art. 282 da Ley de Enjuiciamiento Criminal (Espanha) e do art. 242 do Código de Procedimiento Penal (Colômbia).

Traz-se, assim, na presente proposta, não só regras e fundamentos gerais aplicáveis ao Direito material civil e penal, mas também, regras processuais complementares aptas a pacificar e prevenir dissídios jurisprudenciais e o alongamento processual.

Vale registrar, ainda, que no plano material e processual a norma visa atualizar disposições anteriores, animada a cognição não só pela evolução tecnológica, mas também pela experiência acumulada pelo Direito na observação e tratamento das condutas lícitas e ilícitas observadas.

Por todo o exposto, visando contribuir para o aprimoramento da legislação de nosso País, e entendendo como salutar a proposta que ora apresentamos, contamos com os Pares para a aprovação desta matéria.

Sala das Sessões, de de 2020.

Dep. **HUGO LEAL**
PSD/RJ